RECORDED VOICE: This meeting is now being recorded.

BRENDA BREWER: Thank you, Alan. This is Brenda speaking for the record and I'd like to welcome you all to the RDS WHOIS2 Review Team Plenary Call #22 on March 5th, 2018 at 14:30 UTC. In attendance today we have Dmitry, Alan, Susan, Lili, Erika, Carlton., Cathrin. From ICAN Organization we have Alice, Brenda, Amy, Steve, Lisa and Jean-Baptiste.

We have apologies from Volker, Chris and Thomas, and at this time there are no observers. Today's call is being recorded. May I please remind you to state your name before speaking for the transcript and I'll turn the meeting over to you, Alan. Thank you.

ALAN GREENBERG: Thank you very much. Is there any additions to the agenda or any other business? It is a longer agenda than we're likely to finish today but we're optimistic and we wanted to make sure we could cover if any of the people were not in fact here.

Seeing no hands, I will presume the agenda is accepted as displayed and we'll go onto the first item. Any statement of interest updates? Seeing nothing, we'll go into the first item on the agenda and that is Outreach and I presume I'm turning this over to Jean-Baptiste.

JEAN-BAPTISTE DEROULEZ: Thank you, Alan. So on the blog post very quickly I will provide you with an update, there were no comments received from the review team on the blog post last week, and so the blog post has been published on February 27 on ICANN .org, you have the link in the slide deck.

For right now I will encourage you to spread the word and share this blog post around you and on our side, we will be drafting a note for the leadership that will go out to the [inaudible] leadership to inform them about this and about the review team's next steps. Any questions on that? Also, Alice has placed the blog post link into the chat so that it's clickable for you.

ALAN GREENBERG: Thank you. I hear nothing, I see nothing, we'll assume that is all in order and we'll go into the next item which is the major item in our agenda today and that is sub group updates status. Oh, sorry, I see Lisa's hand is up. I'm not hearing Lisa. I see your phone says your speaking but I'm not hearing any voice.

And Lisa will dial back in, we'll give her a moment. [AUDIO BREAK]

Lisa wanted to suggest that the review team members do outreach to their own stakeholder groups about the blog post. I think Jean-Baptiste already suggested that and we will be sending a message out to the leadership in each of those groups in any case, but yes. Let us go on to the first substantive item and that is the sub group update status, and the first one on our list is Cathrin. Is Cathrin on the bridge yet or in a position to speak?

CATHRIN BAUER-BULST: I'm on the phone. If I may, I will provide the update orally.

ALAN GREENBERG: That is fine.

CATHRIN BAUER-BULST: Excellent. I'm just making my way up to the home office. If you hear I am out of breath it's because our house is very tall and very narrow. So to be quite short I'm updating you on the strategic priorities sub group, which is not entirely my fault, has not yet been very active.

While we did formulate a series of detail briefing questions back in the first task document, we're going to have a first discussion of them tomorrow with the sub group members and on that basis we hope to proceed with reaching a request to ICANN to basically get to the bottom of a couple of factual questions such as in what way, shape or form the strategic priority that is supposedly given to WHOIS is evident in things such as consultation agreements or just strategic prioritization within ICANN as an organization, where we're going to ask for a bit more details on how exactly [inaudible].

On the base of tomorrow's call, we hope to then also determine the best format for this as tentatively it's suggested is that we do that through a written request, so a request for written input that could then be followed up by a conversation, also building on a very positive experience from the compliance sub group where they were able to use Susan's presence in Los Angeles to actually have a face to face meeting

with the compliance team to go through a couple of the questions and we might wish to reproduce that through a remote meeting.

And I've also sent a draft of the planning questions to the sub group and have not yet received any comments so I think those are pretty much ready to be shared with the group but I will wait for the endorsement of the sub group tomorrow and then share a note with the group as a whole. That's my brief update for now, I'm available of course for any questions that you may have.

ALAN GREENBERG: Thank you. Why don't we take this break to see if Lisa can actually speak?

LISA PHIFER: Thank you, Alan, can you hear me now?

ALAN GREENBERG: We can, perfectly.

LISA PHIFER: Thanks.

ALAN GREENBERG: The trials and tribulations of Adobe Connect. Is there anyone with any questions for Cathrin? And there are no hands, then we will go onto the next item, thank you. I look forward to that meeting, even though it's at

a semi unreasonable time tomorrow for me. We now have Cathrin on Adobe Connect and the next item --

CATHRIN BAUER-BULST: I'm sorry about the unreasonable time.

ALAN GREENBERG: It's quite a reasonable time for you. Alright, next item on our agenda is privacy proxy if we have someone who is in a position to speak to it, and Susan, that would probably be you if indeed you are going to speak to it or are we going to defer this one?

SUSAN KAWAGUCHI: I really wasn't prepared but I did see your email and I thought maybe if we don't have anybody else prepared to speak to it that maybe we could discuss that a little bit?

ALAN GREENBERG: Sure.

SUSAN KAWAGUCHI: You felt like most of the questions weren't relevant, so I was just wanting to --

ALAN GREENBERG: Let me go back and get the questions, hold on. Let me see if I can pull that up quickly, I'm not sure I can. Sorry, just give me a moment.

SUSAN KAWAGUCHI: We did start to develop questions for ICANN Staff and for just a general [inaudible]. The sub team is developing questions and Alan had some input just as a space for everybody else.

ALAN GREENBERG: There were a lot of questions posed I think mainly by Volker and they're all relevant to the implementation or to the privacy proxy issue but I'm not sure what the Nexus point, the intersection is with WHOIS specifically? The only reason we have privacy proxy services is to protect WHOIS information. There is clearly a connection to WHOIS but as an example are any parts of the implementation will require new technology, what internal systems be used.

I'm looking at some of the other ones, what are the challenges to implementation, those are really associated with the privacy proxy implementation but I'm not sure what the connection is to WHOIS, although conceivably, some of the answers might reference WHOIS, but there doesn't seem to be any apparent connection that we can make right now and therefore that's why I'm asking are these really WHOIS questions or are they an in depth review of the privacy proxy implementation which of course, in terms of the work it has to do, having as contract parties, privacy proxy servers and the contracts and all sorts of procedures associated with that, I'm not sure what the real connection is to WHOIS itself. Maybe I'm missing some point here.

SUSAN KAWAGUCHI: No, that's an interesting perspective in some ways I was thinking, because I drafted some of those questions, probably all of the ones you mentioned, I was thinking that because the first WHOIS review team outlined in quite a bit of detail for what the privacy proxy service or privacy proxy policy should be, that actually [inaudible] the point of implementation or getting close that it was critical to know if this is worked or not, so that's why those questions went to technologies and budget and all those kinds of things. I'll take another look at that and talk to Volker and the rest of the crew and see if we might remove some of those.

ALAN GREENBERG: Again, I'm not sure of if that's really relevant but if it is, I would assume that could be covered with a global question saying at this point, do you see any impediments to implementing the policy? As opposed to going into some depth to all of the potential issues that could arise or the almost looking ahead or saying what might the answers be.

SUSAN KAWAGUCHI: Yes, no that's a good point. I'll note that.

ALAN GREENBERG: Any other comments on this one?

CATHRIN BAUER-BULST: This was just to say that one thing we also discussed was whether there could be some cross [inaudible] with the law enforcement needs sub

group in the sense that we might want to integrate a question or two in a possible survey to be done for the law enforcement needs one on how law enforcement works with the privacy proxy and whether there are specific issues and that might also be true for other user groups but of course that's one that I'm particularly aware of and one thought that actually [inaudible] reaction to Volker's suggestion that we might check with ICANN how many complaints they have gotten on the privacy proxy services thus far, which I think [inaudible] there probably would have been none so far. We clearly need to find some other way of identifying issues if there are any.

ALAN GREENBERG: I would assume with law enforcement you would have to ask, have there been any problems with the current, less formal implementation of privacy proxy servers and do you foresee any or do you foresee any change and if so, what changes with the more formal version?

Clearly, it's been completely unregulated, then there are no rules right now as to, other than the rules of law in the jurisdiction where they live, as to how the information might be unveiled by privacy proxy services, where as in the new implementation perhaps there's something more detailed, although I'm not sure there is. Alright, any further comments on privacy proxy?

The next item, which also we do not have anyone on the call with regard to, is the common interface. That was also Volker's and we have Susan's hand up on that, please go ahead.

SUSAN KAWAGUCHI: Looks like Volker has joined so we should ask [CROSSTALK].

ALAN GREENBERG: We do have Volker, despite apologies. Volker, welcome.

VOLKER GREIMANN: Well, the meeting [inaudible]. Hopefully I'm prepared, but I thought I would join anyway just to make sure that [CROSSTALK]--

ALAN GREENBERG: We just had a recap on privacy proxy, were you on the call at that point?

VOLKER GREIMANN: I just joined, literally five seconds ago.

ALAN GREENBERG: Alright. Susan raised the issue on privacy proxy of my email which had asked to what extent are all of those questions really directly related to WHOIS, as opposed to related to the privacy proxy actual implementation; and her answer, Susan if I can try to summarize very quickly, was really that if there are any difficulties and there's a lot of work that has to be done to implement the privacy proxy policy, if there are impediments to that, then that will ultimately have an effect on WHOIS, and I suggested that maybe asking a simpler question, not foreseeing what the answers are but simply saying, do you Staff foresee any potential impediments to implementing the policy as written?

That's sort of where we stopped in that discussion. I don't know if you have any insight or want to add anything to it at this point but I'll give you a chance and then go onto the next item, if not.

VOLKER GREIMANN: It's a good question but I do think that that there is direct connection between privacy proxy providers and WHOIS, so delving into that is maybe worth our while. Even though we decided that we can have these providers, that does not impact the requirements of data quality that these providers have to meet and even though this data is not in public WHOIS forum, internally we still called WHOIS data even though it's not public, it's just hidden WHOIS data.

ALAN GREENBERG: That is certainly true but I'm not sure how the implementation team are going to comment on that. It's an interesting question of how you ensure quality when you can't see the data.

VOLKER GREIMANN: True enough.

ALAN GREENBERG: I'm not an expert on that policy. I paid relatively little attention to the PDP as it was going on. I'm assuming that whatever responsibilities are on registrars to validate data or validate these formats and any of the accuracy requirements are also intern put on the privacy proxy providers, is that not the case?

VOLKER GREIMANN: Unless I'm very much mistaken, that is the case. It's harder to verify that.

ALAN GREENBERG: It's impossible to verify it.

VOLKER GREIMANN: It may come into effect once privacy proxy providers decides to no longer provide services for certain domain or other cases where they would be required to review the underlying data, for example to inquire who is law enforcements interests that have the right to access that data. If it's then found that this data is substandard quality then we say, that would probably give rise to the opportunity to complain to ICANN compliance and tell them the provider did not do their job right. That would a case where that works.

ALAN GREENBERG: Indeed. Any further comments on privacy proxy?

VOLKER GREIMANN: No, I think we are in a good status here. There have been no further comments that I've seen. I haven't gone through all the emails from last night but I don't think there's any. There were no further wishes for comments so I think the questions that we have at this point will allow us to move forward and we'll allow us to start our work.

ALAN GREENBERG: Lisa put in the chat that obviously one of your requirements is to make sure that policy, the outcome of the PDP address the issues raised in the first recommendation, that I assume something you can do by simply looking at the PDP, we don't have to ask questions at the policy, we don't have ask explicit questions to do that.

VOLKER GREIMANN: Right but there's always difference between the recommendation and the implementation there of and we do not have that implementation stage yet. We may get an indication before we finish our work. We will have to base it on part of the policy, that is the recommendation not the impact policy that will go into effect once implementation work has completed.

ALAN GREENBERG: Given that the budget doesn't allow us to have a time machine, I think we have no choice.

VOLKER GREIMANN: Question for ICANN, could we extend the budget for a time machine? I'd like one.

ALAN GREENBERG: Well, I think the onus is on us to point to suppliers first. Dmitry, please go ahead.

DMITRY BELYAVSKY: It seems to me that problem with the privacy proxy services is very related with [inaudible] to data accuracy itself and to consumer trust. Just because all of this reference from [inaudible] data from our public sources. Thank you.

ALAN GREENBERG: That's indeed true, although nothing I think we can do about it. Any further comments? Lili, please go ahead.

Lili, you're very, very hard to hear, I cannot make out what you're saying.

LILI SUN: Is this getting better?

ALAN GREENBERG: It's a little better, it's still hard but we'll try.

LILI SUN: In the data accuracy [inaudible], I also saw there are overlaps with [inaudible] destination for the WHOIS accuracy for proxy and privacy services is based on the service providers' contact information, so [inaudible] is possible to validate the real registrant contact information and thinking how to deal with this issue and the data accuracy subgroups.

ALAN GREENBERG: Alright, thank you. I think I heard what Lili was saying and I'll try to repeat it. She said that there are overlaps between privacy proxy and data accuracy since it is not possible in a general case to verify that indeed they're doing, the question is, are we meeting the requirements of the data accuracy?

Any my take on that is, that's a very real issue, I'm not sure we can do anything else other than report on it and as Volker pointed out, that when information is revealed, at that point then there is an opportunity to look at privacy proxy information and in the small samples that are revealed and say were there accuracy problems? If something is revealed to law enforcement, that doesn't make it into the public, however the UDRP does require that as one of the results of a UDRP the information about the real registrant is revealed.

It's an interesting aspect that in fact you can force a privacy proxy information to revealed by filing a UDRP and unless it's proven to be completely frivolous and maybe even that case, the UDRP rules require it to be revealed. We do have a small sample of examples where proxy, WHOIS information is revealed in a public sense, a very small sample but other than that, you're right but I'm sure there's anything we can do, other than identify as an ongoing problem. Lili, did I capture what you said accurately?

LIL SUN: Yes, I think so.

ALAN GREENBERG: Thank you. Lisa, please go ahead.

LISA PHIFER: This actually is a good example of some place were as you review what in fact was implemented in response to the first review team's recommendations, you can identify in this potential gap the inability to assess improvement in accuracy for records that are privacy proxy register and you could make a recommendation, for example, that some of the data be periodically audited for accuracy. I'm not suggesting that be the recommendation but just trying to suggest how this process could work, to identify gaps or potential gaps and then suggest ways to try to remediate them.

ALAN GREENBERG: Thank you, Lisa. Yes, I think that's what I was imply that it could be something that we'd identify as a gap. Not 100% clear that the policy allows to even audit that information but again, I'm not an expert on privacy proxy, I may be wrong on that one.

Anyone else with any further comments on privacy proxy? Then we'll go back to the common interface one and ask Volker, is there anything he can contribute on this even though he is unprepared?

VOLKER GREIMANN: Not anything at this stage I'm afraid. We have exchanged question but there has been little to none traffic on the mailing list. I would very much say that we're basically at the same stage that we were at last week.

We of course had the Staff prepare the planning questions, which have been forwarded to the group and there have been no comments on those, so I think we're good to go with those. Unless anybody else would like to add something at the last minute there has been tumble weeds on the list afterwards, I assume everybody's good with them.

ALAN GREENBERG: And we'll give people a moment to put their hand up if they want to raise any issues or write anything in the chat. Apparently, there is nothing. The next item on our list is anything new, Stephanie is now on the call I see. I don't know if she's prepared to speak about it. Stephanie are you with us?

STEPHANIE PERRIN: I am indeed. I'm afraid I was late getting my input in, so was Alan, I was in great company. It looks like we've got converging among the three folks who completed the pole, that would be Alan and Susan on which of the many WHOIS policies will be qualified under the anything new, that we think we should focus on.

I would say that we certainly need additional ones but we had agreed on our last call to focus on the top five. I think can move forward then focusing on the top five and start coming out with something by March 9.

ALAN GREENBERG: Alright, Susan do you have any thoughts on that? I will say that on the sub group call, we had some disagreement about what are we required

to do with the anything new items and there was some difference of opinion whether we must do an in depth dive on each of them or do we do a quick assessment and then do the ones where we believe there is something significant related to WHOIS that we need to further look at?

We decided to take an in between path of try to identify the most important ones without really commenting on the others at all and we do have convergent pretty much on which five or six to look at. Susan did you want to make any further comment?

SUSAN KAWAGUCHI: No, I'm fine.

ALAN GREENBERG: Okay. We do have the matrix up there and you can take a look at that. Essentially, we each identified which of the ones we thought were the most important ones and I thought I had ticked off three not two but maybe I'm wrong. It looks like in total we have about five, because there was pretty much convergent -- I guess we have a total of six that are identified by somebody as requiring further work on it and I guess the next step then would be for the group to try to do a somewhat more in depth assessment of what are the WHOIS implications and to what extent do we need to full team on each of these.

Clearly, we're in a position where we might almost adding 50% to the overall workload of the group if we do this and we have to consider whether we have resources to do that but I think the first step is do a quick assessment and see where we are on that. Lisa said there was

only two in my email, okay, I'll look at it again. I thought I had ticked off three but I maybe dreaming, anyone else want to comment on this, either Susan or Stephanie, now that we have that chart up or do we just go back and do some work on our own? Stephanie, please go ahead.

STEPHANIE PERRIN: There's one that I really hesitated about ticking and you know it's my favorite, and that is the procedure for handling conflict privacy law and I didn't tick it because I didn't see any support from my followers and I thought let's try and work for the ones we do support but I think it is important for this review team given that we're about to leech forward on yet another implementation review team on the WHOIS and GNSO has just approved that I believe, I can't remember whether we voted it through I think we did last meeting but I don't see a near end in sight on the GDPR compliance, we are still going to have to have some kind of an exit strategy for contract parties.

It's probably going to be really ugly. I think at some point we have to look at the procedure for the WHOIS conflict. I don't know how this is something new, it's the only policy we've got, so maybe somebody can explain why this falls under something new, that might help? Thanks.

ALAN GREENBERG: Thank you Stephanie. I've put myself in the que. My understanding of this item and maybe I'm mistaken, was it is the specific procedures that were put in place for registrars or registries to get exemptions due to privacy or other legal reasons. My understanding is with the implementation of even an interim implementation of GDPR, we are

going to be -- to some extent, some of the reasons, some of those needs for exemptions will disappear altogether because presumably we will believe that our current procedures now address GDPR.

Certainly, those procedures are not likely to be the ones that are going to go forward. Part of the GDPR implementation is going to have to be to review those procedure for registries, registrars, anywhere, not only Europe to get an exemption, so I'm working on the assumption that those procedures are not going to be the ones going forward and there's not a lot merit in us reviewing those, which is why I didn't consider that one at all eligible for our review.

I just thought we are almost surely going to have a different set of procedures going forward, regardless of what those procedures are and that's why I didn't think there were relevant to this discussion. Lisa, please go ahead.

LISA PHIFER: Thanks, Alan. I was going to suggest that possibly one way your sub group could move forward with your quick review of the top six was to divvy these six amongst the three of you and just try to identify the questions you'd want to address within the sub group for those six. You may find that you have very few questions in which case perhaps it's not important to dig into it or you may find you have a lot and that would be the starting point for addressing whether you have additional resource needs.

ALAN GREENBERG: I will point out, at least my understanding of this sub group was to do the triage, not necessarily to do any in depth work that resulted from the triage. Again, that specialized and we might not be the right people for that but I don't disagree. I think going forward that's a reasonable way forward. Erika, please go ahead.

ERIKA MANN: Thanks, Alan. I want to come back to a point you just raised, and the question whether investigation is actually helpful because concerning the way -- because in the future it might not be a relevant question any more. I do have doubts there because -- and I sent you some documents and I'm pretty sure you have seen them, concerning the future and the question how law enforcement [inaudible] will be able to access data, critical data in the future.

This question is not going to fade away, quite to the opposite, it will become more relevant because if you can't see WHOIS data or you will only be able to see certain amount of WHOIS data and all the other WHOIS data will be based on a particular request, then of course it become interesting to know how these particular requests will be able to be sent forward. This is already a complicated issue but just look forward to the future and so far, I wonder whether the [inaudible] might remain relevant and interesting in the future in a different.

It might be still interesting to see, did it work and what were the main complications in the past about it, just to understand if the procedure, the way it was established and how it worked would just be a model

maybe for future request from law enforcement or from other legitimate entities to request information about WHOIS.

ALAN GREENBERG: My understanding of that item is this is the one that will give registrar or registry a waiver to not display information. I don't think it addresses at all, how that information would be available to law enforcements should law enforcement want it. This I thought was just the procedure under which ICANN grants the waiver.

ERIKA MANN: You're absolutely right, but my question was maybe not precise enough. But I wonder if the way ICANN granted the waiver and the way evaluated the information it received based on why it considered the [inaudible] would indirectly give some indication how it could deal with law enforcement requests concerning WHOIS data in the future. It might be not the case, it's just a question which I have, so I'm not saying it is the case, I'm just raising a question.

ALAN GREENBERG: I think your question falls completely under the work we already are committed to, does the current WHOIS policies meet the needs of law enforcement? I think that's directly under it because one of the currents today, is what if law enforcement wants to get information that is now being hidden because of the waiver? I think that's squarely under the law enforcement one today without any pushing at all. Stephanie.

STEPHANIE PERRIN: I just wanted to raise a couple of issues that I've noted in a preliminary review of the proposed model. The first is that compliance with data protection law outside of the GDPR is optional, so I think that's a bit of a flaw right there because WHOIS conflicts with law is not solely for Europe and that's a bit of a problem. The model that we are about to embark on, doesn't embrace other law.

The second thing is the tiered access has been tossed over to the GAC to develop. If this tiered access system comes up with what are constituency calls all you can eat data, once you get beyond the wall, in other words, that it is not targeted and limited and if it continues to allow third party data processers to scrape all the data and reprocess it and sell it, then it would be my argument that plenty of data of registrars are going to have to make an exemption under WHOIS because the model will not be compliant with GDPR and it will take a couple of years for that to sift through the courts, get the inevitable complaints.

I don't agree that it won't be necessary. I have no idea, how we're going to reformulate this thing so that it actually works, I've said that a zillion times but something will be necessary.

ALAN GREENBERG: And I think I agreed with you, that there may well be a requirement for exemptions from policy law even if it's not GDPR, although there may well be something in that case but I don't think we're in the position to evaluate the GDPR implementation on the fly as it' going forward. I really don't think that is our job. Cathrin, please.

CATHRIN BAUER-BULST: Thank you, Alan. I think you -- It was in response to Erika's comments and I think you made a couple of my points already. I think the one thing I still wanted to say was that there was a question whether this procedure of conflict with privacy law was in any way new and I think Lisa already made the point in that chat that it is in fact new because there it recently revised and I think there's only been one case since which is the Amsterdam case, which had asked for a waiver to respect the Dutch implementation of the current European data protection directive 9546.

There's not too many cases but there have been changes and there's also of course if you want to call it a case law precedence that have developed at ICANN during the implementation of the policy so it makes a lot sense to look at it. I fully agree with Erika on the need for possibly a different procedure to deal with waivers and from what would then be actually waivers from privacy law as opposed to waivers for the benefit of privacy law, that might indeed be something that's possibly necessary in the future but I would agree beyond the scope of this review team and even beyond the scope of the law enforcement needs.

I think this brings us back to the point of which point in time we take for our evaluation which I think we're going to have to test and then stick to. If want to take the interim model into account or not here, so far, we've said that we really want to look at how things were before, if we stick to that then I think we should probably not include all those points in our review.

ALAN GREENBERG: Thank you. Any further comments? I think at this point we're committed to look at the ones we've identified, either the five top ones or the six ones and work from there and see what comes out of that in terms of what we then recommend to the rest of the review team that we do in depth or not.

I still see hands from Stephanie and Cathrin, I think they're both old. Not hearing Stephanie's voice I'll presume it is an old hand or at least no longer valid. Then next item on our agenda other anything new is law enforcement needs. Thomas had that one, he has since given his apologies. Cathrin, are you in a position to give us an update on that?

CATHRIN BAUER-BULST: I can try although I have to say I missed the last phone call that we had as group. The outcome of that as far as I understand the review that Thomas has given at the previous update on this we are also looking at briefing request to the OCTO team for the security guys at ICANN to determine whether there's anything specific law enforcement issues and what the interaction has been between them and law enforcement and in parallel it was purposed to do sort of an informal outreach to the community to identify issues on an individual basis.

I have since suggested that we might want to further prepare even for that informal outreach because one issue that I see with the previous review was that for the law enforcement needs there was little feedback actually from law enforcement and so I wanted to use all opportunities that we have to get standardized feedback that we can then compare

and put into digestible format so that we have the same questions of everyone and get comparable answers.

I haven't heard any feedback on that and in parallel I've seen on the list that we've encouraged further fleshed out the briefing questions in particular to the OCTO team to be a bit more specific so that they open to do, we've had that group call, we've had two calls actually and we now stand at the this stage and we finding the requests for the briefing and determining how exactly we wanted to move on.

ALAN GREENBERG: Thank you, Cathrin. There was one other comment on the list other than Lisa asking for fleshing of questions before we approach the OCTO team and that was from Chris, saying essentially if I can summarize that whatever extent WHOIS meets enforcement needs today, it is going to be inevitably significantly lessened with the interim implementation of GDPR and is there any real merit in doing a lot of in depth study and questioning of law enforcement today when we know it's going to change, it's going to change of the negative and maybe we're better off delaying to till May to at least them know what the world is like.

They may not have experience in it but at least then can try to assess at that point, what the impact of GDPR is going to be on the law enforcement community. That may be something we want to consider going forward. I see Erika has her hand up.

ERIKA MANN: I like to caution us a bit, this whole GDPR hype, when you look back when it was designed, it's many, many, many years ago, law enforcement understanding still poor, so when you read the document I have sent to you and they are the latest request from and I'm talking about European Union but this is true globally, from governments who have to deal with information, they have hard time to receive.

This is not just in relation to WHOIS but this is in principle and data that relates either to activities or when you read the document relates to intersected property wide information they can't receive neither as well. There's different sources which are mentioned in these papers and again, keep in mind I'm not just talking about the European Union.

Having said this, I'm pretty sure we will see very soon a change in how governments want to receive such kind of information and I'm pretty sure WHOIS will become more relevant in the near future. They will then have to decide and will have to talk about, how they want to find a way of dealing between these two conflicting legislations inside the European Union or in other countries as well. Between legitimate law enforcement and between data protection privacy.

I just want to caution us not to give up the idea that WHOIS data will remain relevant and important. A lot of data will be hidden and will not be visible to the immediate public but it will still remain relevant. I just want to caution us to be a little more prudent here.

ALAN GREENBERG: Thank you, Erika. I don't think anyone's disagreeing with that but at the same time I think this statement is correct, although may be not

understanding something that even law enforcement has the right to get something and a process to follow to get it, that still means they have to follow that process and potentially it is something that they can't get instantaneously which they can get now and therefore there are, if nothing else, timing and perhaps logging and reporting requirements that will kick in.

It's likely to change, even if GDPR is adjusted to try to balance those conflicting issues within the European Union and until we know what the process is we really don't have a handle on assessing how much law enforcement's going to be impacted or not. I see two hands but I think they're both old now at this point, Cathrin and Erika.

CATHRIN BAUER-BULST: I think what Chris has raised is the point that we have discussed on the leadership call several times, does it make sense to do this exercise now? And I fully agree that it is very challenging to make and assessment of the WHOIS as it was, given that it's going to radically change. I cannot agree more, what we're doing is part of a historical review that will perhaps not be of very much relevance any more but that brings me back to the point before, we need to pick and choose.

We either say okay, we hear ourselves as assessing the interim module with all its values and drawbacks in the hopes of informing the work of the policy development team but it's a completely different task from the one that we originally set out to do which I think we're still previously agreed to stick to, which is to look at how it worked before hand and we can maybe still draw lessons from that.

That being said of course the way the interim model is shaping up it's going to radically affect law enforcement and also on Erika's point, I think one of the major obstacles for law enforcement or any public authority will be to find the right legal basis to assess not publicly available data because that is no longer covered by existing rules such as the Budapest convention and other national implementation.

We really need a new legal basis for law enforcement beyond any model that we adopt at ICANN level for law enforcement even to be able to legally access the data from the EU and that's going to be a significant challenge.

ALAN GREENBERG: Thank you, Cathrin. In terms of where are we -- where do we stop doing the evaluation, I think with the change we did to the terms of reference, we have acknowledged that GDPR will be making some changes and we will try to assess things by the time we have our final report at least based on the interim GDPR implementation. We can't assess the policy, it isn't written yet but we did agree that would factor in the interim GDPR implementation. I think we have no choice but to do that.

As you point out, the world may need international accords on some of this and as Erika's pointed out, the European Union may have to make some changes to balance the various competing interests within Europe but again, we're not going -- I don't think we can hypothesis what's going to come out that a year from now, all we can do is work to what we have and I think we already did acknowledge that we would factor in

GDPR once we know where that is going but that's as far as I think we can go. I see Erika and Lisa.

ERIKA MANN: I think I understood you better now. I agree with you, as long as we evaluate the current status and interim status sufficiently enough, I don't think we need to go into in depth but we need to understand what is working and what is not law enforcement just to understand the threshold where it becomes so critical for law enforcement that it can't receive information sufficiently, quickly which you need to receive, so I'm talking about the super critical information, sufficiently timely or where the WHOIS data is so poor that even if they receive the information it is irrelevant because the information is just not relevant.

I think this would be good because this will be a question which will remain even in the future because even if everything will be hidden then still the information they would receive upon request would still have to be actual so that they then can actually continue working on it because otherwise if there is no accuracy then its total irrelevant. I think I am on the same page like you.

ALAN GREENBERG: I think we're already covering those under the accommodation of accuracy and law enforcement. Lisa, please go ahead.

LISA PHIFER: Thanks, Alan. In listening to this it occurred to me that some of the actions that have already identified are really planning and preparatory

actions regardless of whether needs to be assessed are law enforcement with WHOIS as it is today or law enforcement with WHOIS as it may be modified through GDPR compliance.

The briefing with OCTO for example to learn about their interaction with law enforcement and potentially gather contacts there to conduct some kind of outreach that's broader, that can probably happen immediately without answering the question which needs are you assessing.

Structuring the questions that you want to ask during outreach as Catherin has suggested also could be done regardless of the timing of the outreach, so I guess I would encourage the sub group to move ahead with those preparatory steps as you think about whether you want to ask law enforcement whether their needs are met with a current system or with a potentially modified system.

ALAN GREENBERG: Thank you, Lisa. Any further comments on the law enforcement item? Cathrin, please go ahead.

CATHRIN BAUER-BULST: We have already shared a list questions, I reviewed the ones from 2012 report and also shared the ones that I have previously asked of European law enforcement in the context of our work on the WHOIS issue. The questions are under discussion and indeed if we can build on those before we do the outreach then we would have more comparable input later on. I think we're on a good path.

ALAN GREENBERG: Stephanie.

STEPHANIE PERRIN: I'm just wondering what are the chances of getting actual hard data from law enforcement and I would have thought that subsequent to the publication of expect working group report they might have engaged in some of this hard data collection and analysis but precisely what do they need from WHOIS? What can they do using anonymized data? What are time gaps that are usually relevant? What is the ultimate purpose of the access to the data? Is it a prosecution? Is it scatting? Is it analytic? What is it? Have we got data on how often the access the system and what for? Because if we have I certainly haven't seen it.

Maybe in the public safety working group but until we know precisely what they need we can't figure out how to respond to their needs because hit or two has just been keep the WHOIS wide open for it and even if we were to do that on an interim basis, regardless of any conflict with law, in other words allow them to access without a legal instrument inside the tiered access system, we still need that data so that we can come up with a final, more complete model. That's a question in case you missed it. Thanks.

ALAN GREENBERG: Thank you very much. It's interesting, at this point they were already living in a world, law enforcement, where data is masked because privacy proxy data is not available to them globally without any process. What we're really doing, going forward with implementation of a GDPR

type of modified WHOIS practice is, we're simply changing the subset of data that is hidden verses the subset that is not hidden.

I don't think the world is completely unknown, how it's going to affect them and how it important it will be, is something we have yet to determine and that will partly based on how much data is hidden and how much is not. I don't think the overall environment is changed, other than where the balance is. Stephanie, I think that's an old hand and we have Catherin next.

STEPHANIE PERRIN: Just as a follow up, it is an enduring question that I have, why we do not have more hysteria about the inaccessibility of the privacy proxy data among the cybercrime spiders, now the answer that I have heard is that they get access to the zone files and that solves their problem. Is it possible that the law enforcement community? If not, then why is not more hysteria?

ALAN GREENBERG: I can't answer why there's not more hysteria, I can hypothesis that they're pragmatic people and they know that we're not going to make privacy proxy services disappear and they have to accept that. It's interesting that for talking to people, even the fact that you are using a specific privacy proxy service is indicative of something. Cathrin, please go ahead.

CATHRIN BAUER-BULST: Just to say also in response to Stephanie valid remarks about needing to know what data is used for which purposes, I think there is now some very good use cases that the public safety working group with the [inaudible] law enforcements put together for this [inaudible] attack force exercise last summer that some of us participated in to create a list of use cases and there was also work done on the use cases in the context of RDS PDP and indeed in the context of the first WHOIS review team which includes what law enforcement uses for which type of investigation.

Some of that is not publicly available because it tells a lot about investigative techniques but I think we have enough evidence to be able to make the case for certain purposes and to be able to assess the necessity and proportionality as it relates to specific data elements.

I think that's a key one and in terms of privacy proxy, indeed my impression has been from interacting with law enforcement that in many cases they just take what they're given and they try to work with whatever they can assess and they're just made by the fact that they can frequently not access information that would be useful for investigations and then those investigations that die a silent death and that's how it goes, in the balance of things we're going to have to accept.

Indeed, I agree with Alan that frequently law enforcement takes a pragmatic approaches, that being said a lot of agencies are very actively involved in the work of the implementation team as Volker will be able to tell you, represented by one of the delegates from the public safety working for the GAC and there are some quite serious concerns about

the workability of privacy proxy polices in particular when comes cross boarder access.

I think indeed your normal law enforcement officer will often not even be able to tell the difference between a ccTLD policy and a gTLD but there's the ones that are more into the subject to provide significant amounts of input to the public safety working group.

ALAN GREENBERG: Thank you, Catherin. Any further comments? And seeing no action we will go on to the next item on the agenda and that is consumer trust. Erika.

ERIKA MANN: Let me be brief. Two things, we had a call last week and during the call we had different topics which came up which were considered for review. Within the sub group we asked colleagues to review particular items.

First of all, I must apologize that I couldn't deliver on the vote, was supposed to have access in the evening to internet but it just didn't work. I just came back today, this morning actually. We received one comment from the Dmitry which actually very interesting and Alan replied to it. This was a debate we had last week and it's an interesting debate because it goes beyond probably our sub group and it relates to the question, how we can actually define trust.

An old question when you review the old WHOIS data and in publications it always comes back around to the question that how trust

can be defined for consumers. Dmitry, his points to the -- I want to mention them today because they are interesting because he came back to the conclusion he divided the consumers into different categories, which I think he's right, common users, registrant, professionals and law enforcement people and then we looked into the different ways how is trust is defined, how trust can be kept in different environments.

I don't want to go into the details, just want to indicate you what we are working on. Other than put forward and came back with a more radical, questions based on what Dmitry put forward and probably is most -- Alan, your most radical point was to say when you consider that under various privacy legislations data will become less available, how much should we and future review teams focus on the issue?

I'm just giving you a quick overview where we are. Dmitry scheduled a new call and I think Susan, I think we still have to send back some requests to the points which you identified as we would cover them. This is where we are right now.

ALAN GREENBERG: Thank you, Erika. I put my hand up because I wanted to very briefly present where I went with my statement. We know that the number of people who use WHOIS data to establish whether trust someone or not is moderately small.

The number of users who will consult WHOIS data, the number of users who are not also registrants who consult WHOIS data I suspect is very, very small. To what extent that really gives a level of confidence of who

they're dealing, which is what I think consumer means in this case, is pretty small.

I think we would have a hard case, we ICANN or registrars that say we want to collect contact information and information about who the registrant is for the purposes of consumer trust, I think we'd have a hard time making that case before privacy commissioners. In which case implies that consumer trust benefits from WHOIS are answerer, they're an accident of the implementation and they may provide some good but if they are that low key, is it really a relevant topic to be discussed and what I'm really saying is were the words consumer trust tossed into the affirmation of commitments regarding WHOIS is an interesting thought but are we in a position perhaps by the time we finish this study to conclude that studies of consumer trust with WHOIS information are minimal at best and probably worth removing from the bylaws are something we shouldn't be looking at in the future because it's just not a significant reason why WHOIS is there and it think that's something we can't answer right now but I think as we do the work on consumer trust, we should be looking at with an eye to asking ourselves, do we want to continue and have the next review team also look at consumer trust or was it an interesting idea whose time has passed? I see we have at least one hand up, Erika please.

ERIKA MANN: It's an interesting question you raised. I'm not so sure because I think when we look back we have to assume that WHOIS is still in early days. Let's imagine continue like it is right now and there would be no change because of privacy laws and it would just continue, probably it would

become more relevant over time first of all because there would be more data, there would be more comparable data and more players then they use it now.

The second point I think I would want to make is that the second category I find most interesting Dmitry identified, actually the third one and this market professional, registries, resellers, lawyers, domainers, when you look into their debate about WHOIS and they have separate channels where they debate this topic, it's actually a super relevant one for them and they use it quite frequently, I can't say how frequently they use, one would have to talk to them and how relevant it is for them really, it's just my assumption based on the debate I see but my understanding is its super relevant for them.

I think your question crucial Alan and we should keep it in mind because if will identify there is no need actually for the connection or the connection between consumer trust and WHOIS is not relevant then it will have serious implication. I still assume it is relevant but this is only based on the few points I just made.

Carlton by the way is making a comment in the chart room, I don't know if you have seen it. He is saying in relation to Dmitry's categorization, the only one I see that has a direct veering on trust and WHOIS data is law enforcement and maybe IP forces. Now, his last point into the IP, I think he's absolutely right, law enforcement we already debated so I'm not going into detail IP people they need this information and so I would assume consumer trust remains probably a relevant topic but we will take your point into consideration definitely Alan.

ALAN GREENBERG: Thank you. One of the things I think the group has to do and we're not going to do it today, is decide whether for instance domainers and registrars are consumers? In the context of how this term was used originally. I suspect now. We do have several people with their hands up, we have 10 minutes left in the call and we really do need to get on to looking at a few of the other things, specifically the face to face meeting and the plenary call.

Unless someone has something absolutely compelling they have to say, I would ask people if they could put their hand down but if there is anyone who has to say something please keep if very short because we do have to continue before the end of the call. Stephanie, please go ahead.

STEPHANIE PERRIN: I consider it really compelling when you and I agree whole heartedly on a point. I just wanted to say I totally endorse what you said about consumer trust. I think one of the problems under the GDPR is the ability for individuals to take a case and consumer trust is not best satisfied but access to WHOIS these days. We need much better security measures then WHOIS can possibly provide. I just like to put that on the record. Thanks.

ALAN GREENBERG: Thank you very much. It's an interesting topic and one that's certainly I and other people will have a lot of fun with. Next item is the sub group report template and I assume that's Lisa.

LISA PHIFER: We just wanted to note to you that on the sub groups page you can find the template that was put out for reports from each of the sub groups. The template just briefly to tell you includes an introduction of the topic, a summary of the relevant research materials, that includes what you're reading, briefing received and inputs that you may have received during meetings and of course the big section of the sub group report is your analysis of findings, reporting your findings and your analysis of those.

There are then sections for identifying the problems, the potential problems that you see, that maybe gaps in implementation of the first review team's recommendation implementation or it may be other items for the other sub groups but an identification of the problems that you see. Then of course, formulation of the new recommendations that you wish to put forward to the full review team.

As you begin your work here, aiming for our Brussels' meeting, you may wish to start fleshing out some of these sections, for example the summary of the relevant research you could probably begin building from the materials you've already identified and have discussed how you'll either divvy up or all review that work. If you need any help in actually transcribing anything into the template to begin your document, Staff is available to help you with that.

ALAN GREENBERG: Thank you very much. Any further comments on that item? Seeing nothing, the next item is the plenary call schedule. I'll note that schedule for calls between the ICANN and our face to face I believe we decided our fixed and that we would have calls on the 23rd, 2nd and the 6th of April and we are now looking at the schedule going forward for can we adjust to try to head better attendance. I'll point out today's attendance was pretty good. I'll turn it over to I presume Jean-Baptiste or Alice, I don't know who?

JEAN-BAPTISTE DEROULEZ: I can tell you that, thank you, Alan.. Just a quick reminder that last week I shared with all of you an email individually [inaudible] your time zone and asking you to confirm your availability during a given week so that we can look at what would be a better time for all of you. So the names consisted on a slide, just a reminder as your name appears [inaudible] to return to me the excel sheet filled with your availability. Thank you.

ALAN GREENBERG: Thank you very much. I note you seem to be scheduling calls that are all scheduled in weekdays in pretty much all time zones, so it ends pretty early on Friday to accommodate those who are ahead of UTC. I'll note for in my case anyway, I attend, I have a lot of calls and not all of them are fully under my control and I'm not sure I know when all the calls are going to be over the next six months and I suspect I'm not the only one with that situation.

All we can do at this point is do our best and hope that the world doesn't change too much around us. Let's move forward on this, it's the best we

can do and hopefully we'll come up with a schedule where we can try to get better attendance on a regular basis.

JEAN-BAPTISTE DEROULEZ: I just wanted to reply to a comment on the slide that all the different times where provided, and in fact this was a reply to a suggestion from Stephanie in the last plenary call about the fact that she could be taking calls much earlier during the day, so this is just to have an overview of when everyone is available to see whether that could help or not.

ALAN GREENBERG: Understood. The next one is face to face meeting before ICANN 62, and I would prefer to differ that discussion till a time when Chris is on the line unless someone feels there's some decision we have to make immediately. My recollection is we have until sometime in April or May to make a request, is that correct? I'm guessing it is.

JEAN-BAPTISTE DEROULEZ: That's [inaudible] so I believe so, yeah.

ALAN GREENBERG: Okay. Lastly, we have confirmation of decisions reached and action items out of this meeting.

JEAN-BAPTISTE DEROULEZ: Thank you, Alan. On decisions reached, Alan mentioned there will be plenary calls on March 23rd, 2nd and 6th of April. Under action items, for

sub groups the first one privacy services sub group we have Susan to review the list of questions of Alan's comments [inaudible] that he shared with the sub group. On anything new, the sub group will have to which policy procedures will be addressed and which [inaudible] to do so. Consider the need to review the procedure of defining conflict and assess the need to review each of the items [inaudible] in depth.

The law enforcement sub group will finalize the briefing questions for OCTO and questions to be covered during informal outreach to law enforcement. Consumer trust sub group will consider the core discussion about the definition of consumer trust within the sub group.

All sub groups [inaudible] deadline for the sub group report is 5th of April and will need to be submitted at that date so that others have enough time to prepare for the Brussels' face to face meeting on 16, 17 and 18 of April, and if you need any help on that you can reach out to the ICANN Org support team. On ICANN 62 face to face meeting, this has been reported to the next plenary call.

ALAN GREENBERG: Thank you very much. I did not hear any other items on any other business, I had no requests and I'll give people one last moment. We have the compliance sub group meeting in one hour from now and the strategic priority group meets at 12 UTC tomorrow and I believe those are the only meetings we have scheduled prior to the ICANN meeting. With that, I'll call this call to an end and Lisa said data accuracy meets at 11 UTC, on which day? Tuesday. Why is that not on my calendar. Not that I really want to meet them.

BRENDA BREWER: The invite was just sent at the start of this meeting.

ALAN GREENBERG: Oh okay, that would explain. Thank you very much for participating in this call. I think it's been a really good call, attendance has been great and we'll look forward to seeing you all either in the sub groups at the ICANN meeting if you are there, or on our next call after the ICANN meeting. Thank you, all. Bye-bye.

[END OF TRANSCRIPTION]