ICANN Transcription

GNSO Temp Spec gTLD RD EPDP – Phase 2

Thursday 01, August 2019 at 1400 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at: https://icann.zoom.us/recording/play/WHmldryIIwfZ4Zi8L3ZhdUpelsnSw77p2NXlsW3J-5d3PgnC5cdOfXyLrluK2Rj5

Zoom Recording: https://icann.zoom.us/recording/play/G-iO2Fzv6Wmp66NX9feo_A_dc9-tmvt9gI_LI6WzYQzwzjUKk1QlUoK8u2kUEDFO?startTime=1564668012000

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

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

TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the GNSO EPDP Phase 2 Team meeting taking place on the 1st of August 2019 at 14:00 UTC.

In the interest of time, there will be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourself now?

Hearing no one, we have listed apologies from Greg Aaron of SSAC, Marc Anderson of RySG, Matt Serlin of RrSG, Thomas Rickert of ISPCP, and Alan Woods of RySG. They have formally

assigned Tara Whalen, Beth Bacon, Sarah Wyld, Sean Baseri as their alternate for this call and in the remaining days of absence.

Alternates not replacing a member are required to rename their line by adding 3 Zs to the beginning of their names and adding at the end in parenthesis their affiliation-alternate, which means you are automatically pushed to the end of the queue. To rename in Zoom, hover over your name and click Rename. Alternates are not allowed to engage in chat apart from private chat or use any other Zoom room functionalities such as raising hands, agreeing or disagreeing. As a reminder, the alternate assignment form must be formalized by the ways of Google link. The link is available in all meeting invites towards the bottom.

Statements of Interest must be kept up to date. If anyone has any updates, please raise your hand now or speak up. Seeing or hearing no one, all documentation and information can be found in the EPDP wiki space.

Please remember to state your name before speaking. Recordings will be circulated on the mailing list and posted on the public wiki space shortly after the end of the call.

With this, I'd like to thank everyone for joining and turning it back over to our Chair, Janis Karklins. Please begin.

JANIS KARKLINS: Thank you, Terri. Hello everyone. Welcome to the 11th meeting of the second phase of the EPDP. The agenda of the meeting had been circulated. So far no comments have been received. As you noted, the leadership took into account those few comments that

had been made after the previous call suggesting that question of accreditation may be postponed slightly. Therefore, we're suggesting that we would do the first reading of two cases. The one we started yesterday on investigation of criminal activity where domain names are used and to take another one from group 4, which according to the poll came up as the most typical one from that particular group.

So, with this explanation, would team be willing to work according to proposed agenda? I see no objections. We will then do so. Thank you. Let us move to agenda item 3, early inputs review.

The last time – after the deadline which was suggested for groups to raise any comments or objections or questions in relation to submission of other groups, no submission have been received at that point and I suggested that we would instruct staff to use proposed material for their analytical work in preparation of the zero draft of the policy recommendations. So after that, there were few comments on the mailing list saying that silence not necessarily means agreement and therefore I would like now to ask a very simple question, when are groups will be ready to discuss early inputs that have been submitted upon request? And then when could we examine those early input submissions? Anyone has a proposal?

I see no one. Those who objected and requested the discussion, would you want to come forward? In absence of any request for the floor on my question, let me then suggest that answer to that question should be posted online on the mailing list.

So, the question is, when will groups be ready to discuss early inputs that have been received from different groups? At the suggested deadline, no comments have been received. Then when I suggested that the early inputs then would be taken into account in our future work and we would not discuss them any further, then objections have been raised and said that we have to discuss them. Now, my question is, when we will do that? Any proposals?

I see now Ashley followed by Marika. Ashley, please go ahead.

ASHLEY HEINEMAN: Yes. Thanks, and I apologize. I'm not raising my hand to answer your question necessarily, but I did just want to note that despite how late this is, the GAC will be sending in its early inputs today. I apologize that this is coming so late, we have some snag. It's getting the clearance and this timing and I don't expect this to be any heavy load or addition to the people's workload. It's a very short submission, so just wanted to flag that's coming your way and I apologize sincerely. Thanks.

JANIS KARKLINS: Thank you, Ashley. Marika.

MARIKA KONINGS: Yes. Thanks, Janis. This is Marika. I just wanted to make sure as well that – because I saw that there was some comments to the action item on the list that the way the staff interpreted that action item was not that we would just follow the input without any kind of

consideration of what was provided but more that staff would review it and the drafting of possible recommendations for further consideration and flag those areas where maybe there were opposite views or points were raised that might require further conversation. So, at least from the staff perspective, we didn't take that as instructions that we would just follow whatever was provided but more that we would take that input into account when drafting the initial report recommendations and noting where input might require further conversation. But of course, I think as we've indicated previously there's our preference that the group looks at that and maybe specifically indicate where there's agreement or where there are certain areas of disagreement that may require further discussion.

JANIS KARKLINS: Thank you, Marika. I was trying to say exactly the same that you would use those inputs in your work drafting the zero proposal. And then of course if there are conflicting inputs, that would be brought to attention of the team as a whole. There is a question from Farzaneh, what is the GNSO process for considering early inputs? Could you answer that, Marika?

MARIKA KONINGS: Yes, thanks, Janis. I also responded in the chat but there is an expectation that early input is reviewed and addressed by the working group. And I'm just putting the link in here as well and for that purpose, staff has developed – and it's not only specific for the EPDP but it's also a tool that's used for other PDP Working Groups and we also used it in Phase 1. They were calling that the

input review tool. So staff has already taken all the input that was received and kind of organized and categorized it in a way that we hope will facilitate the consideration by the group.

The format that that template uses – but again the group can of course decide to do it differently – that the group would kind of document how it considered the input provided and whether it agreed with it, it disagreed with it, or what kind of action it took based on that input. And other efforts we usually then post those results as well, that those that have provided inputs are able to review how the group addressed it. I think as we mentioned previously as well, of course we're in a bit more but unique situation that in this context I think all those that have provided input are also active in this effort, so the group may need to balance how much time to spend on reviewing the early inputs versus that input also being raised and flagged by the groups that have provided that input through the course of deliberation. So, that is something you may want to weigh and consider.

JANIS KARKLINS: Thank you, Marika. Actually, because of this factor, the proposal was that if any group finds something unacceptable in submissions of other groups then they would flag that and then we would then consider that particular divergence of use. And so far, no contributions have been received from any of groups on the sort of input.

Now I have few more requests. I see Margie, James, and Mark Sv. In the meantime, Milton suggested to discuss it next week.

MARGIE MILAM: Hi. My question is, is there a way to incorporate in the worksheet the points from the groups, so that as we go through the issues, we can look at the input from the various groups? To me that seems like a reasonable place to have the conversation of what was raised in these input documents and that way it's a little more structured of an approach.

JANIS KARKLINS: I think it is possible but there is also a separate document created where all inputs have been compiled together for ease of reference and comparison. James, please.

JAMES BLADEL: Hi. Thanks, Janis. I've been collaborating a little bit with my registrar colleagues and we're just trying to confirm that we know that we submitted our early input prior to Marrakech in June 21 and that we also have some comments collated and submitted in the Google Doc by Sarah on July 26. So, we're just trying to get everything situated here and make sure that we've got all of our homework turned in. And maybe this is a question for Marika. Are we submitting comments on the right document here, or are we supposed to be sending them somewhere else, to a list? I want to make sure that our work is being recorded. Thanks.

JANIS KARKLINS: Yeah, James, my apologies. I did not mention that your group indeed submitted comments on early inputs. My apologies. Mark Sv, please.

MARK SVANCAREK: I'm not entirely clear on what the purpose of this exercise is, sorry for being dense. So, all these early input and comments on it will be put into one document I guess and then what will happen to that document, what is the purpose of that document? How would it advance our work? Could you clarify that? Thanks.

JANIS KARKLINS: Thank you, Mark. I think that is a charter requirement or [inaudible] requirement. Let me take Alan before going to Marika for final answers. Alan Greenberg, please.

ALAN GREENBERG: Yeah, thank you. Clearly there's not an awful lot of interest in doing this and given that the early input really ask the questions of how do we address Phase 2 and how do we address all the issues in Phase 2? I would suggest at this point that we defer addressing the early input as such and factor it in as we come to section by section. Because otherwise, we're doing Phase 2 in brief, and then doing Phase 2. Thank you.

JANIS KARKLINS: Thank you, Alan. Marika?

MARIKA KONINGS: Yes, thanks, Janis. This is Marika. I just wanted to confirm again that indeed there are two separate activities that staff undertook in response to the earlier conversation. One was to incorporate the input into the SSAD worksheet, and that has already been done and I posted the link in the chat and the ideas. People are able to review that in the context of the discussions on the different topics and then separately we created at the request of the group the Google Doc with the objectives for groups to be able to either provide clarifying questions, comments or reactions to some of the input provided. And as you know, to date only the Registrar Stakeholder Group has provided input there.

In response to Alan's suggestion, I do want to note that if you look at the input provided, there are two different aspects to the inputs, some of it is responding to the charter questions or providing substantive input on what should be considered in the context of responding to the charter questions. But there's also input that has been provided on potential additional questions that should be asked or potential rephrasing or reconsideration of a certain charter question.

So, again, I've noted that some of the substance may be considered in the context of the deliberations but the group may also want to review whether any of the input in relation to the charter questions. Additional question is something that should be addressed, for example, in the worksheet by adding further questions or objectives to some of the topics.

JANIS KARKLINS: Thank you, Marika, for this clarification. So I understand that this is a requirement that we have to do. As Alan said, there's big interest in that, that this is our obligation.

Let me propose the following. Please review the compilation that have been posted on Google Doc and then we would devote some time for discussion of inputs received on the compilation of early inputs, maybe not next call but the call after, on the 15th of August. That would give us little bit more time and possibility to still provide input and also read early input from the GAC that will be circulated, as I understand, later today. Would that be okay?

I see no objections, so then we can proceed to the next agenda item on the use case categorization. If I may ask staff to introduce the topic. Will that be Marika?

MARIKA KONINGS: Yes. Thank you, Janis. Terri, if you maybe let me screen share, I'll pull up the document that I sent out early on this week. Just one second. You should all be able to see this now.

Basically, this represents the results of the survey that we sent out last week and just to refresh everyone's memory, we discussed at last week's meeting the categorization of use cases that was proposed by a small team of volunteers and in attempt to group together use cases of similar nature or at least the expectation was that responses to the questions in the pamphlet might be similar of nature, and as a result it might not be necessary to go through all the use cases in detail but it might be possible to derive some common conclusions from those use cases that are

deemed similar and as such. And the objective of the survey was to identify for each of the groups the use case that were of being the most representative and as such that one would then be used as a starting point for the deliberation. But as I said, that does not mean that the other use cases in that same category would not be considered but we probably would approach them from a perspective of trying to identify what in those additional use cases is of such a different nature that we'll need to further consider, assuming that some aspects of the use case might be the same and as such would not need to be further discussed.

So, we have six groups responding to the survey: NCSG, Registry Stakeholder Group, ISPCP, SSAC, and the Registrars Stakeholder Group. And as I said, you can review those results and some of them were pretty close and as you may have seen as well in the proposed schedule of discussing the use cases. In certain cases, the leadership team and staff have made a suggestion on how to approach the order especially where it's very close to call, where either the same score was achieved or very close score was achieved. We've made a suggestion there as for which one to take first.

For example, for this weeks' meeting, we had of course already one group, two identified and I think that use case is actually also confirmed them in the survey as the number one in that group. I've done for the group for the first reading there actually two that were really, really close and the other one was the SSAC case. But as we knew that some of the SSAC members were not present today, that's suggested to the leadership team that it may be we're starting with the ALAC 1 for our first reading today.

So, what you see here in the schedule is also the proposed deadline that then are associated with that discussion and that flows from the earlier conversation we had in relation to the approach for dealing with the use cases. Again, the first reading is an opportunity to kind of walk through the use case, by the author of the use case, or respond to any questions for groups to already be able to express any kind of concerns or suggestions they may have. But then the ask of everyone is that by the next day, so by Friday of that week, those added concerns, proposals are submitted in writing to the list which then will allow the use case authors with staff support as needed to then distribute an updated use case prior to the next meeting in which a second and hopefully or possibly final reading of that use case would take place. So, that is it's more or less the sequencing we're proposing and you can see here the order that we suggested based on the survey results.

We would go for next week's meeting, hopefully finalize the second and final reading of the SSAC use case and continue the first reading of the ALAC cases. And you see we have a little bit of course of a mix on today's call and then basically move on to group five first reading. This is also one where I think we had an equal score of two use cases here. I think the IP5 and NPC 6 had exactly the same score. Here the suggestion is to go with the use case that has also – that was also flagged in Phase 1 of the EPDP team's work as an issue that requires further conversation. I think in this case, this worth pointing out I think that use case was submitted by I think the IPC but if I recall correctly, I think it's pretty barebone so here is probably an action item for the IPC to further fill that out in due time to make sure that groups can review

prior to that meeting and we can have a fulsome discussion about it.

Basically, that's the sequencing. It continues until late in August where we hope to at least make it through and finalize the leading use case for each category and then we'll get to a point where the group will need to start considering what other use cases in each category need to be further reviewed. And we'll probably need to see in due time whether that's in the form of a survey or conversations where groups can indicate – and again we can look in the ranking that has been provided and basically start with the next use case and basically ask the question, is it substantially different that it requires a full scale review or are there certain aspects that should be considered as you know they might result in a different approach and result in different recommendations for the group to consider?

Then towards the end of August, early September, the leadership team together with staff support we hope to be able then to be able to share with you draft policy principles and draft recommendations that we hope to derive from these discussions, especially the commonalities in some of the cases as well as of course the different topics that we've identified which will form the basis of the discussions for the face-to-face meeting. And then of course, as part of that conversation, the group will need to consider as well how to deal with any remaining use cases which still need to be considered because you know they may result in significantly different recommendations or policy principles or that's the group that believe that through the review that it's hopefully completed by that time, the different aspects have been

covered and that provide sufficient basis for moving to the next topics on the list. That's in a nutshell what we've put forward. I'm happy to take any questions and I'll get it back to Janis.

JANIS KARKLINS: Yeah. Thank you, Marika, for this very detailed explanation. The floor is open for questions. I see Ben Butler. Please go ahead.

BEN BUTLER: Alright. Thanks, Janis and Marika, for the walkthrough. I just wanted to raise as it relates to the SSAC case on the agenda for today specifically like the phishing examples. Greg Aaron is unavailable this week and we had asked whether there would be an appetite to postpone this walkthrough until next week, simply because while I'm perfectly willing and capable of walking through it, to some degree Greg has real-world examples as third party phishing investigations that may make it worthwhile to postpone. Well, I think I believe he brought it up last week but I'm not sure that that was maybe an area of confusion because of the point about SSAC 2 for next week. So, I guess I'd like to get a pulse from the room whether we should continue to read through the SSAC 3 today or could this be postponed until next week?

JANIS KARKLINS: Thank you, Ben. I think we already discussed that and the purpose of today's reading is to raise concerns and not necessarily to answer them, and that will give also possibility to Greg to review those concerns and be well prepared for the second reading during next week's call when he will be available.

And since this conversation is recorded, he will be able to follow that part of conversation after the meeting just to get the flavor of comments from the team members.

I recognize Sarah Wyld, followed by Alan.

SARAH WYLD: Thank you. This is Sarah Wyld from the Registrar Team. Just I guess a procedural suggestion in terms of how we are working through these use cases. One thing that our team found as we worked through the LEA 1 case that we sent an e-mail about I think yesterday, it's a little bit difficult to go back and forth in an e-mail thread. Maybe we could take a lesson from the IRT and have their proceeding and use Google Docs similar to what we did in the early input responses where we could all put comments and then interact in the comments and maybe suggest the changes instead of e-mailing back and forth with each different use case. Thank you.

JANIS KARKLINS: Thank you, Sarah. Indeed the idea is that everyone expressed their concerns and then those are put in updated version, and then after the second reading, the authors are again fine tuning the text of the case in order to get everyone's concerns reflected in the document itself. That's the idea of this method that we're having the first reading where concerns are raised then those concerns are submitted in writing for the benefit of authors of the case. They are taken into account in the second updated version,

and then we're looking already updated version for the second reading.

Alan Greenberg, please.

ALAN GREENBERG: Thank you very much. I have some concerns about the ALAC case that we're going to be presenting today and that I'm not sure how good a use it is of our time. We presented as a valid use case and we strongly believe it is, but the use case made it clear that this was effectively an edge type case in that we can't imagine how one could be have the request to be credentialed. It's going to be one that is going to have to be handled based on the actual merits. This is one where the balancing test is going to have to be done really carefully because WHOIS is not open to anyone who simply says, "I would like to see it and here is my valid reason." You're going to have to make a good case to the controller why this information should be released to an individual who is otherwise unknown to the community. So, although it is a use case and we can spend a lot of time going over the details, I'm not sure how valuable it's going to be in what we learn from it. So, it's on the agenda and we'll do it if that's the decision, but I'm not sure it's really good use of our time. Thank you.

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

MILTON MUELLER: Yes. It's Milton Mueller, Georgia Tech. Both of the previous interventions kind of raised some questions in my mind about how we're treating these use cases. Being with the idea that we cannot discuss SSAC 3 because a particular member of SSAC is not here, disturbs me. Maybe it shows a misconception as to what these use cases are. So, people are not advocating a given use case as something that's always right.

What we're trying to do is saying there are people who have particular uses in mind in which they would request to disclose information and we will go through all of the possible elements of that request, including legal basis and so on and work out what it really entails. I don't understand why we cannot continue to discuss the use of these request for essentially domain name abuse activity that might involve phishing or other kinds of abuse. It should be a generic case. Anybody in SSAC should be fully capable of representing and explaining what is needed if it is indeed a generic security issue, and every absent SSAC member is supposed to have an alternate to fill in for them, so I'm not sure exactly what is going here.

A similar reaction to Alan's comments, again whether or not this is a problematic case that it would involve a manual balancing test for random individuals, that's precisely what it makes it worth discussing, that we would figure out as part of this use case what would be required and what kinds of constraints or enabling activities we would want to do. So, I'm not sure why Alan is proposing to sort of pull back from that particular use case when it does in fact pose some very interesting issues and maybe that we decline to recognize this as a legitimate use case. It's a perfectly

viable outcome of any use case that people have and proposed. But that's exactly why we're discussing it in this stage. So, I would move ahead according to our agenda on both of these use cases.

JANIS KARKLINS: Thank you, Milton. Yeah, I think that our initial conversation when we agreed to categorize those use cases was that they would represent a lot of similarities, but then the difference is would be taken on board once we would go through few cases per group and then the reading of the other cases would be quick because they would focus exclusively on differences rather than commonalities with the previous cases in the same group.

Therefore, we need to start with something in each group and then go through. And I personally found the group for case interesting are also from the point of view of accreditation, so that will give us at least on that particular topic something that we would not have or ideas that we would not have in the case of law enforcement or the case of SSAC. So, in absence of other request for the floor, so I would like to suggest that we accept staff proposal and we will follow what we have now on the screen. Of course, with understanding that if we would not be able to read the case or go through the case as planned, we would review the timeline and would allocate sufficient time for the review.

That said, I expect that every team member or group would do the homework and would put in writing their concerns, because without that we would spend maybe our time inefficiently in the call. So, I would really encourage all groups to take this homework seriously. And if preferences to work on the Google Doc, no issue

with that. We can provide that opportunity for any comments or concerns that you may have on each individual case. So, may I take that this would be acceptable moving forward?

Thank you. Maybe then we can go to the SSAC case and continue our conversation where we ended last time. The last time Greg presented the case and then some members already expressed their concerns and that we did not exhaust the list of speakers during that meeting. If I recall, it was Margie who's in line and then I think – sorry, I don't remember the second one.

The purpose of this reading is again to go through quickly. We're still on the bullet B on different tasks. So, I open the floor for any comments, concerns that team members would like to express on sub point B. Who is ready to start? Milton, please go ahead.

MILTON MUELLER: If you remember last week, we had started to enter into the issue of the multiple possibilities here regarding what information is necessary. If our specific case here is phishing and most phishing cases, the non-law enforcement parties are primarily concerned with flagging who does phishing domain, taking it down, or blocking it in order to disable the criminal activity, they are may or may not be interested in most cases in attribution. Of course, they cannot be prosecuting them. They would have to relay that to law enforcement.

So, I think the issue here is, do we need to break this down into those specific cases which the actual disclosure of non-public information is necessary because again, for a lot of the phishing

and anti-phishing activity, it's not. It just isn't. There's all kinds of things that the anti-phishing groups use such as the date of registration or the similarity which is automatically detected to certain common names and they use this information to block domains to mitigate phishing. So, I would wonder if we could strip this down the number of tasks here. If you could scroll up a bit. I'm looking at 4, 5, and 6.

Thank you. I see 3 now – truthfulness of contact data. What additional domains maybe related? For example, IP address is not non-public data. So, you could do matching of nameservers, registrars, and many kinds of information about the domain without necessarily disclosing any non-public information. I'll stop there.

JANIS KARKLINS: Thank you. Thank you, Milton. Next is Margie.

MARGIE MILAM: Hi. The thing that I think is really important with regard to phishing both on the criminal side and the civil side is the attribution aspect because the WHOIS data, the actual contact information is a unique field that is often repeated by the bad actors when they register multiple domain names. What we're trying to accomplish in this kind of a use case is not simply play whack-a-mole, which is to take it down at the ISP level but to actually identify the network of operators, of domain names that could potentially be operated by the same entity. And that's why the attribution is particularly important. So, I disagree with the perspective that

contact information is not necessary. It is in fact very necessary to ensure that you're trying to capture the entire gamut of domain names that are potentially at play in the phishing event.

JANIS KARKLINS: Thank you, Margie. James? James Bladel.

JAMES BLADEL: Hi, thanks, Janis. And thanks, everyone. If we could scroll down just a little bit further, I think it's Task 3. I just wanted to react to some of the language put forward here regarding accuracy and I want to emphasize first of all that accuracy of contact data is always desirable and something that we should aspire to achieve to the highest level as practical.

I just want to note here, falsified domain registration is a sign of bad faith and constitute fraud. I don't know, I'm not comfortable with that language that implies that there's a criminal intent when there could be errors or other types of things that may not be a sign of bad faith.

And accuracy checks, particularly when you introduce cross field validation, we found that that the level of false positives goes way up and we start flagging things as inaccurate you know upwards of 10% false positives inside the U.S. and Europe and much, much higher levels outside of that. So, I just I take objection I think to the way that Task 3 is framing the concept of data accuracy as inaccurate data implies criminal intent, number one, and that introducing the very problematic approach of cross-field validation

would solve it when in fact it only exacerbate those errors. So, I just wanted to get that on the table. Thank you.

JANIS KARKLINS: Thank you, James. Next is Alex Deacon followed by Mark.

ALEX DEACON: Thanks, Janis. I just wanted to make a comment on Milton's intervention from earlier. It seemed if we are discussing a generic SSAC use case, which I think has been suggested we do versus a specific phishing one, then the tasks outlined here by SSAC like how they've done that I think do a good job of describing what happens in the real world investigation and a lot of those tasks also happen for other non-SSAC use cases. And that it includes – again in the generic use case – the need for disclosure of RDS data. So I just want to make sure that we understand or maybe agree on exactly what is the scope of these use cases, how generic are they, how specific are they, and I think that will indicate the need for disclosure in many cases. Thanks.

JANIS KARKLINS: Thank you, Alex. I think that we are not maybe writing ideal use cases here but we're using use case methods to clarify our own understanding of different aspects that may be useful in formulation of policy recommendations. So that's how I see this conversation and that a case is just a tool. Mark Sv please.

MARK SVANCAREK: Thanks. I think Janis said and Alex had already covered my point more or less which is that we do have this challenge that if the use cases are very, very specific, we'll have too many of them and then people will want to combine them. Then if we want to combine them then people will say they are not specific enough and they will want to create nuances. Definitely it's a real challenge that we face. It may be appropriate while we go through the use cases to mention sometimes this is not true or sometimes this is very true or this is almost always true, something like that to clarify the various permutations of these use cases. But if you see this as an exercise, as a discussion mechanism or just basically a tool that is not based on the use case has to be perfect in every regard or perfectly specific, then I think we can move forward.

So I wouldn't suggest making these much more specific or breaking them down into more use cases at this time. It's appropriate for Milton to intervene and say, "Hey, there are some examples where there's variations on this." I think that's perfectly in line with using this as a tool but specifically breaking this into more use cases I think we've already talked about that and rejected that idea because then you have the proliferation of use cases. Thanks.

JANIS KARKLINS: Thank you, Mark. Milton followed by Brian. Milton, please.

MILTON MUELLER: Again, I'm not arguing for the proliferation of use cases necessarily. I'm arguing for careful discrimination between activities or uses that require disclosure and those that do not.

So, let's just go down the list here. Task 4. Suspending the domain that is problematic does not require any disclosure. In fact, it happens constantly without any such disclosure based on various kinds of automated algorithms.

If I may tell you that in my classes, I have students do a phishing exercise and they're frequently surprised to learn how quickly their proposed domains are recognized as phishing domains and blocked before they can even get their assignment finished. No WHOIS disclosure is necessarily required to do that.

The same with Task 2. The IP address is going to be public and the WHOIS records we don't need disclosure for that.

Task 5 I think is an interesting borderline case in which you would need disclosure, but one could argue that maybe that's the point in which you turn it over to law enforcement and let them do it. Or you could argue that we do want private actors to be able to uncover identity. So, let's have that discussion.

Task 3, assessing the accuracy and truthfulness of contact data, I agree very strongly with GoDaddy comment about that that this is a completely different use case. It's about assessing the accuracy and it's not really part of mitigation of phishing or various kinds of domain abuse. It is a logical step away from that. You're doing various forms of assessment on the accuracy of the registration information which could result in all kinds of false positives.

So I think what I'd like to see happen here is for these tasks to be winnowed down to those that actually require disclosure. I'm not proposing that the ones we throw out become new use cases, I'm just saying let's pare this one down so that it actually is use case for disclosure.

JANIS KARKLINS: Okay. Thank you, Milton. Brian?

BRIAN KING: Sure. Thanks. I think I would remind everybody of a couple of points that are necessary and GDPR doesn't mean absolutely you can't do it without the disclosure but necessary means reasonably necessary. When we talk about phishing attacks, Mark Monitor's phishing anti-fraud service measures our success rates in how quickly we get things taken down in minutes and hours. I think that informs what necessary means in this case and that needs to happen quickly. So that informs how important it is to get the disclosure. If there's something else you might be able to do but it's going to take you a week or a couple of days, phishing attacks happen, the damage is done in the first hour or two hours and certainly by 48 hours, the phishing attack is generally over with. So, I would note that.

Then the other point I wanted to make was on Task 3. I think we might be able to pare the language just a bit and get this to a point where folks can agree on it. What we're really looking at here is the falsified domain registration data, so I think James made a good point that just because the data is inaccurate doesn't mean

necessarily there's fraud afoot. But for falsified domain registration data, it is a sign of bad faith and probably constitutes fraud. So inaccurate doesn't necessarily mean falsified, but when it is falsified, that typically does indicate fraud. Thanks.

JANIS KARKLINS: Thanks, Brian. Mark Sv followed by Chris.

MARK SVANCAREK: I'm going to take my hand down. I think all these points have been in-depth already. So, thanks.

JANIS KARKLINS: Thanks. Chris Lewis-Evans?

CHRIS LEWIS-EVANS: Thanks, Janis. I just want to cover something really that Milton said which is right but I think on some of the items that don't require disclosure, there is some process and activity that may take place with the data that has been gained by disclosure mechanism.

As we're looking at Task 4 I think it was, it doesn't require any disclosure of any data, it may use some of the data that has been disclosed to you in a previous task to aid you with that processing. So I think it's very important that we have the tasks split here as Alex has said. I think it's a good way of showing how any disclosed data may be used.

I think obviously for Task 6 as well, you don't require disclosure to report to law enforcement but if you've already got data that has been disclosed to you then you are going to pass that on. So I think how the data is handled once it has been disclosed by the party that is carrying out the process is obviously a very important part of GDPR and the way that this use case has been laid out allows us to see what process and activity takes place and where the data can be handled throughout all that process and activity. If we were just looking at where the data needs to be disclosed then I'd agree with Milton. But I think the extra bits in here showing where the data may be processed had already been disclosed by the third party I think is an important part to keep. Thank you.

JANIS KARKLINS: Thank you, Chris. Margie followed by Stephanie.

MARGIE MILAM: Thank you. A couple of points on the way phishing attacks are addressed. I deal with this quite regularly in my job. It's true that sometimes they're picked up by phishing services and addressed quickly. It depends upon the registrar, the registrar's willingness to cooperate. So you can see a situation where the registrar doesn't take something down or put it on hold yet the domain name is still able to be used for phishing. So what typically can happen in that scenario is you use any tool possible to try to get that taken down. One of them is the false WHOIS complaint. That's an active tool that we turn to when we are unable to take down a domain name that's used for phishing through the registrar.

So I just wanted to flag that. The accuracy element is relevant for that and we need to keep in mind that there's many ways that phishing attacks are mitigated and we don't want to stop the security community from being able to use those tools effectively to protect end users.

The other point I wanted to raise was I don't see why we need to be so specific in the use cases, in other words, ask for further revisions or deletions. I thought this was a tool, really, to help inform our policy recommendations. So one of the things I would like to see and as a better understanding of what we're going to do with the use cases, because obviously there's areas where some of us may disagree on some of the wording or some of the principles there, but really the question is what are we going to do with these and how does it trickle up to policy recommendations? Because what I don't want to do is perhaps waste time in rewriting these when they're not even going to be part of the final report or part of the policy recommendations. As I understand, these are simply tools for helping informing our discussion.

JANIS KARKLINS: Thank you, Margie. Let me maybe tell you how I see it. Of course we're not tasked to write the use cases. So this conversation provides better material for better understanding of issues for all of us. And certainly staff is capturing every grain that falls out of this conversation and puts down those grains in order that will be presented in September as a zero draft for policy recommendations. I think that those use cases will be attached ultimately as a reference document to the report that we will produce but not beyond that. So they need to be reasonably

accurate that people understand also the correlation between what we're proposing as policy recommendations and where that policy recommendations come from. That's how I see what will happen with the use cases at the end of the exercise.

Let me turn now to Stephanie. Stephanie, please go ahead.

STEPHANIE PERRIN: Thank you very much. I did type a few remarks in chat a while ago but I guess I had I better say them in order that they get on the record and someone possibly listens.

Point number one, while this is a useful case as a discussion instrument, I'm going to request that we do what I requested we do during the RDS discussions and make a footnote, noting that this is purely discussion instrument because the amplitude of the use case makes it very worrisome. There's an awful lot of things bundled in here.

Okay. Number two, on the accuracy issue, if inaccurate data alone were an indication of malicious or criminal intent then we should take down the credit reporting agencies because they're running at 60% accuracy. We don't do that so we shouldn't consider doing it on the WHOIS because there's plenty of inaccurate data in there that is not fraudulent. It is just plain inaccurate data. Same thing applies to government. The inaccuracy rates in government records for social services and western democracies aren't terrific.

Okay, the third point. This business of having the data preemptively – and I'm referring to Chris's latest intervention – it is convenient if you're the private sector third party that has no

delegation by law enforcement to do this work, so no delegation under law to be collecting personal information. If you are going to prosecute, then fine – this is what I typed into the chat – go get the personal information then. It's not as if in the takedown procedure you have obliterated all of the data and you can't get it, right?

I think that the allusion of these two things disturbs me. You can't have the third party collecting personal data so that the police can prosecute on their behalf. I'm well aware that it happens. I am well aware that at least in western democracies, the telecoms' authorities are collecting more data perhaps than they should and are then handing it on. But that doesn't make it correct and it puts ICANN as this trusted multistakeholder organization in a very awkward position to be doing this. It's one of the major flaws in the delegation of the disclosure instrument to ICANN in my view.

I'm referring it back to the letter from Jacob Kohnstamm back in about 2012 in which he points this out. That was when he was Chair of the Article 29 Working Group and he was commenting on the new Registration Agreement. Thanks.

JANIS KARKLINS: Okay. Thank you, Stephanie, for your input. Let me suggest that we leave Subsection B for the moment and go to subsection C. Any comments on Subsection C? Subsection D? Milton, please.

MILTON MUELLER: Just on C. You went a bit quick for me. There's a mention of tech contact name. I thought we were getting rid of that or that we considered the registrar abuse contact where the registrar itself to

be the tech contact. Am I mistaken? Or if I'm not mistaken then that would be an unnecessary part of this use case.

JANIS KARKLINS: Okay. Thank you for your comment. Margie?

MARGIE MILAM: Hi. I disagree entirely with what Milton just said. Our Phase 1 report includes tech contact. And one of the main points of tech contact is to deal with things like phishing. So, that to me is just a completely contrary view to what the Phase 1 report says.

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

ALAN GREENBERG: Thank you. I do believe we omitted in Phase 1 the paper mailing address for tech contact however. But the name and e-mail and phone, I believe, are still there.

JANIS KARKLINS: Thank you, Alan. Sarah Wyld?

SARAH WYLD: Yes, thank you. For Section C, I would like to confirm that the specific data elements to be requested which would be disclosed would be minimized and specific for the request at hand. So if

they're not relevant, they would not be requested and should not be disclosed. Thank you.

JANIS KARKLINS: Thank you. Ben Butler?

BEN BUTLER: Yes, just to respond to Sarah's question. That is correct. If it's not necessary for the specific type of investigation that's happening, they wouldn't be requested. Because this is kind of a broad, general purpose, type of abuse investigation, though largely using phishing as the example we just included. Basically, I think it was [said in chat]. If it is of interest and relevant to the specific investigation then it would be requested, otherwise, no.

JANIS KARKLINS: Thank you, Ben. So let us move to D. There is comment from Farzaneh or question from Farzaneh. Chris, please. Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Thanks, Janis. I've had a few issues with the number of different lawful bases for the parties here. The vital interest is a very difficult lawful basis. Basically, the process is vital to protect someone's life. There is very, very few instances where you'll get that before you don't hit one or the other lawful bases. I would suggest that one is probably unrealistic and certainly for phishing. I really don't see there's been an appropriate case.

Then also the public task, we're not talking about the request to being a public authority, so therefore, F or M or C may be better. So certainly getting rid of those two as an initial is a minimum on our [inaudible] have a little bit look at a couple of the others as well but certainly those two straight away, we need to do that. Thank you.

JANIS KARKLINS: Thank you, Chris. I think that Subsection D should be read together with the Subsection E that provides additional information on each of the list of lawful basis.

I recognize James next in line. James Bladel, please go ahead?

JAMES BLADEL: Thank you. I think I'm probably echoing Chris and some of the chat I think, some of the comments in the chat. Subsection D looks like a shotgun approach to defining a legal basis and I think that it needs to be narrowed down to those that are more specific and applicable because otherwise, I think it actually increases rather than decreases the vulnerability that this would be challenged or questioned. Thanks.

JANIS KARKLINS: Thank you, James. Farzaneh?

FARZANEH BADII: Thank you. I'm wondering how 6(1)(b) applies to this use case because I don't see an explanation in Section E for supporting

information. And also if you're invoking 6(1)(f), you have to provide justification for the balance and carry out the balancing test. I have been saying that for a long time. Because 6(1)(b), if I'm correct, is when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into contract. So, I don't understand how that applies. I don't think that in this use case, there are sufficient reasons to invoke 6(1)(f). At least they have not been provided. Thank you.

JANIS KARKLINS: Thank you, Farzaneh. Ben, I will ask Mark first and then you will answer our questions. Mark, please. Mark Sv.

MARK SVANCAREK: It may be of interest to look at use case BC-1 for a little bit more detail on the Section D. For instance, in BC-1, we talked about the cases where the investigator actually has some sort of relationship with the data subject, for example, people who use Microsoft online services may have opted into certain levels of protection or that may even be a contractual requirement as terms of use. So an edge case, it wouldn't apply in most cases but it is certainly possible that it would.

In BC-1, we also discussed D and it was our conclusion that it would seldom be justified to use D, and so in BC-1 we did not include it, but you can envisage those rare cases where human trafficking or something like that is involved. So whether or not that rises to the occasion of including it here in this use case, this is a

good conversation on that. Just pointing out that in BC-1, we elected not to include it. Thanks.

JANIS KARKLINS: Thank you, Mark. Now, Ben.

BEN BUTLER: Thanks. I do want to just start off by saying we recognize that as written D and E do look like a shotgun approach – and that's not the intention – we were trying to capture that there are edge cases that we could go through where potentially any of the 6(1) basis would be the one that most applies. But those are going to be edge cases we fully recognize that in the overwhelming majority of these cases 6(1)(f) is probably the most applicable.

As Mark said, 6(1)(b) performance of a contract would potentially take place when a data subject has contracted with say a reputation service provider or phishing provider to make sure that their contact information isn't being used in reporting a phishing attack. So we recognize they're edge cases, they're the minority, but 6(1)(f) and the requisite balancing test that would need to be performed is probably the most common one. If we want to just focus on that, we can. We just wanted to point out in the use case there are situations where the other ones might be a better fit.

JANIS KARKLINS: Thank you, Ben. I would like now to propose to continue with the Sections F and G, but recognize Margie and Milton. Margie?

MARGIE MILAM: Thank you, Janis. One of the things I put in the chat was that I thought when we first started talking about the use cases that when we got to this section, we were recognizing that legal advice was to be sought from Bird & Bird on the legal basis and that this was essentially a placeholder until we receive that legal advice. So I just think some of this discussion is premature, so we get that advice from Bird & Bird. Thank you.

JANIS KARKLINS: Thank you, Margie. Milton?

MILTON MUELLER: I think that it's very clear what we need to do here, which is indeed to delete everything but 6(1)(f). I think the point is not that there might not be edge cases in which different legal basis might be used. The point is that those are in fact different use cases. For example, to use the Mark Sv's case in which you have a contractual relationship, that would be easily covered under the use case which revolves around 6(1)(b) which does involve a contractual relationship. So that would be covered clearly by another use case. I think that Chris pointed out that in things that really do involve public safety or some kind of law enforcement role. Those are already covered by the law enforcement cases. And private parties cannot be pretending like they have the authority to be acting in the same way and under the same legal basis as designated law enforcement authorities. So I think it's pretty clear what we have to do here.

JANIS KARKLINS: Thank you. I think that this conversation provided a lot of food for thought for a second and for Greg to review these Subsections D and E, and bring up the new version for the next reading.

In light of time, we have 5:15 now Europe Time. We have 45 minutes remaining and we still need to get to the end of this and start the next case. So I would suggest go to sub point F on safeguard applicable to requestor. Subsection F – any comments? I see not immediate comments.

Subsection G. Brian?

BRIAN KING: Just a quick note – thanks – on F. We should be careful with code of conduct. I can't see the footnote there. That's a term of art that could potentially be problematic if we wait for it. I mentioned this before. Yeah, right. It's distinct from that but it's also distinct I think from GDPR. The wording that we're looking for there is probably a data processing agreement that includes all the safeguards that the processor will take or the new controller the requestor will take when processing the data. So we probably want to update that away from the specific code of conduct term of art to something like data processing agreement. Thanks.

JANIS KARKLINS: Thank you, Brian. I don't see further requests on Subsection G, safeguards applicable to entity disclosing a nonpublic registration data. Any comments on this?

I see none on Subsection H, safeguards applicable to data subject. I see no request for I, safeguards applicable to system itself. Sarah?

SARAH WYLD: Thank you. Sorry, still in Section H. Just curious about that last sentence, "The registrar data subject must have the responsibility to respond to notices," I believe that is already part of the Registrar Accreditation Agreement, this is already a required thing. I'm just curious as to why it needs to be included here as well. Thank you.

JANIS KARKLINS: Okay. Thank you for your question. Not need to immediately answer but if you want, please quickly, Ben.

BEN BUTLER: Yeah. I believe what Greg was trying to phrase here is that under the Temp Spec, the WHOIS inaccuracy process has largely fallen down or not been able to continue to be utilized and that we're just advocating that there needs to be some way for that to continue to have without responding to notices of inaccurate data.

JANIS KARKLINS: Okay, Sarah?

SARAH WYLD: Thank you. Yes, as I said in the chat, perhaps I misunderstood what Ben just said. The WHOIS inaccuracy program continues to run as required. We send out annual WHOIS data reminder notices. We send out WHOIS verification requirements. We suspend domain names when they do not complete their verification. And I think in Phase 1 we determined that requirements related to accuracy don't need to change. We already have accuracy requirements in place. So, maybe I misunderstood you. Thank you.

JANIS KARKLINS: Okay. Let's leave this conversation for the next time, that there may be some additional clarification could be provided over in the text.

Let me propose to go to Subsection I. Subsection I – any comments? I see none. There is one from Sarah. Sarah, please.

SARAH WYLD: Somebody's requirements here – reverse search, wildcard search – those are not currently part of the functionality that we offer and I would like to be very careful before we start bringing those in, so I think I just like to flag that for a lot of consideration before it becomes part of the requirements.

JANIS KARKLINS: Okay. Thank you. James Bladel?

JAMES BLADEL: Hi. Thanks. I just want to echo that these additional capabilities and functions were never part of the previous RDS system. They were offered by third party data harvesting firms and should not be on the table for our future discussions. Wildcarding and reverse lookups and that stuff starts to get really, really close to this idea of tracking and surveillance, and I don't think that's the intent of what we're trying to build a system to do. We're trying to build a system to provide some accountability not to follow folks around the DNS. Thank you.

JANIS KARKLINS: Thank you. Alex?

ALEX DEACON: Thanks. On that part, I agree, James, which is why I suggested in the past that functionality that hasn't existed in the past and it may not exist in the future just be deleted as a safeguard, it doesn't make sense in my point of view to include these non-requirements, if you will. We could cook up an unlimited amount of non-requirements here. I think it would be best for clarity to just remove them. Thanks.

JANIS KARKLINS: Okay. Thank you. So, SSAC is listening and taking good notes on all the proposals that we have. I see no further requests on Subsection I. Ben?

BEN BUTLER: Your point is well made. We're taking notes on this. Item one for I, we're not asking for that as a policy recommendation. We're simply pointing out that if there was a legal way to do that under GDPR, that type of capability would be useful. But we're not trying to skin that particular cat at this point. We're happy to remove point one.

JANIS KARKLINS: Thank you for clarification, Ben. Subsection J. Mark Sv?

MARK SVANCAREK: Hi. I was generally agreeing with the conversation here that we should be careful of mentioning non-requirements or things that are not functionally available. But I do want to be careful about what James is saying about things being illegal or unethical. Certainly if someone were to go to a data controller and provide their information to the data controller, and the data controller were to perform the balancing test and say, "Yes, I am able to look for all the instances of this particular e-mail address," that's not a general thing. That's not people just trolling through the registration data on an ongoing basis but that would be a very, very targeted thing that might happen inside. And that would be subject to 6(1)(f) –

JANIS KARKLINS: Sorry, Mark. We did not hear you awfully well. You're faded.

MARK SVANCAREK: I was just trying to say that –

JANIS KARKLINS: Now it's very good.

MARK SVANCAREK: Okay. Sorry. I just want to make sure that we're not making blanket statements about certain things being illegal or unethical. I think it's not productive to this conversation. Certainly if you look at BC-2, you can see an example where wildcard search would be perfectly legal. A targeted wildcard search within a single data controller could be perfectly ethical and legal. So let's not make blanket statements about that. It's probably not great, not healthy.

JANIS KARKLINS: Okay.

MARK SVANCAREK: Farzaneh, the example would be [inaudible] to look at. It would be [inaudible]. We found a case of the domain name, those being they're able to use. We went to the reseller that had provided that domain name and they agreed based on our evidence to look for other instances of someone using that same e-mail address. And we discovered that that person had used their same information and doesn't [inaudible] registration as part of the same infrastructure. [Inaudible].

JANIS KARKLINS: Mark, we do not hear you again.

MARK SVANCAREK: Okay, sorry.

JANIS KARKLINS: So, will you continue? Okay, Stephanie.

STEPHANIE PERRIN: Thanks. I just wanted to – at the risk of being tedious – really raise the point that there is language all the way through here about accreditation and authentication of users. Accreditation and authentication of users identifies who the requestor of the data is. It does not and cannot automatically mean that the request is a trusted "don't have to check it" request. So I think there is an assumption here that accredited users will have routine access to the kinds of data that they routinely look for but that's an unwarranted assumption that Sarah has just put into the chat. You still have to validate the actual request. Thanks.

Oh, and one point that I didn't bring up previously and I do apologize for bringing up later, I did want to respond to Mark Monitor's [inaudible] as a justification for getting speedy access and therefore also the personal data. That's not really a calculation that you make their business model and how speedily they can respond to customer needs when you're balancing the fundamental rights of the user. Unfortunately, ICANN has such a bad history in balancing the fundamental rights of the user that we do tend to forget that that's what this exercise is about. Thanks.

JANIS KARKLINS: Thank you, Stephanie. I think all of us agreed about five or six meetings ago that the accreditation does not necessarily mean access to or disclosure of information. So this is not first time that trickles up so that's [obvious].

Let me quickly go to James and Brian that we can continue. James?

JAMES BLADEL: Thanks, Janis. I note that Ben from SSAC said that they would probably be striking the bit about wildcards and reverse search and things like that. So, I'll be brief. And, Mark, if your heartburn is around the use of the words "probably unethical" or "probably illegal" then I can walk that back, if that helps. But I think that it is worth pointing out that those are open to abuse particularly because it creates a new role for this SSAD system which is that it now tracks registrant behavior across TLDs and across registrars. So, for example, if I had an account and multiple registrars registering domain names and multiple TLDs, that sort of visibility across the entire ecosystem is not something that currently exists that would suddenly become available if this use case were endorsed or if those features were added. I think we need to be very careful about adding that and putting ICANN or whoever operates this system in that position.

So, I don't disagree that we could probably line up a million and one anecdotes were having access to those facilities would be useful in tracking down cybercrime. However, they're just way too

open I think, vulnerable to abuse and used for non-stated purposes. But I note that SSAC is saying they're going to strike them. I'll hold that conversation until we get to BC use cases. Thanks.

JANIS KARKLINS: Thank you, James. Brian, quickly please.

BRIAN KING: Sure. Thanks. Just to address Stephanie's point, it's not Mark Monitor's business model that I'm talking about. What I'm referring to is how phishing attacks need to be addressed regardless of who's doing it. It needs to happen quickly and the fact that things need to happen quickly is a factor that contributes to the decision about whether the disclosure or the access is necessary in a given case. There's a number of factors that go into other disclosures necessary and that's going to be one of them. I think that addresses all the points. Thanks.

JANIS KARKLINS: Thank you. On J – accreditation. If I may ask SSAC, Ben, so [you're right] that some users who can be accredited. If that would be possible for the next iteration that you also provide your idea or your vision, how that could be done by whom, what would be the process very briefly, that we also engage a little bit in the discussion on these topics in more detail than just in general accreditation could happen. Ben, please.

BEN BUTLER: I'm happy to take that. We can certainly flesh that out a little bit. I will point out that Anti-Phishing Working Group has already submitted during the [8/1] public comment at some point that there's a proposal to potentially credit members of the Anti-Phishing Working Group and right now requisite data protection agreements and that sort of thing. We're just saying that some of those user groups if possible for accreditation to happen and APWG is just one that has already been exposed.

JANIS KARKLINS: Okay. Thank you. Any other comments on J? Milton?

MILTON MUELLER: Yeah. I just want to flag that I think we have very different concepts of accreditation and what it is here. In my understanding of accreditation, there would not be an accreditation for the Anti-Phishing Working Group. There would be an accreditation process which essentially was designed to hold any party or any group accountable for misuse of the information and there would be no special recognition given to particular groups. They would simply be a generic accreditation. This is not something we need to get into now. Obviously, it's in the future but I just want to flag that that we do have different notions of accreditation at play here.

JANIS KARKLINS: Thank you. That's interesting to know how different cases or in different cases the segregation could be organized.

I would like now to see whether on M, N, O, and P would be any comments at this stage. I see no immediate request for the floor. So let me then suggest those who spoke and feel strongly about issues they raised, please do the homework. There will be a document posted that you could provide your inputs in writing ideally by Friday, end of business, in the worst case by Sunday, 8 of the day wherever you are, that on Monday, staff and penholders could start looking at those comments and review the case and bring it to the attention of the group already by Tuesday that we are well prepared for the next reading on coming Thursday.

With this, I would like to draw the conclusion of reading this case and move to the next one. That will be online buyers' identification and validation of the source or services. I will invite authors of this. I understand that would be Alan, if I'm not mistaken. Alan?

ALAN GREENBERG: Yes. Thank you.

JANIS KARKLINS: If you could walk us through quickly to the case and then we will open for initial reaction and comments.

ALAN GREENBERG: Yes. Thank you. I'll do a brief introduction and turn it over to Hadia to walk you through the actual phase. As noted at the top of this one, because we however made a tentative decision, still to be discussed in Phase 2 to not distinguish between legal persons

and natural persons, this use case is something that we might have put into a real edge case because they were not many potential uses and it became something which we think is much more relevant. So the legal natural issue will come up again within Phase 2 and that may alter this use case if and when it does, and if and when we make decision.

Clearly, this is a use case that successful use of this use case is going to depend on the requestor being able to justify why this is a special case and in fact requires confidential information to be revealed. It's not something which we believe is likely to be done by ticking off a box because the controller will not likely have any knowledge of who the requestor is, nor the details of the specific case which makes this one different. Nevertheless, since we cannot presume that there will never be such a good case and many of us know that there are instances where this seems to be a desirable ability, this we believe this is a valid use case that needs to be looked at. I'll turn it over to Hadia to do a section-by-section review. Thank you.

JANIS KARKLINS: Thank you, Alan. Hadia?

HADIA ELMINIAWI: Thank you, Alan. First, I would like to confirm that consumer protection is within ICANN's mission and the European Data Protection Board has noted this and its letter to ICANN on July 5, 2019 where they said the European Data Protection Board has taken note of ICANN's Bylaws which require ICANN in carrying

out its mandate, and in particular as part of its review process to assess the effectiveness of the current gTLD registry directory service and whether it's implementation meets the legitimate needs of law enforcement promoting consumer trust and safeguarding registrant data and to quickly address issues of a competition, consumer protection, security, stability and resiliency.

Second, I would like also to note the importance of this to consumers and a policy paper by the Organization for Economic Cooperation and Development states that easy identification of online business is a key element for building consumer trust in the electronic marketplace. And I would like to note here that this is a benefit not only to the consumers but also to the commercial website owners where it is necessary for them to have the consumer's trust in order to be able to prosper on the Internet.

Starting with the case, what we're looking for here is for online buyers or Internet users that are trying to purchase services or goods from the Internet to be able to verify the legitimacy of the website that they are dealing with. Again, I agree to [write] that we are talking about commercial websites like websites selling goods and services. So we are basically talking about legal persons. Again, typically those kind of websites would have their information available online publicly. But what if it is not there and the user wants to access the website or purchase the service and wants to validate the website? So why is nonpublic registration data necessary?

Again, as I said, GDPR expects information of legal persons to be readily available. So if for any reason this information is not available and the user wants to make sure that the website is a

legitimate one and wants to look at the information, then that's the reason. The data elements that would be required, those are typically contact information.

The lawful basis for this would be 6(1)(f) and (e) supporting info to determine local basis for the requestor. Recital 47 says, "The processing of personal data strictly necessary for the purposes of preventing fraud also constitute a legitimate interest of the data controller concerned."

So, preventing fraud is a legitimate interest. People supporting info. So people selling goods or services online typically have the contact information available. Again, the purpose is to prevent fraud. The necessity, again if you're using 6(1)(f), there needs to be a necessity, and the necessity here, the user should demonstrate clearly that this information is not publicly available and that he/she are not able to opt payment.

Then the balancing test here, this is an easy one actually because we are talking about commercial websites. Disclosure of contact information of commercial domain names is reasonably expected by the registrant and has minimal privacy impact. So I will say this is one of the cases where if you can actually verify that this is a commercial website then you can verify the identity of the requestor, then the balancing here is quite an easy one. Then again, I would refer to Recital 47 where it says, "At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."

Indefinitely, commercial websites do expect their data to be available publicly. And for that, maybe we shall need some detailed privacy notes like the controller or processor would need to have detailed privacy notes in this regard.

Safeguards applicable to the requestor. So the requestor needs to identify that the required information belongs to a commercial domain name. It's to prove that the contact information is not available through other means and to agree to use the data for the legitimate and lawful purposes described above.

Safeguards applicable to the entity must only supply the data requested by the requestor. That's obvious. Must return current data. That's obvious as well.

The safeguards are all those given to the data subject under the GDPR. I would like here to refer also to the public benefit. This also would be part of the balancing test because there's wider public benefit here. And for sure, yes. There is a wider public benefit. Providing a mechanism through which ordinary users would confirm the legitimacy of a website is a benefit to both the consumers and the commercial website owners, where in case the site is a legitimate one against the trust of the users. If it's not, then the user could report the site before he/she are actual victims. I think it's really important to have a mechanism or a path through which actually users could confirm or maybe be able to report a website before actually they are victims and that definitely saves other users as well.

Accreditation – we don't see that accreditation of users would be possible because of course we are not looking for one user that

will continuously be looking up websites. Definitely there is no need for accreditation here. Authentication definitely yes.

What information is required to be provided of course of the website. The requestor, a contact information. Why this data is being requested, for example, the user would say that he's trying or she's trying to purchase that thing from the website or they got an e-mail from this website, promoting this. Then they decide, for example, accessing the website to make a purchase or something. They will need also to approve that they cannot find any kind. They cannot contact the website owners and they would also need to state why they think that this actually put a non-legitimate website, for example, you might have booked an online ticket from a website, not a known one. Then again this is also a bit for consumer protection by the way. I mean this is good for competition. This is good for competition because right now you know you would only go to those big, well-established websites, well-known names in order to make sure that you are not going to be a victim of any kind of fraud. So if you're booking an online ticket or a hotel, you would go to those really well-known websites. But what about small websites that are trying to make their way through? Sometimes you don't use them because you just don't trust them. And maybe they are trustworthy.

For example, if you're buying an online ticket from a website that's not known to you and after they have confirmed, for example, and you haven't paid yet or maybe paid but they haven't withdrawn the money yet and then you receive an e-mail saying, "To confirm your reservation, we need your ID as well." Ordinary users might say, "Well, maybe for chasing an online ticket, maybe the ID is

required as well?' Of course, it's not. But then you could be suspicious. So if you received such an e-mail and then you want to confirm you've already booked your ticket and you want to confirm, is this a [legitimate] website or not.

JANIS KARKLINS: Hadia, if I may ask you to get to the end of the introduction.

HADIA ELMINIAWI: Yes. I'm almost done. That's about it. That's the case. The expected time of response – instant acknowledgment of the request.

Is automation possible? We don't think that it would be possible. However, that's yet to be explored.

The requirement to expected timing of substantive response. The requirement to validate request will likely result in relatively poor response timing. Okay. But, yeah, as soon as possible.

Then the retention period is until the verification is complete.

So, I'm done here and I'm happy to answer questions. Thank you.

ALAN GREENBERG: Have we lost Janis?

JANIS KARKLINS: Oh, sorry. I muted myself. Thank you, Hadia, for the presentation. In view of time, I would take a few comments and maybe a

general nature, and then we will revisit the case during the next call. I have Milton, Mark, and James in line in that order. Milton, please go ahead.

MILTON MUELLER: Yes, sir. This is Milton Mueller at Georgia Tech. I think the key issue here which to me suggest that this is a case that probably should be discarded is the distinction between ex post and ex ante checking. What Hadia is saying is that she is curious about who's behind the website. She's thinking of buying something from it but she can't find any information about it.

This in itself is not a crime unless the website is in a jurisdiction that requires that information to be posted. And as a consumer, you have every right and it's probably quite reasonable for you to refuse to do business with the site that lacks the forms of information and data you think you need to be assured of the validity of the service. So the consumer has an option. Nobody is inherently defrauded by this lack of information. [Inaudible].

Now if you're talking about ex post, you have been defrauded by a website. Then that is indeed I think is a legitimate grounds for disclosure and that would fall under other use cases regarding fraud by non-state actors or by law enforcement authorities. So I don't think we need this case. There are in fact many jurisdictions in which commercial websites do have to post this information and we haven't even resolved the issue fully as to legal versus non-natural persons in terms of what will be the status of their WHOIS records. Finished.

JANIS KARKLINS: Thank you, Milton. Mark Sv.

MARK SVANCAREK: Okay. I'm going to try and talk. Can everyone hear me? How's my microphone?

JANIS KARKLINS: Not really. But please try.

MARK SVANCAREK: Okay. Well, how about now?

JANIS KARKLINS: Please go ahead.

MARK SVANCAREK: Okay. Fine. Just a clarifying question for Hadia. I think you anticipate that the user makes a typical 6(1)(f) request and then the data controller will look at it. If the data controller has a legal, natural distinction ability, they would say, "Hey, this is not even protected and they would just share it." But what if they don't? If they don't do that, how would they perform the balancing test? Thanks.

JANIS KARKLINS: Thank you, Mark. James?

JAMES BLADEL: Hi. Thanks. Very quickly, I think there's a fundamental flaw in this use case which is that it conflates the registrant of a domain name would be operator of the website. And maybe that was true 10 or 15 years ago, but that is certainly not an iron clad relationship particularly in the instance of websites that function as marketplaces where individual buyers and sellers come together. I mean example is PayPal knowing whether or not someone is on eBay doesn't necessarily tell me whether or not I can trust the seller just because they are on eBay. There are numerous examples like that.

Also just a couple of thoughts here. This strikes me as an overlap with an industry tool which is currently in use which is the Extended Verification SSL Certificate which does verify the operator of the website as well as provide the trust that the transaction will be secured and encrypted and that the integrity of the operator is at least known. We – GoDaddy and then the rest of the industry – have been trying to encourage folks that if you don't see an SSL site lock on a website, you probably should not consider it a trustworthy website for commercial activities. I'm concerned that holding up WHOIS data is some sort of alternative check would undermine those efforts to promote the use and adoption and recognition of SSL as a way to enforce trust.

And then on the backend – I think this is what Milton is going for – if someone is actually defrauded as part of a commercial transaction then the registrant information of the domain name might be useful but I think that falls under a different use case, it probably starts to look more like it would come through under an

LEA request. So I had a hard time figuring out where to fit this one and I think if you start to tug on the thread that registrant is not website operator then the justification for this use case kind of evaporates. Thank you.

JANIS KARKLINS: Thank you, James, for raising these points. Stephanie?

STEPHANIE PERRIN: Thanks very much. James has raised a couple of the points that I wanted to make. I really do think that it's time as he pointed out to move on the conflation of the domain name provider and the operator of whatever business is on there is a big problem nowadays. Consumers should not be encouraged to rely on the WHOIS generally to get data. Quite frankly, whether you choose to regulate as a government or whether you choose to not regulate, you at least owe your citizens the consumer education that they should not be giving their money to people that they cannot trace. That's the responsibility of what I call above the waterline. It should be on the website. If we can't tell who you're dealing with from the website then don't deal with them. It's a weak association as James is pointing out in the chat. So that's a pretty clear point.

I appreciate Hadia's background on the thinking behind this but much of the thinking is related to what I call above the waterline. It has to do with the web presence, which is none of ICANN's business. We cannot get into the trustworthiness of what appears on a website. It is not within the remit. Thanks.

JANIS KARKLINS: Thank you, Stephanie. Taking into account the time which is four minutes before the end of the meeting, I would not give the floor now for answers to ALAC folks. Rather, please keep your arguments for the next time. The case will be also published on Google Docs, and those who are wishing to put comments in will be able to do so immediately after the call though it's not necessary for next call because we will continue first reading during the next Thursday's call.

So, if you really do not insist to speak now then please take your hands down. If you insist, please keep your hands up. I see hands are still up. So then I will ask Hadia and Alan to speak.

HADIA ELMINIAWI: Thank you, Janis. I'm sorry for that. I'll be really quick. I won't be replying to everything, but just to James point. I would like to note – yeah, I was just picking it up. The Federal Trade Commission issued a statement on WHOIS in which it said, "The WHOIS database is critical to the agency's consumer protection laws, to other law enforcement agencies around the world, and to consumers." Also they said that WHOIS databases often are one of the first tool FTC investigators use to identify wrongdoers.

Quickly, to Milton's point. What he's saying actually does not serve a competition well. And again, SSL you cannot always depend on them – you cannot always trust a website that has SSL. That's quick responses. I have other responses as well, but

being conscious of time, I give the floor to whoever is next. Thank you.

JANIS KARKLINS: Thank you, Hadia. Alan?

ALAN GREENBERG: Thank you very much. I'll be very brief. The intent of this was not to be speculative of we're curious about who this is but when there is a valid case and egregious case that needs to be followed up. And if that means that the introductory sections need to be clarified to say that then fine. But just to be clear, this is not meant as purely speculative "I'm curious" and simply saying if there's a problem, turn it over to law enforcement. It's not a reasonable issue given that your local law enforcement is not going to take a case. It's very, very significant against a organization that is likely outside of its own jurisdiction. So, just to bring the focus back that if indeed we did not present the premises properly, that needs to be fixed. But that doesn't alter the issue that we're trying to look at. Thank you.

JANIS KARKLINS: Okay. Thank you. I think this initial conversation gave some ideas on the views of different groups on the case. So we will continue next time. For this, the document will be published for comments but this is not a homework. The SSAC case is a homework for next week.

With this, again we ran out of time. We cannot take point 7. We will take it next time provided that we will be more disciplined and I will be better managing the time. So with this, I have to close the meeting. Thank you very much for your participation. Please do your homework. The action items will be posted online. And if you noted there is a request for all team members to review their Statement of Interest and make sure that they're updated and accurate. With this, thank you very much. This meeting stands adjourned.

TERRI AGNEW: Thank you, everyone. Once again the meeting has been adjourned. Please remember to disconnect all remaining lines and have a wonderful rest of your day.

[END OF TRANSCRIPTION]