ICANN Transcription

GNSO Temp Spec gTLD RD EPDP - Phase 2A

Tuesday, 04 May 2021 at 14:00 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. Attendance and recordings of the call are posted on agenda wiki page: https://community.icann.org/x/2ASlCQ

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

TERRI AGNEW: Good morning, good afternoon, and good evening and welcome to the EPDP P-2A team call taking place on May the 4th be with you, 2021 at 14:00 UTC. In the interest of time, there'll be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please identify yourselves now? Hearing no one, joining us a little later in the call will be Becky Burr and we have listed apologies from James Bladel of the RrSG and Amy Bivins of ICANN Org. They have formally assigned Owen Smigelski as their alternate for this call in the remaining days of absence.

All members and alternates will be promoted to panelists for today's meeting. Members and alternates replacing members,

when using chat, please select all panelists and attendees in order for everyone to see the chat. Attendees will not have chat access, only view to the chat. Alternates not replacing a member are required to rename their lines by adding three Z's at the beginning of your name and at the end, in parentheses, your affiliation dash alternate, which means you are automatically pushed to the end of the queue. To remain 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 functionality such as raising hands, agreeing or disagreeing. As a reminder, the alternate assignment form must be formalized by the way of the 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 to share, please raise your hand or speak up now. Seeing or hearing no one, if you do need assistance, please email the GNSO Secretariat. All documentation and information could be found on the EPDP Wikispace.

Please remember to state your name before speaking. Recordings will be posted on the public Wikispace shortly after the end of the call. As a reminder, those who take part in ICANN multistakeholder process are to comply with the Expected Standards of Behavior. With this, I'll turn it back over to our chair, Keith Drazek, please begin.

KEITH DRAZEK: Thanks very much, Terri. And good morning, good afternoon, good evening, everyone to the EPDP Phase 2A meeting number 19, on Tuesday, May 4th, 2021. As usual, we'll go through a quick review of the agenda. I'll ask for any input and we'll get started. So, as Terri noted, Becky will be a little bit late joining us today. Should note that we did receive the response from Bird & Bird on the remaining question. So, I think there will be some work expected for the legal committee and for the EPDP team in acknowledgement of the receipt of that input. But Becky will join us later on and we can circle back with her at that point to touch base briefly on that.

So, the agenda today, we're going to split essentially evenly between the first topic on our agenda, which is the feasibility of unique contacts. Several groups have provided input to the table that was requested, specifically calling out at this moment, the BC, the Registrars Stakeholder Group and SSAC. So, when we get to this section, I'll turn to representatives of those groups to speak to briefly the input that they provided and then we will go through a walkthrough of the staff-proposed writeup on the text for this particular section.

Once we get through the feasibility of unique contacts, we'll move to the discussion of legal and natural. And again, this is focused on the charter questions but specifically now focusing on the writeup for guidance, for registrars that choose to differentiate between legal and natural.

And in the agenda, you'll note that there's quite a bit of detail that's been included in the document here, that actually reflects back to and refers back to some of the input that's been received from

various groups. It calls out specific questions for the group to consider and to respond to. So, we're going to spend a fair bit of our time, in the second half of the call, focusing on the language that's in the agenda. So, rather than popping back and forth between documents, the language in the agenda here really does call out some of the stuff that we want folks to focus on today. So, while we're getting kicked off here, please do a review of the agenda to make sure you're prepped for that.

And then we'll do a review of the expected homework assignments at the end. And probably just, as I mentioned, check in with Becky on the legal committee.

So, with that, let us go back to the top of the agenda. Let me pause and see if there are any questions, comments suggested edits to the agenda. Okay. Seeing none, let us jump right in. So, item number three on the agenda, feasibility of unique contacts. And again, we're going to review the input that we've received. If any other groups have input that they would like to share but hadn't yet provided by the deadline, as far as the document is concerned, you're more than welcome to get in queue.

But with this, I would like to turn to the document that's on the screen specifically capturing the input from the BC, Registrars Stakeholder Group, SSAC. It looks like GAC may have some additional language there as well. So, anyway, let's go ahead and kick things off. If I could turn to our BC colleagues to lead things off here with the input that they've provided on the feasibility of unique contacts. Mark SV, thanks so much.

MARK SVANCAREK: Thank you. So, I think we've established that the creation of pseudonymous email addresses is technically feasible. So, I think that question has already been answered. Whether or not it should be a requirement is really what we're talking about. And we do think it should be a requirement, first because of its feasibility but also because it is a privacy-enhancing technique.

These pseudonyms can be used for a variety of purposes. They can be used for contacting people. We've expressed several times that the web forms are not always an effective mechanism for contacting people, specifically … Well, first of all, you don't really know if they've been received and read. Secondly, depending on the design of the web forms, it may be impossible to actually convey the message that you want to convey, which again leads to not very good uptake on the other end. And finally, they would assist with correlation, depending on the granularity of them, whether they're across a single registrar or at a bigger level.

So, because of these benefits, we do think that creating them should be a requirement and we think that further work should be done on developing the policy for the safeguards in their use—when they should be published, how they should be disclosed if they are not published, and the like. Thanks.

KEITH DRAZEK: Thanks very much, Mark. Much appreciated. I will move next to … And if folks would like to get in queue and ask questions or provide initial response, you're welcome to do so. I see Sarah, go right ahead.

SARAH WYLD: Thank you. Yes. So, this is Sarah Wyld speaking to the Registrars Stakeholder Group position on this topic. I won't reread our entire comment. You can view it in the document. I will, of course acknowledge that it is technically feasible, yes, to have this unique registration or registrant-based email. But there are risks involved, not only to the registrar.

And I know we tend to focus on the risks to our own businesses in these conversations but also, it's very important to remember the risk to the domain owner, right? As we've mentioned in our comment, there are spam emails that will be sent to their email addresses, correlation of what domains people own, actually does or can reveal identity, can reveal sensitive information. And thus that is something that does need to be strongly considered, carefully considered.

So, we continue to believe that the web form is an adequate, successful method of allowing communication to the domain owner and putting a unique email is an option available to registrars. The domain owner can choose to consent to putting their real email address in the public registration record or we have the web form. And I think that is sufficient so that's our statement at this time. Thank you.

KEITH DRAZEK: Okay. Thanks very much, Sarah. And we will turn next to our SSAC colleagues for their input. And I'll note that other groups did,

after the deadline, provide input so we'll circle back to them shortly. But let's turn to SSAC colleagues now.

STEVE CROCKER: Thank you. I have to confess that I'm quite uncomfortable with the idea of trying to provide pseudonymous email addresses. I'm not at all convinced that it is safe and appropriate to do that. There's a lot of technical stuff that we could get into that probably is not easily accessible in this forum. But let me suggest the following idea.

If the purpose … And I have to say, I really hate to be on the opposite side of this from Mark SV, who I respect greatly on this. But an alternate way of doing the correlation is simply to have a trusted service in which you provide the domain names that you're interested in and ask, “How many of these are related to each other or what's the structure?” and have that service be—have that full access to the registration data. No need to have any cryptographic intervention or pseudonymous representations.

And that way you have a great deal more control and especially have control over evolution. If you try to have one algorithm that is going to transform everybody's email into some scrambled form, then you're at risk if that algorithm has to be changed or is found to have some weakness. I could go on about that, as I said. I don't want to do that. So, I do have to confess, we're not all of the same mind within SSAC but position that I want to put forth is that there are other ways to accomplish what wants to be accomplished—better ways, I would say. And that the idea of trying to impose this pseudonymous algorithm on everybody is not a useful way to go.

KEITH DRAZEK: Thanks very much, Steve. And if we could scroll back up and we're going back to … I guess it's question number one. And next on the list, and the question here—I'll read it—is whether or not unique contacts to have a uniform anonymized email address is feasible and if feasible, whether it should be a requirement. So, next up is the GAC. So, if I could turn to GAC colleagues to introduce their input. Thank you. Would anybody from the GAC group like to speak?

LAUREEN KAPIN: I can jump in and get ahead of the crowd here. We wanted to note that we think the uniform anonymized email is feasible but that has to be tempered with sufficient safeguards to ensure that the registrant is protected vis-a-vis remaining anonymous to the public. And this is an issue we had flagged early on, that the key here is that the system creates sufficient safeguards so that this is a truly—and I think Steve used the better word here—pseudonymous email that the public cannot decode, so to speak.

We also did, however, appreciate some of the concerns raised by other stakeholder groups with the current system, in that there don't seem to be safeguards baked in to make sure that this web form reaches the registrant and promotes a response. And that's in addition to what it sounds like there's some technical limitation sometimes with the ability to use the web form to communicate the full set of information that's desired to be communicated. Thanks, Keith.

KEITH DRAZEK: Thank you, Laureen. Thanks for jumping in. So, I saw Chris Lewis-Evans' hand go up. And Volker, I see yours as well. But, Chris, I'm going to turn to you if you've got anything to add to what Laureen has said.

CHRIS LEWIS-EVANS: Yeah, thanks Keith. So, I just wanted to add that as well, just after reading through the Registrars' input and hearing from Sarah just earlier. So, I think as Laureen said there, I think one of the things that concerns us is that there is sufficient safeguards to protect the data while still catering for some of the requirements from this anonymized email address. And one of the scenarios that comes to mind is there are a number of registrars that are currently using pseudonymized email addresses in their privacy proxy givings. So, it'll be interesting to see how the registrars are providing safeguards under this mechanism at the moment and what functionality those pseudonymized email addresses give. Thank you.

KEITH DRAZEK: Thanks very much, Chris. I appreciate that. Volker, you're next and then Alan Greenberg.

VOLKER GREIMANN: Yeah. So, thank you. I think what we heard is that web forms aren't sufficient. And I agree sometimes that they could probably need some more rules and regulations to make them more

efficient or better to use but it doesn't mean that the web forms are, as a tool and as a concept, not fit for purpose. I also read that there should be a way that basically provides a confirmation of receipt, or that it has been read, or even prompt a response. Well, email doesn't do that either. So, even if you have an email, you have no idea whether somebody reads that email address or that email ever or no guarantee that any response will be provided. So, basically email is the same as web forms. There's no difference there. And I'll pass back to ALAC now. Thank you.

KEITH DRAZEK: Thanks, Volker. Alan, you're next.

ALAN GREENBERG: Thank you very much. A number of things. Clearly, we have enough evidence—we have enough examples—that web forms, as they're currently implemented today, don't work or don't necessarily work. If we wanted to spend a significant amount of time writing rules about what a web form must allow you to do, perhaps then we would have something viable, perhaps. But we haven't even talked about that and clearly, we're not going to do that. So, I just don't see how web forms are viable.

Volker says that email doesn't give you proof of receipt or reading. That's correct but at least you can verify that the email address exists today. A web form translates it to some email address that may not even exist today. It may have existed when the registration was created, but it doesn't necessarily exist today and there's no way of indicating there's a path to it. So, yes, you can't

verify that emails be read but at least you can verify it's gone to a valid email box and someone may read it.

Steve's idea of a third party could well work. But again, that's so far from anything we've discussed. And a concept of a third party who can access everything just is not going to happen in the world we're in today, not with this PDP anyway.

So, the ALAC strongly supports pseudonymized addresses but if pseudonymized is really problematic because of the ability to cross-triangulate and figure out more information, certainly anonymized addresses, there are no such failures. And even the issue of spam can be addressed with anonymized addresses which turn over periodically. And there are registrars around our table today who have used that successfully. That is, the address periodically changes so it can be harvested but it won't do much good later on.

So, let's focus on what we really can do and make sure that we end up with something which is useful. The original Bird & Bird letter said anonymized email is, in fact, personal information because the registrar can figure out who the registrant is from it. Well, the registrar knows who it is based on the domain name itself. So, that argument is somewhat specious and we do have a strong statement saying anonymized email address is actually a privacy feature that we should be considered. So, the ALAC strongly supports pseudonymized, but at the very least, we should have as a baseline anonymized email addresses. Thank you.

KEITH DRAZEK: Thank you, Alan. David, I'll turn to you next but I just want to make a chair's intervention that we've had multiple conversations over the last several months on the topic of the web forms.

I'd just like to remind everybody that if there are issues or challenges with web forms in today's environment and looking forward, that those should be dealt with through the EPDP Phase 1 IRT, related to the existing policy requirements that are going through implementation and/or through ICANN Compliance, if there are Contracted Parties not living up to the expectations and requirements. So, I want to make sure we don't get derailed on a topic of web forms. Thank you for the reminder that that's one of the areas of concern. But let's not go down that rat hole if we could please. David, and then I saw Alan Greenberg's hand go back up. So, David, over to you.

DAVID CAKE: Yeah. Well, you've pretty much said quite a bit of what I was going to say, that we seem to be confusing the issue of anonymous email versus a web form, which I think is a perfectly valid question, though as Volker points out, it won't necessarily magically mean people were responsive. But that which is an implementation issue and the issue of pseudonymized emails, so it consistently uses the same email, who maps one to the other … I tend to think it should be possible with some hashing scheme but it seems to have a number of potential issues. And I don't agree that implementation details that Steve suggests make it unlikely to be something that we'd quickly reach any consensus on.

But the real issue I find here is, it's been described as privacy-enhancing technology—and it appears to be the whole point of the elaborate pseudonymous email scheme—is to provide very specific private information in such a way that it ducks just under some legal limits but is still useful if you have some information that you are able to correlate it.

And it's really just are they very—the difficulty and that loss of privacy, is that worth the benefits, is the real question here rather than is this scheme …? What are the dangers and costs of this scheme versus the fact that it is designed to give up some privacy? I think the very specific amount that is considered valuable, I think is really the issue here. Thank you.

KEITH DRAZEK: Thanks very much, David. Alan, you're next and then I want to turn back to the overview and the introduction of the comments submitted by the groups. I'll come to the IPC next. But Alan, over to you.

ALAN GREENBERG: Yeah. Thank you very much. Two quick points. Number one, Keith, we cannot rely on an IRT to set rules about web forms. That would be imposing new rules on registrars which would be very detailed, very specific and that's just not something an IRT can do. If we had a new policy saying, "You can use web forms but the details of what you must include and what capabilities it has will be set by the IRT," fine. But I haven't heard anything like that. So, you can't take what we have today and what's being proposed

today and say, "The IRT will fix that problem." That's just out of scope for an IRT setting new rules that have never even been discussed in a PDP. That's number one.

Number two, Volker said that forwarded email doesn't bounce back to the user. But right now, if an email that is sent, either by forwarding or by the web form, bounces, the registrar has positive proof it wasn't delivered. And no registrars, to my knowledge, are relaying that back to the original requester, even though technically they could. And I understand some of the difficulties of matching that up when the bounce comes in. But nevertheless, if the registrar receives positive proof that the message was not delivered, that's important. Yes, it would be nicer to get positive proof that it was delivered and read but the converse is also an important thing, which is completely out of what anyone's doing today and out of anything we discussed as setting policy. Thank you.

KEITH DRAZEK: Thank you very much, Alan. And again, I'm happy to be corrected at any point on anything. But my recollection was there is an EPDP Phase 1 Recommendation—a policy recommendation specifically on web forms and reconfirming the Temp Spec language that there must be a web form or an email address. And when and where registrars are required to provide web forms, and do provide web forms, it seems to me that that's both a Compliance question, if they're not living up to the expectations, but also an opportunity for the IRT to work to clarify what the expectations are for web forms.

But again that's really out of scope for this group. I understand that it is a view and a concern of many that is supporting and/or keeping the focus on the question of email addresses. But I just want to make sure that there are other places where the web form can be dealt with. And again, I'm happy to be corrected if I've got any of that wrong. Brian, you're next. I don't know if your hand is up to introduce the IPC points or to make another comment but I'll hand it over to you regardless.

BRIAN KING: Thanks, Keith. My hand was up first to speak to the point that you just made. In the language on the screen with the little Roman I there, the question of whether an email address should be a requirement is being answered in part by the fact that there is no other way to contact registrants. So, the failure of the way that some Contracted Parties are implementing web forms today is strong evidence that this should be a requirement. So it's, I think, really inappropriate to try to take that off the table because that's a big part of the reason why we're saying that this should be a requirement.

So, I hope that clarifies that I realized that policy matters around how a web form must act are best handled in a group that's chartered to focus on that specifically. But you can't prevent us from using that as evidence or an argument why an email address is required because we need contact registrants. And the only way, in many cases, to do that today is broken. So, I hope that clarifies the point. Thanks.

KEITH DRAZEK: Yeah. Thanks, Brian and I'll respond. And again, I completely agree that if the concern as described exists, then there's no harm in referring to it. I'm just trying to prevent us from going down the rat hole that I feel like we're going down and that's to spend a whole lot of time talking about the deficiencies of web forms rather than the topic before us. So, fair enough to flag it as a foundational concern but let's not spend a whole lot of cycles on it—on the web form discussion itself. Marc you're next, then Mark SV, and then I'll come back to IPC.

MARC ANDERSON: Thanks, Keith. There's a lot being said here. I want to remind everybody what we agreed to in Rec 13 in Phase 1. And also remind everyone that Rec 13 is there specifically to meet the purpose that we agreed to in Recommendation 1, specifically, purpose number 3, which is enable communication with the registered name holder on matters related to the registered name. And in Recommendation 13, we say that the registrar must provide an email address or web form to facilitate email communication with the relevant contact. And as registrars have pointed out, the registered name holder also has the ability to provide consent to publish its email address.

Now but then we go on and we say, "The registrar must maintain log files, which shall contain confirmation that a relay of the communication between the requester and the registered name holder has occurred." And a lot of, I think, the concerns that have been raised here is concerns that there's no way of knowing that that relay has occurred—that the registered name holder has received the message that's being sent.

And we discussed this in Phase 1 and that's why we specifically put in this application that registrars must maintain a log file. And we go on to say that such records will be available to ICANN for compliance purposes upon request. So, we already talked about this. We already baked in this mechanism so that there can be confirmation that the relay has occurred and that registrars are passing any of these contact request onto the registered name holder.

KEITH DRAZEK: Okay. Thank you, Marc. Mark SV, you're next and then IPC.

MARK SVANCAREK: Thanks. The previous two interventions sort of build up to what I was going to say. I think we should be very cautious about saying, "Hey, just take it up with Compliance," because if you look at what the policy is, the Compliance would not be able to enforce something that says, "Please design your web form in such a way that I can specifically tell someone that X, a particular thing." So, people can design their web forms however they like. They can have no inputs at all, no checkboxes, no free form, or they can have a very robust and fulsome design. And that's not an issue that you could take up with Compliance.

Marc is right that you could take up the issue of, "Are there log files?" I think we all know that such a request would probably go nowhere and there'd be no transparency into it. Although it's true. That one is in the policy. But just generally, problems with web forms are not related to that aspect of the policy. They're related to

the aspects that weren't well-defined in the policy. And so, going to Compliance to resolve, them which has been mentioned, by my count, at least three times in this phase, isn't going to be effective and we should avoid that.

And I apologize that I had to once again talk about web forms but as Brian said, if it's one of the motivations for creating this new policy, we are forced to mention it. So, thank you and sorry.

KEITH DRAZEK: Yeah. Thanks very much, Mark. Appreciate that. I have some thoughts to add but I'm going to turn to IPC and I want to get through the rest of the input on the screen. We've got another question down below so let's keep moving on. Good conversation so far though. IPC folks?

JAN JANSSEN: Thank you, Keith. I think that we can be pretty short here. It has already been said that making this mandatory is feasible and that is feasible both from a technical point of view and from a legal point of view. I want to remind everybody here that the Bird & Bird memo mentions that the risks are low. If we find ourselves in the low—in the bottom left corner of the little scheme that was proposed by in the memo.

And it is automated disclosure there. It may not be the lowest risk but then again, we need to look at what do we want to achieve and what is the real purpose of making this available. And that is contactability. That is contactability, that's one thing and another thing is that there needs to be some way of finding a correlation

between different domain names. And that is really crucial if we want to preserve some of the policies that should, frankly, remain unaffected by this EPDP. And that is rule 4B2 of UDRP, where every interested individual must be given the opportunity to establish that a registrant has engaged in a pattern of bad faith conduct.

And that is something that was done in the context—that was a policy that was developed in a context, where all of the information was available. So, now we are clearly in a different context where very few information is available and this really impacts one of the previous policies. So, we need really to find the correct balance again between what can be disclosed in a pseudonymized fashion but ensure that we preserve some of the pre-existing policies that really were developed for the interest of the internet user. And this is really what we should aim at preserving. Thank you.

KEITH DRAZEK: Thank you very much, Jan. Volker, go ahead.

VOLKER GREIMANN: Yes. The problem with the correlation is that it can be used by good guys but it can also be used by bad guys and it was never a feature that was built into or baked into the WHOIS by design. It was something that third parties could provide because they were able to analyze bulk numbers of WHOIS, which they had basically grabbed by questionable means before, and then market the raw data in forms that were beneficial for some parties, yes. But it was never a feature of actual WHOIS.

As it also has the problems of bad actors using that data for their purposes, correlation has to be viewed, first and foremost, as a risk factor for the registrants because under GDPR, we first have to look at the risks and the impact that released data can have for the data subject. And only after that, we can use the useful features of such disclosures. So, this correlation, while I absolutely admit that it was beneficial and that it had some very good purposes, is just not a sufficient argument for allowing a uniform email address.

And also, with regard to the UDRPs, it's not like that correlation is the only way that you can show bad faith of the registrant. In fact, the number of UDRPs, if I'm not very much mistaken, has increased since GDPR has come out and people are still winning those. So, absolutely they must be able to prove bad faith and just the lack of not being able to show other registrations that a registrant might have is not anything that excludes someone from proving that their UDRP is in fact warranted and that they have the right—they should have the domain transfer to them so yeah.

KEITH DRAZEK: Thanks, Volker. Alan Greenberg then Marc Anderson.

ALAN GREENBERG: Thank you very much. Volker is conflating the anonymized/pseudonymized address with what is published in the public WHOIS. You could, for instance, put anonymized addresses—that is unique ones—in the public WHOIS and make them roll over periodically but provide synonymized email in a

disclosure through SSAD. That's not the service who scrapes the whole of WHOIS and finds correlations. But if an intellectual property holder is requesting information on 10 domains that are potentially infringing and want to use it to have a UDRP on it, they would then find out that, through a synonymized address, those 10 domains are all held by the same entity.

So, let's not conflate whether it's available publicly in the public WHOIS versus the SSAD with whether we use that concept at all, pseudonymized and anonymized. And there's nothing to prevent using both but using pseudonymized through the SSAD as the contact information. And that doesn't allow all the bad guys to scrape the information and use it. Thank you.

KEITH DRAZEK: Thanks, Alan. Let's turn back to the list and I think next up is NCSG. Okay. Manju, go right ahead. Thank you.

MANJU CHEN: All right. So, can we scroll to our statement, please. Our statement was quite simple. We believe the existing recommendation is sufficient and we don't think there's further changes needed.

But I'd like to come back to what was kind of suggested by other people previously. So, people are saying that it’s necessary to make a correlation between email addresses because that was how it was used to perform some functions they use for some policies—for example, UDRP. But I actually put it in the chat too. Simply because you used it, it doesn’t mean it was right to use it. And it doesn't mean that now we're protecting the registrant's

right—that you can still use it but compromising registrant's rights. And actually, Steve put it in the chat too. It's very different objectives. One is to contact the registrant and I think web form works very well to contact.

And just another note, if you're saying web forms are not contacting the registrant, I am not sure if you're saying you can't reach the registrant because they're not replying or you are sure that they don't get the email. Because even if you get the address of the registrant and you're sending emails to them, they don't have to reply. You don't reply to every email you get, right? So, I don't think that's a valid point to argue for pseudonymized email as a requirement. I think that's about it. Thank you very much.

KEITH DRAZEK: Thank you very much, Manju. And we'll move then to Thomas Rickert. I see that there's also some activity going on in chat. If folks would like to speak, I invite you to the queue but next up to Thomas. And Thomas, you may be muted.

THOMAS RICKERT: Can you hear me now?

KEITH DRAZEK: Yes, we can. Thank you.

THOMAS RICKERT: I apologize for the delay. Now, we haven't submitted an answer in writing. I'd like to go on the record with our response from the

ISPCP, nonetheless. Are anonymized or pseudonymized email addresses feasible? Yes. Is it desirable? We think no, because an important point is that it can't be reverse engineered. So that the communication must be unidirectional. If you have email addresses, there's always the risk of an autoresponder being active and revealing the identity of the registrant. This wouldn't be the case with web forms which, we have commented on earlier we prefer.

Also, the purpose of this processing is to allow for contacting the registrant. And this purpose can be achieved with a web form instead of pseudonymized or anonymized email address.

Additionally, we have to bear in mind that we have to follow the principle of privacy by design. We need to choose the means which is the least privacy invasive. And we think that this is true for web form and not necessarily for an email address. If the group chose to go for email addresses, then we would highly recommend they make it a requirement for our support that it is not per registrant but per domain name and that it is even rotated so that no data can be reverse engineered to identify individuals. Thank you.

KEITH DRAZEK: Yeah. Thanks very much Thomas. And the queue is empty. If anybody would like to get in queue, please do. And then I think we have maybe some input from the Registries next, if we scroll down properly.

I just want to note that I think one of the things that we're picking up or I'm picking up—and maybe it's a reminder to us all—is that there's a clear distinction between contactability and correlation. I think that was noted by Steve earlier, both in the introduction as well as in chat. I noted that earlier in chat. I think we keep coming back around to the distinction between contactability, which is, I think, a much easier question to deal with. And then there's the separate and more challenging question when it comes to privacy of correlation and the methodology through which you would correlate.

So, I just want to make sure that that's clear to everybody. I think, at this point, I guess the question is for the purposes of our work and purposes of developing language for the initial report, what's the path forward? Is there an opportunity for the group to come together on some consensus recommendations on this point? And pretty soon, we're going to need to start pivoting from identifying the individual groups' concerns to trying to find that path forward so please keep that in the back of your mind. Marc Anderson, you're next then Alan Greenberg.

MARC ANDERSON: Thanks, Keith. I was going to speak to the Registries' response on this but I didn't know. Alan has his hand up. I don't know if he's wanting to respond to what Thomas said.

KEITH DRAZEK: Thanks, Marc. Go ahead and then we'll come to Alan next.

MARC ANDERSON: Okay. Thanks. So, first off, Registries have not yet responded to the form. I apologize for the delay. It's taken us a little bit longer than I had hoped to get through our comments. But I will speak to it at a high level and say, similar to the SSAC comments, in discussing feasibility of anonymized email addresses, we discussed the fact that there seems to be two drivers for why groups want this. And as noted in SSAC's comments, it seems to be, one, as a contactability mechanism and, two, as a way of doing correlation.

And on both of these, we came to the conclusion, really, that this is not the best way of achieving either of those aims. We noted that nobody is really pursuing this as a privacy-enhancing technique—that this is a way of accomplishing two completely different goals--one contactability and the other a way to do correlation. And in both of those cases, as I think everybody has noted, while it is feasible, we do note that some of these are not trivial amounts of work and we're not sure that the amount of effort involved justifies the potential benefit. In both cases, we think that that this is really not the best way of achieving either of those goals.

And specifically on contactability, we think the existing mechanisms outlined in Recommendation 13 from Phase 1 are more than sufficient and a much better path forward. On correlation, without speaking to whether or not we support correlation, we do note that this does not seem to be a particularly good way of achieving that goal. Seems like it creates additional risk, additional effort on the part of contracted parties and we

questioned whether it would actually achieve the desired goal at all.

KEITH DRAZEK: Okay. Thanks, Marc. Alan, you're next and then I'll put myself in queue.

ALAN GREENBERG: Thank you. I just want to note that people keep on conflating anonymized and pseudonymized with reversibility, and whether the algorithms can be reversed engineered, and things like that. The fact that there is a correlation that we can go from the either the public address or the one that's provided by SSAD to the real domain—to the real email address, would be done by a lookup table that everyone doesn't have to use the same algorithm. It could be used certainly for anonymized. The registrar could even use multiple algorithms for different domain names based on the time it was registered or something like that.

So, there's all sorts of techniques and the two are not conflated. So, I think even when there's good arguments being made, they're being weakened by the presumption that there is necessarily reversibility, reverse engineering, or ways to correlate. Thank you.

KEITH DRAZEK: Okay. Thanks, Alan. Marc, I saw your hand go up, presumably in response so go ahead and then I'll put myself [inaudible].

MARC ANDERSON: Thanks Keith. I just want to respond to Alan. I guess, I understand that one of the reasons why groups are pursuing this as a path forward is to have the ability to do correlation. In fact, I think that was very clear in the IPC comments, for example, to pick out one fresh in my mind. And I think what I just understood you saying is that you do not support correlation and that you think efforts should be made to prevent correlation.

I guess I just want to understand if I—I just want to make sure I understand your position okay and then just comment that at least as much as I understand it, like one of the goals of at least some of the groups is, in fact, the ability to do correlation. So, I guess, I'm trying to understand where you are and make sure I understand other people's positions correctly.

KEITH DRAZEK: Thanks, Marc. Alan, go ahead.

ALAN GREENBERG: Thank you. We would far prefer pseudonymized email and the ability to correlate, at least from the addresses provided by the SSAD. So, although you can't necessarily find all of the domains owned by that registrant, or at least by the registrant with that contact information, you can at least verify whether the ones you've looked at are. So, yes, we support synonymized as widely as possible, as whatever we can sell in this PDP clearly.

But if that is truly unachievable, then at the very least we need anonymized. So, yes, we support correlation certainly for the domains that have been queried. But if we can't get that at the

very least, we need an anonymization, the current web forms—and I know we're not supposed to talk about it—are not working. And I don't believe an IRT could set sufficient detailed rules to make sure that they would work. If we want to set those rules in this PDP, fine, but we're going to have to start thinking about it soon. So, my answer is nuanced because we can't always get exactly what we want but we need something better than what we have today. Thank you.

KEITH DRAZEK: Thanks, Alan. Much appreciated. Melina, you're next.

MELINA STROUNGI: Thanks, Keith. Just to further build on Alan's point, because indeed as maybe there are several different views in terms of correlation, if we at least we could agree as a minimum on the contactability point, which is something that already is in included in the recommendations, right—the possibility to either use a web form or an email address.

So, given the fact that, indeed, there are some problems noticed in relation to web form, if at least as a minimum we could consider the possibility of using anonymized email addresses—and by anonymized, I mean anonymized vis-a-vis third party to the public—and use this as a starting point of contention, then maybe we could take it from there because this is the point, I think, where more or less we're all on the same page. Thanks.

KEITH DRAZEK: Okay. Thanks, Melina. Appreciate your input. I'm going to put myself in queue here. Just to note in terms of timing, we do need to move on fairly soon to the next topic on our agenda, which is getting into legal and natural. The second question under this heading was, if feasible but not a requirement, what guidance if any, could be provided to Contracted Parties who may want to implement uniform anonymized email addresses? And I'm just going to say anonymized or pseudonymized here.

But I think this is … Based on the previous conversation, I don't sense that there's consensus on creating a new requirement at this time for anonymized or pseudonymized email. So, the question then turns to, if it's feasible but not a requirement, what guidance could we provide? And I think we need to start thinking in terms of what we want to include in the initial report here on that point. And I'm going to suggest this as a possibility but I'm interested in feedback. This group could create a recommendation around guidance for registrars, that could also be funneled to the IRT from Phase 1 on the topic of web forms and/or anonymized email addresses.

So, again, I think the key here is, we do have an existing requirement for contactability using either a web form or an email address. The Phase 1 IRT is currently active. This could be a further input as guidance to that group and to registrars and Contracted Parties, around possible considerations. But I think we need to start thinking about the path forward here in terms of what we could recommend, both to Contracted Parties and to the IRT from Phase 1, as guidance—as recommendations from the group that probably come up short of a full-blown policy requirement.

So that's just my sense of the group at this point but I'm happy to hear from others. And I think what we need to do is to focus here briefly on this next question before we move on but note that this question is something that we're going to have to come back to in a future call. Brian, go ahead.

BRIAN KING: Thanks, Keith. And I regret that we haven't had a chance to put an assessment in here or guidance. One thing that I noted above, just recently, that I will put in here is that if we're thinking about proportionality and how best to enable contact with a registrant in a way that that is the least intrusive, involves the least processing of personal data is that, if you think about all the RDS data fields, the email address is really the least likely to be personal data, right?

If you're an individual registrant, chances are you don't have multiple mailing addresses that are at your disposal, right? At a least common denominator, you probably don't have multiple phone numbers, for example. So those are probably more likely to be personal data. But we know that email addresses are typically free of charge and can be made up of basically any string of characters. And so, in fact, that's probably the one field that doesn't necessarily need to be personal data at all.

I know we try to be super careful and limit processing of personal data. But if we're looking at proportionality, I think guidance that we can give to Contracted Parties is, “Look, tell registrants not to put personal data at an email address,” and then that that could

be a proportional response or a way to allow contactability of registrants. Thanks.

KEITH DRAZEK: Thanks, Brian. And I think there's some additional chat going on. If folks would like to get in queue, please do. But I want to just open the queue at this point. We don't have time to go through line-by-line, group-by-group. I want to just open the queue here and see if anybody has any constructive suggestions for a path forward on guidance that could be provided to Contracted Parties and/or the IRT from Phase 1 on the web form issue, related to the use of web forms and/or in this specific question, those registrars who choose to implement uniform anonymized/pseudonymized email addresses.

And Brian, I take your point that your suggestion there was that registrars should advise or instruct registrants in the registration process to not use email addresses that contain personalized data and that certainly could be guidance. How that's implemented, I think, is another question but I won't speak to that. Sorry, I'm just trying to keep up with chat here. Folks, if you would like to get in queue, please do. I think sometimes we do better when we can actually speak and hear each other rather than double tracking in chat.

All right. I'm not seeing any hands at this point so I think we probably should put a line under this one today. We will come back to this, obviously. Please be thinking about a path forward in terms of consensus on guidance and then let us move to the next item on our agenda, which is legal and natural. So, what we're

going to do here is again—and we may not get through all of this today—but to consider the guidance writeup that the staff has consolidated based on input. Caitlin, I see your hand. Go right ahead.

CAITLIN TUBERGEN: Thanks Keith. Before we move to the legal versus natural issue, we had in the agenda for staff to do a quick overview of the writeup for feasibility, if you'd like me to quickly walk through that.

KEITH DRAZEK: Yeah. Thanks, Caitlin and thanks for the reminder. Go right ahead.

CAITLIN TUBERGEN: Thanks Keith. Before I go into detail about the staff writeup, while Berry is pulling that up, I just wanted to give a couple of disclaimers on it. The first is that this writeup was done over the weekend, which was following the deadline for feedback, and several groups provided feedback on Monday. So, that feedback won't be reflected in this version. However, as always, you can propose edits and comments, concerns in the form of comments in the Google doc.

And the other disclaimer is that, similar to the writeup for legal versus natural, there's a lot of background text included at the beginning of the writeup. This is for the purpose including in the initial report and it's supposed to be factual representation of previous recommendations, what the genesis of the questions

was. And so hopefully, there wouldn't be any comments in relation to the first sections. But, Berry, if you could just scroll back up.

You'll notice that the format's very similar to the legal versus natural. The first section deals with the actual question being posed by the GNSO Council and that the way the team went about its work. The second section is the relevant definitions. And as you may remember, in Phase 2, there was an issue about the use of the word anonymized and that it was probably a misnomer because for data to be truly anonymous, it needs to be anonymous to the controller. And because a registrant's contact information or some pseudonym generated by the registrar wouldn't be anonymous to the registrar, that was a misapplied term.

So, we use the term pseudonymous in Phase 2 when we posed questions to Bird & Bird. However, the team had suggested further consideration of those definitions. So, early in Phase 2A, the legal team discussed the updated definitions that were used in the Phase 2A questions sent to Bird & Bird.

So, you'll see at the bottom, the registrant-based email contact, which of course would be a pseudonym that corresponds to all of a registrant's email addresses at a particular registrant, versus the registration-based email contact which, as some of you had mentioned earlier in the discussion, this would be on a per registration basis rather than on a per registrant basis. So, they both deal with pseudonymous contact information but one is on a registration-based and one is on a registrant-based.

As we move down the document, this includes the relevant background info and the initial EPDP team observations. The first section deals with the annex to the Temporary Specification, where that quoted text is copy pasted right from the Temp Spec, which is the question that this team was trying to address in Phase 2. And then there is the cross-reference to section 2.5, which is stated in that text.

As you move down, we've included the relevant Phase 1 recommendations, which have been referenced many times today as well as in previous conversations. Recommendation 6, which deals with consent, and Recommendation 13, which deals with requirements around email addresses and web forms.

We also included the previous conclusion from the Phase 2 final report which was essentially that it's feasible but there were some problems based on the legal guidance that we received. However, the team did receive that legal guidance late in the process and accordingly, some of the stakeholders asked for more time to consider this issue which is why the GNSO Council allowed the Phase 2A team to further consider the issue.

And then the final section is the proposed response to the Council questions. And again, as a reminder, this doesn't factor in some of the feedback that we received yesterday and today. But essentially, the way that it is written as of right now is that the team acknowledges that it is technically feasible to have both the registrant-based email or a registration-based email. However, there are risks involved that prevent the EPDP team from making a recommendation to require Contracted Parties to publish a registrant-based or registration-based email address at this time.

However, the team does note that certain stakeholder groups have expressed the desirability for both of these contacts, in particular where a registration-based email contact would be beneficial for the purposes of contactability and a registrant-based email contact be beneficial for correlation purposes. And then the last paragraph notes that we received legal guidance from Bird & Bird on this issue and that we would attach that as an annex to the guidance.

I'll note that support staff felt uncomfortable going through the memo and copying, pasting certain portions of that memo since if there is specific guidance that the EPDP team members would like to highlight, you're more than welcome to do so but staff thought that was probably not our job or we were uncomfortable choosing the guidance that the team would like to highlight here.

So, that is where the writeup currently stands but as I noted a few times, this doesn't incorporate all of the feedback we've received so all the team members are welcome to include additional guidance that you'd like to see or propose changes to what is currently there. And with that, I'll hand it back to Keith. Thanks, Keith.

KEITH DRAZEK: Thanks so much, Caitlin. And apologies for almost missing that because I think that was critically important as the team looks to focus on developing language for the initial report. So, just a reminder to everybody, this is the proposed and draft text for the initial report.

So, now that we've gone through the conversation, or at least preliminarily gone through the conversation based on direct input, it's really important for folks to start focusing on the draft writeup, making sure that we've identified any sticking points, if there's anything that's sort of in a can't-live-with category, that we start flagging that as soon as possible because this is going to become the foundation of the initial report. And I think the inclusion of all of the references and all of the context is critical but at the end of the day, it's a question of what we're going to recommend as a group and then put out for public comment. Alan, I see your hand. Go ahead.

ALAN GREENBERG: Thank you, Keith. I just want to make a comment and I'm not quite sure how we should be handling this. Phase 1 listed email, anonymized email, or a web form as something which is not redacted. That is, it's in the public WHOIS whatever—in the publicly accessible record, published record. I don't believe we ever, in Phase 1 or in Phase 2, talked about whether this is the same information that is provided on a reveal through the SSAD.

And I think we probably should have somewhere along the way—and if we didn't do it, then maybe we need to do it now—clarify. Is this same anonymized address or a URL for a web form, what is provided through the released information from the SSAD or is it something different, potentially, which could be either the real email address or it could be anonymized, pseudonymized. There's lots of options. But I don't think we've ever had any clarity as to what contact information is provided by the by the SSAD on a reveal, as opposed to what is published in the WHOIS. Thank you.

KEITH DRAZEK: Thanks, Alan. I will admit to not knowing the answer to your question. Many of you on this call and on this team have been involved in Phase 1 and Phase 2 far more deeply than I have. So, I think it's a good question. I think it's a legitimate question and maybe one we should come back to. I don't know if anybody has any initial reaction. I see Sarah's typed in the chat. Sarah, would you like to speak up?

SARAH WYLD: Hi. Thank you. I'm going to see if I can find specific references in the Phase 2 final report as we continue this meeting. But the understanding that I came out of that phase with was that it was the real registration data. I don't think we talked about disclosing pseudonymized or anonymized data via the SSAD but I like the idea. Thank you.

KEITH DRAZEK: So, thanks, Sarah and thanks Alan, for teeing the question up. So, I think the key takeaway there is that, at least from Phase 2, there was an understanding that the real registration data would be disclosed via SSAD in response to a request. And I see there's some additional language being posted in in chat there.

So, all right. Let's move on. I think we need to turn now to legal and natural. We're going to review the guidance straight up. I'm going to turn back to Caitlin here pretty quickly. But again, the key here is that we now have some consolidated language here in the agenda for us to go through and we are pivoting again to try to

focus on consensus recommendation language for guidance to registrars who choose to differentiate on the question of legal and natural. So, Caitlin, if I can hand it back to you. Thank you so much.

CAITLIN TUBERGEN: Thanks, Keith. So, hopefully you all had a chance to review the agenda that we circulated but you'll notice that there were four outstanding questions from our last call. And the first question is in reference to the third part of the guidance, or guidance number three, which is about registrars having the option or should consider using some type of flag in the RDDS to help indicate the type of data concern in the registration.

And I'll note that in the table that we used, ALAC has suggested approximately, I think, eight bullet points that amounted to more specificity to registrars who would like to implement that type of flag. So, our question to the group is, is more specificity needed here for implementation purposes or would that be too prescriptive? The current guidance already includes references to a type of flag but we're wondering what's missing here or what else would be helpful for registrars to know in reference to the flagging mechanism? Thanks.

KEITH DRAZEK: Thanks, Caitlin. I see Brian has his hand up. If others would like to get in queue, please do. Brian?

BRIAN KING: Thanks, Keith and thanks Caitlin. I'm wondering how much time we need to spend on this or whether we really need to call it explicitly guidance. Maybe we do but just go slowly or don't spend too much time on this because Contracted Parties are going to have to do this in order to comply with the SSAD regulations to automate disclosure of personal data after it has been revealed once and determined not to be personal data. So, that's already something that they're going to have to implement. Maybe we just note that in order to comply with EPDP Phase 2 recommendation whatever the number is, that Contracted Parties are going to have to flag data as one way or the other in their systems. Thanks.

KEITH DRAZEK: Okay. Thank you, Brian. The queue is open. Marc, go right ahead.

MARC ANDERSON: Thanks, Keith I think maybe I want to start with a follow-up question for, for ALAC. I'm not sure exactly what they're hoping—what their suggestion means in terms of implementation. If we're just talking about a flag in the registrar's system to indicate if it's personal or non-personal data, that wouldn't necessarily be a flag in the RDDS. RDDS systems are generally query systems. And so, I don't know if that's what you mean when you say a flag in the RDDS or if you're looking for an indication in the response to an RDDS query, which are two very different things.

And I understand this to be guidance for Contracted Parties that choose to differentiate. And talking about a flag kind of confuses me in this context. I thought about how it would be done otherwise

and, from all practical purposes, there would need to be some indication in the registry system that the data is legal, or natural, or personal, or non-personal. And so I'm not really sure what this guidance is attempting to achieve. I'm sorry. I'm rambling a little bit. I guess I'm asking for a little bit of clarification from ALAC as to what they're hoping to accomplish with their suggestions for guidance here.

KEITH DRAZEK: Thank you, Marc. And I've got Hadia and Alan in queue. If there's a direct response to Marc, I'll offer it to either one of you. I assume, Alan, you're responding to Marc and then Hadia I'll come back to you. I'll let you all work it out. Thanks. So, Alan, go ahead. You're on mute.

ALAN GREENBERG: Sorry. The difference between a registrar field and an RDDS field is that one is purely internal to the registrar. The other is not. So, for instance, if the registrar is complying with the thick WHOIS requirements for new gTLDs right now, a flag in the registrar system is not conveyed to the registry. So, the registry doesn't know this is a legal person or not. Moreover, it's also not put into escrow. It doesn't go into a variety of other places. So, having a defined field in the RDDS is really important because that means—that conveys a lot of information, which otherwise is completely lost within the registrar system.

So, by putting it in the … When we talk about an RDDS flag, we are talking about an RDDS flag. Now, since we now have a new

field, we have to go back to the Phase 1 work and say, "Is this a redacted field or is this a public field?" I personally believe it should be a public field but we've never had the discussion because we've never had that field there. Thank you. I hope that makes it clear.

KEITH DRAZEK: Thanks, Alan. Hadia, you're next and then I think Alan wanted to follow-up on Alan's point. Sorry, Alan Woods wanted to follow up on Alan Greenberg's point.

HADIA ELMINIAWI: Okay. Thank you, Keith. So, basically, I wanted to respond also to what Marc just said. So, basically, it's a label. It's a field just like Alan said and we are proposing three types of fields. So, one is a field that differentiates between legal and natural registrants. And that field, we suggest that it should be required. And then two other fields, one that differentiates between the data, non-personal and personal and a third one that differentiates—that says if this data is protected or not protected. So, those are basically fields. Labels.

And I don't know if we need to go again through, why is the differentiation between the registrants necessary and what extra benefits does it give? Because I think we discussed this in detail a lot but again, this is the proposal. And does it need to be …? Definitely it's important to be a field and then the field would pass from the registrar to the registry and that would provide consistency along the data across registries and registrars. Does

it need to be conveyed to the requester as well? Well, not necessarily but the importance is to have this kind of consistency across registries and registrars. Thank you.

KEITH DRAZEK: Thank you, Hadia. Alan Woods, you're next.

ALAN WOODS: Thank you very much. Yes, I feel like going a little bit too much in the weeds so I would keep myself from going too far. But this is again, this assumption that because it works at the registrar level, it will automatically somehow work by us reading a flag at the registry level. And again, that's not really true to be perfectly honest.

If we are saying that there was a mandatory requirement to do X and we have to rely on X, well then, we're adding two layers of issue there. If the registrar gets it wrong, that means that the registry has also, by extension, gotten it wrong as well. If we're saying it is a non-mandatory but it is based on guidelines, then the registry does have an obligation to ensure that before they accept a mere flag in the system, that they have a means of testing that. And they would have to have a means of testing that at every single registrar that is feeding them the data.

So, again, when we're talking about levels of complexity, you're putting in a factor of complexity times the amount of registrars and the means by which they are testing it at a single registry level. So, I think we need to be very careful when we're saying that, if it applies to a registrar, it should apply to a registry and they can just

read it from the flag. In reality, as a controller, that would be a dereliction of duty and of legal obligation, where we just merely accept it. So we would need a little bit more.

KEITH DRAZEK: Okay. Thanks, Alan. Would anybody else like to get in queue on this point? All right. I'm not seeing any hands. So, look, folks, we have about 10 minutes left on today's call. We do have another call scheduled on Thursday, of course.

So, I'm going to take a moment here and hand the microphone back over to Caitlin. Caitlin, I'm going to ask you if you would give an overview similar to what you did for the language above on unique emails. If you could give us the five-minute or five-to-seven-minute overview of this to tee us up well for the next meeting on Thursday, I would appreciate it. So, Caitlin, if I could hand it back to you and then we'll probably need to move to wrap up today's call. I'm sorry that we didn't get through as much as we'd hoped for. But, Caitlin, thank you.

CAITLIN TUBERGEN: Thanks, Keith. So, the other outstanding questions, the first one is that, as you know, we've had three scenarios for how self-identification could work or if the registrar could determine if it's a legal versus natural person. And the second question is in reference to, again, feedback we received from ALAC. And that is that the scenario should be removed entirely and replaced by the registrar table. And the registrar table is, as a reminder, the table that Registrars circulated a while back in response to the initial

proposal from GAC. So, we wanted to see what others thought about that as a suggestion.

And then the second question is in relation to scenario two, which is when the data subject self-identification occurs at the time when a registration is updated. If you can scroll down a little bit, Berry. The note here is that the GAC provided some feedback that it would be helpful to have some clear timelines as to when that self-identification would occur. And so, we're looking for guidance from the group, if there are any example timelines that we could include here to address the concerns from GAC.

We can scroll down a little bit, Berry. Scroll down a little bit more. Thanks, Berry. And then the final question is in reference to scenario three and that is when a registrar chooses to—or decides or determines that the registrant is a legal or a natural person. And I believe the example that had been previously given is that some corporate registrars who are familiar with our clients can already determine that the registrant is a legal or natural person. And I know that NCSG has expressed concerns with that and would like that scenario to be removed entirely.

I did want to note that Volker had proposed some language about third party verification. This was a concept that was referenced in the memo from Bird & Bird. The proposed language notes that third-party verification is not something that's explicitly prohibited but it's also not something that's specifically recommended by the EPDP team. In response to that addition, the NCSG has again expressed objection to the scenario and also to the specific rewrite as NCSG believes this makes scenario three much worse. And so, we wanted the team to consider these concerns and

determine if or how they can be addressed. So, those are the remaining questions that we'd like to get through on Thursday.

KEITH DRAZEK: Thanks very much, Caitlin. Much appreciated and concise and helpful as always. So, I'm just going to note here that we've just got about seven minutes left on the call so I'm going to ask if anybody has any input, any thoughts they'd like to share on what Caitlin just described. I see that Alan is asking for the URL for that document in the chat so if we could make sure that's made available. And then I see hands from Brian and from Hadia. So, Brian, over to you.

BRIAN KING: Thanks Keith. For the last point there, I understand that the NCSG has a policy position that the registrant should be in a position to control the—to self-designate and they don't want the Contracted Parties to be able to override that. But the data protection law is pretty clear that the obligation falls to the controller to make that distinction about whether the controller is processing personal data and process it accordingly. So, I think we can note that but we can't overrule the GDPR here. Thanks.

KEITH DRAZEK: Thanks, Brian. Hadia, and then Stephanie.

HADIA ELMINIAWI: Thank you, Keith. So, I raised my hand just to note that our suggestion to remove the scenarios depends on the bullets or the items included above. So, definitely if the items before the scenarios do not actually emphasize or tell us the—does not give a good summary of the guide and what the registrars or registries need to do, then the scenarios would be necessary. Thank you.

KEITH DRAZEK: Okay. Thank you, Hadia. Stephanie, you're next?

STEPHANIE PERRIN: Hi. Thank you. And I'm just wondering on what basis Brian is saying that NCSG has a firm policy position that the registrar should be able to decide. We have been having a very vigorous debate that is still, to the best of my knowledge—and I'm one of the debaters—not decided as to what our final advice on this is. Basically, yes, we firmly believe that registrant control is desirable when it comes to protecting. Obviously, an individual is the only person who can consent to disclosure, pursuant to the existing obligation that we have for registrars to provide an opportunity for registrants to disclose if they elect to do so.

But on the matter of distinguishing between legal and natural, we are still divided as to whether we firmly believe that that is in the hands of the registrant. And here's where I agree with Brian. The data controller has the responsibility and the liability to determine whether he or she is disclosing personal information. So, regardless of what the registrant says, they cannot disclose personal information if they don't believe that the registrant,

whoever that representative may be, is capable of making that decision. Is not capable in the sense of being intelligent enough. It relates to authority, available information, updated-ness etc. So, I think we're trying to get that resolved. Thank you.

KEITH DRAZEK: Thanks, Stephanie. And in light of time and not seeing any more hands in chat in the queue, let us move to wrap up our call today. We've got two minutes left. Just want to do a quick review of the expected homework assignments. Alan, to your point about the URL, I think this was a document that was circulated to the list yesterday, if I'm not mistaken and we'll follow up with staff to make sure that everybody's got a reminder and pointer to that.

So, expected homework assignments before the 7th of May, this Friday, we need to review the proposed feasibility of unit contacts write-up for the initial report. Following today's call, the staff will do a review and an update of both of the documents, both of the write-ups and circulate for the group. And again, please work in those documents in the form of comments—not red lines but provide comments and input to the document itself once circulated. And that's the same for the legal and natural guidance writeup. And again, staff will work to update that document following today's call, in preparation for our work on Thursday.

So, please everybody, especially on the legal and natural point, before Thursday's call when we will turn back to this topic, make sure that you've reviewed the latest version of the writeup that will be circulated shortly by staff. But do spend time and make sure

that we're covering that so you're prepared to engage during the plenary call on Thursday.

And then finally, we've got a note here that by Friday that the GAC and the Registrar team should review updated version of the write-up and indicate to the EPDP team if the GAC's updated proposal on the registrar table, respectively, need to be included, where it would be included and what aspects it would cover etc.

So, please, let's make sure that we cover the homework assignments, be prepared for Thursday, and we'll dig deeper into the discussion of legal and natural and specifically the writeup. I think the key here, folks, is we need to be focusing on the writeup documents primarily if not exclusively. So let's make sure we're doing that. Stephanie, I see your hand. Last word and we'll go to close. Stephanie, is that a new hand or an old hand. I apologize.

STEPHANIE PERRIN: Old hand. Sorry.

KEITH DRAZEK: Okay. Not a problem. Thank you. Okay, next EPDP team meeting, Thursday, 6th of May at 14:00 UTC. We'll confirm action items on the list and thank you all very much for your participation and let's make sure that we focus on those writeups please. With that, we'll conclude today's call. Bye all.

TERRI AGNEW: Thank you, everyone. Once again, the meeting has been adjourned. I will stop all recordings and disconnect all remaining lines. Stay well.

[END OF TRANSCRIPT]