ICANN Transcription
GNSO Temp Spec gTLD RD EPDP – Phase 2A
Thursday, 22 April 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/4ISUCQ
The recordings and transcriptions 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 P2A Team Call taking place on the 22nd of April 2021 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 yourselves now.

Hearing no one, we do have listed apologies from James Bladel of the RrSG, and they have formally assigned Owen Smigelski as their alternate for this call cand any 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 chat. Attendees will not have chat access, only view to the chat.

Alternates not replacing a member are required to rename their line by adding three Z's to the beginning of your name, and at the end in parenthesis your 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 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 speak up now or raise your hand. Seeing or hearing no one, if you do need assistance, please e-mail the GNSO secretariat. All documentation and information can be found on the EPDP Wiki space.

Please remember to state your name before speaking. Recordings will be posted on the public Wiki space 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: Thank you very much, Terri. Good morning, good afternoon, and good evening, everyone. EPDP Phase 2A Meeting #16 of the 22nd of April. So, just a couple of quick notes before we kick things off. I'll just do a quick review of the agenda in a moment. But I would

just like to lead off by saying thanks to everybody who contributed and continue to contribute to our working documents, both the write up document as well as the high-level summary of responses on the question of whether consensus policy changes or amendments are needed. I think this has been an excellent example of contribution and engagement. So, just a quick note to say thank you for all the work, both on the e-mail list as well as into the documents. And we'll get to that.

But I want to take a moment to just remind everybody—and especially as we enter what is essentially the last five weeks to develop our initial report—to try to remain constructive and respectful in our engagement. Disagreements are fully understandable, if not expected, but I want to make sure that as we enter this last phase of our work over the next four to five weeks, especially as the work intensifies and perhaps differences of opinion become more crystallized, that we all continue to remain respectful, constructive. That we're seeking to de-escalate arguments rather than escalate them. That we make sure that we are not being personal in any engagement that we have or exchanges that we have. And that we're trying to work together to try and identify opportunities and paths for compromise and consensus.

So, I just want to flag that. I know that it's going to get potentially contentious over the next several weeks, and that we've got some differences of opinion within the group. But I just want to remind everybody that we do have Expected Standards of Behavior, and that I'm just asking everybody to again sort of double down and try and remain constructive and respectful as we do our work.

I think we've done a very good job of that so far, and this is really just a reminder to everybody to try to maintain that and to reapply those principles.

So with that, I will move to a quick review of the agenda, and then I'm going to hand it over to Becky for a quick update from the Legal Committee.

But essentially, as we circulated previous and what's on the screen before us, we're going to start with the discussion on the feasibility of unique contacts. We did receive a response from Bird & Bird to the question submitted on the topic of the feasibility of unique contacts. When we get to this section, I'll again hand it over to Becky for an introduction to the memo response that we received around the definitions. And we'll have some discussion on this topic.

Once we finish with that, we'll move to our discussion of legal and natural. And then specifically, we will lead off in focusing on the feedback received, I think, from almost all groups. And thanks, again, for your input on this question of whether any updates are required to the EPDP Phase 1 recommendations about the need to either move from "permitted" to something else if there need for additional consensus policy work or changes to the pre-existing consensus policy recommendations.

And then if we get through that and there's time, we'll move to a review of the write up document that's been circulated where folks have provided input. I've noted that there are further contributions on the e-mail list today. And that's all very welcome.

So, that's essentially our plan for today. Let me pause and see if anybody has any question/comments/suggested additions with the agenda before we get started.

Okay, seeing none. Thank you very much. And with that, let's go ahead and kick things off. So, Becky, I'm going to hand it over to you now for an update from the Legal Committee. Thank you very much, and over to you.

BECKY BURR: Hi. Good morning, everybody. Our update hasn't really changed much. We received answers to all but question three, which is the question regarding the implications of the manner in which EURid, ARIN, and RIPE are implementing GDPR with respect to WHOIS data; and a question as to whether the language of the NIS 2 proposed directive regarding distinctions between legal and natural persons should be seen as some sort of precedent that helps us interpret what the rules of GDPR are.

So, we're still waiting for that last item, and we will circulate it as soon as it comes. But otherwise, I believe that all of the other memos have been circulated to the plenary.

KEITH DRAZEK: Okay. Thanks very much, Becky. Any questions or comments? All right, Becky. Thank you very much for that update. And I will turn back to you here momentarily. Let us now move then on our agenda to item #3, feasibility of unique contacts. And again, just to recap, the questions before us from our charter are whether or not unique contacts to have a uniform anonymized e-mail address is

feasible. And if feasible, whether it should be a requirement. And if feasible but not a requirement, what guidance, if any, can be provided to contracted parties who may want to implement uniform anonymized e-mail addresses.

And, again, I think we've had some movement and some development on our definitions. And, again, we'll talk about that here in a moment when talking about anonymization, pseudonymization, etc.

Steve, I see your hand. Go ahead.

STEVE CROCKER: Thank you. I thought I would just jump right in on this. I've said a little bit on this before, I think. And I just wanted to summarize. [It's a] fairly strongly-held view.

There are at least two different things that are conflated in the idea of pseudonymous and uniform e-mail addresses. One is a service to the registrant of having a uniform way of identifying themselves when they choose to do that. And the other is the desire for third parties to be able to correlate different registrations. Those are completely separate, and they tend to get conflated, as I say, in this idea of a unified e-mail address.

The short answer to the question is no, it's not feasible to impose something like this, particularly with the idea that it would be anonymized and avoid correlation, and particularly it's not feasible to do it over against the wishes of the registrant. The registrant can always make up a new identification if they want.

So, I think it's important to tease those apart for the basic idea of how do you contact a registrant without disclosing who they are. The answer seems to me blazingly simple and implemented by quite a few of the registrars. You simply provide a forwarding process through the registrar. And that's the end of that story, I think.

I'll break off and you can have [the debate] further if people want to push back on any of those points.

KEITH DRAZEK: Thanks very much, Keith. And I will hand it over to Becky here in a moment, but I'll open it up to see if anybody would like to respond to that. But I do want to just put a marker down to say we don't want to go back and reiterate and rehash the discussion about whether web forms are sufficiently functional today. I think we've had that conversation. I think that's really a conversation, at this stage for this group, related to … That's an ICANN compliance and/or a Phase 1 IRT issue at this stage. So, I want to avoid rehashing that conversation.

But what that, let's get back to the queue, and then I'll hand it to Becky when we get through. Anybody that would like to speak on this one. Volker, your response to Steve?

VOLKER GREIMANN: Yes. Obviously, I agree that it doesn't seem feasible because of all the arguments that we've ready raised in previous calls. In a way, you could argue that there is already a uniform e-mail address that many registrars have which applies for all

registrations that go under their ticker. But that is, I think, not what it intended here. Uniform has issues that cannot be resolved in a manner that is privacy friendly, and therefore we should probably look at other alternatives. Thank you.

KEITH DRAZEK: Thank you, Volker. Would anybody else like to get in queue before I hand it to Becky? All right, Becky, over to you.

BECKY BURR: Thanks. Sorry, I had a little problem unmuting. On this one, we have a nice memo from Bird & Bird that basically confirms its previous guidance that both the registrant-based system and the registrars-based system involved involve processing of personal data because it's obvious that the intent is actually to contact the individual. And the point of having the SSAD system is that individuals with legitimate and proportionate interests would be able to identify those.

So, I don't think that there's any question but that our analysis was correct on that. Having said that, they also confirmed, of course, that both of the approaches involve the use of privacy-enhanced technology.

And they essentially provided a grid that said, "Here's the risk from highest to lowest." And if we could go to that grid. Yeah. So, a registrant-based e-mail contact. Remember the e-mail is the same for a registrant, no matter how many, for all of their registrations. With web publication, that involved medium risk. And, of course, I

just want to say that they say this reflects the important assumptions and caveats that they provide later.

The registration-based e-mail contact with web publication is probably low, so a single e-mail that is not carried over across a particular registrant's registrations.

Automated disclosures of a registrant-based e-mail contact is probably low, but automated disclosed of a registration-based e-mail contact is the lowest. None of these are without risk. All of them involve the processing of personal information, but that's the order in which they see them.

Now, they have some other cautions about the assumptions that they're making here. Also, assumptions related to the fact that they assume, for example, that if … Well, I think that the memo kind of speaks for itself on it, but this is the meat of the memo here. All of it involves personal information processing.

The range of risk: the highest risk, is publication of a registrant-based e-mail contact, and the lowest risk is automated discloser of a registration-based e-mail contact.

And I think unless you want me to read it in detail, that's probably the high-level summary that people need.

KEITH DRAZEK: Yeah. Thanks very much, Becky. No need to go through it line by line, for sure. This was part of everybody's homework assignment, and I'm sure folks have read it. So, I just want to open the queue and encourage folks to get in queue to engage. If you have

questions, please ask. If you have views, please bring them and let's get into this one.

Volker, go ahead.

VOLKER GREIMANN: Yes. Of all the words that I've read in there, I like the word "lowest" most, so that's probably the choice that I would end up supporting. And that is fortunately also the choice that I've been advocating on the list for a while now, so that would be automated disclosure of a registration-based contact. I think that is the one that probably has the biggest chance of consensus that has the lowest risk attached to it, that has the highest amount of confidence that the requestor is not able to abuse this kind of access to this data, that this data still can be assessed in a meaningful way by those that have legitimate interests.

And quickly, I think it bears a chance to significantly improve the functionality of SSAD. It gets the cow off the ice on a lot of questions with regard to automation that we've had in Phase 2. I think if we go in that direction, we will solve so many problems and so many discussions that we can focus on the remaining details of how to implement it and how to make sure that this can be part of SSAD because, obviously, it might require some changes to the decisions that we made in Phase 2.

But I think it's the best way forward that we have, and it's the best one that gives us the chance of success within the time that we have as well. Thank you.

KEITH DRAZEK: Thank you, Volker. Jan, you're next.

JAN JANSSEN: Thank you, Keith. And thank you, Volker. I for sure understand that you like the word "lowest" the best, and that's understandable. But we also need to think how to bring the risk assessment in line with other long-existing policies that are based on legitimate interests of Internet users.

To give a very obvious example here, it's in the UDRP which is the longest-standing consensus policy. There is a possibility to show a pattern of registrations that can be indicative of bad faith. That is a long-standing policy. And if we opt for the lowest here, I'm not sure if we are not de facto revising the UDRP, and we are not chartered to do so. So, I think that this perspective is also needed here.

KEITH DRAZEK: Thank you, Jan. And Steve, your hand. Go ahead. Steve, you may be on mute.

STEVE CROCKER: Thank you. Sorry about that So, it's exactly this point that I want to push on. The idea of trying to correlate and see about whether there's a single party or a small set of parties behind a common set of registrations is distinct and separate from whether or not you can contact the registrants.

And in order to facilitate that purpose—that is, to be able to do the correlation—you need access to non-public information. Trying to have it both ways to make the information public and do the correlation is not going to win on any score. It's going to violate the privacy, and it's not going to do a very good job of doing the correlation. And so, I push back again on trying to conflate these two things.

I think it's just very important to treat each of them as independent purposes and to look at what is the best way to implement each of those purposes and give them full weight rather than trying to coalesce them into a single mechanism.

KEITH DRAZEK: Thanks very much, Steve. And if anybody else would like to get in queue, please do. But I've noted that there are some questions in the chat related to Jan's intervention and related to UDRP. And so, Jan—or if anybody else—would like to respond or follow up, I think there are some question or uncertainty or lack of clarity about the connection between this discussion and the implications for UDRP policy.

Steve, I think that's an old hand. And Margie, you're next. Go ahead.

MARGIE MILAM: Good morning, everyone, or afternoon. Yes. I agree with what Jan was saying. Perhaps I can share some insight into that. We're tasked in this group to ensure that the policy enables us to

perform whatever purposes in use cases that are appropriate in the ICANN policy space. And the UDRP, in this case, in one.

And so, what Jan is talking about is that in order to prove bad faith, it's been recognized since, whatever, 20 plus years that you can use the fact that someone has registered multiples domain names that are infringing as proof of bad faith under the UDRP. And so, this is really the question of correlation.

And Steve's exactly right. It probably needs to get separated from the anonymous contact discussion, but there is a definite need to be able to support the use case in the UDRP. We've heard nothing that suggests that it's inappropriate to do so. So, at some point, we should talk about how to do that.

And essentially what you're talking about is getting a list of domain names that are registered by a particular registrant. That's really at the crux of what you're trying to do when you're trying to prove bad faith under the UDRP. And a list of domain names per se isn't personally identifiable information, and so we should find a way to be able to incorporate that into our policy.

KEITH DRAZEK: Thanks, Margie. I appreciate the intervention and clarification of the issue. There is some activity in chat right now, and so I don't know if anybody else would like to weigh in at this point. The floor is open.

So, as I'm quickly reviewing the chat, it looks like there's some question or concern about whether that's in scope and whether … Let's see, I'm just scrolling here, excuse me. Yeah, so I'm just

going to pause and see if anybody else would like to get in queue. I think there's some question here about whether … Well, let me back up.

So, clearly there is a distinction or a different between contactability and correlation. Right? And the ability to produce or secure data beyond the contactability of the registrant. And so, I think that is a fundamental issue. I think, for the purposes of our discussion today in Phase 2A …

I think Steve has identified the conflict between having an anonymized of pseudonymized contact. And then I think Becky reinforced her view on the relation to privacy implications.

I've got some folks in queue now. Thank you for bailing me out. Owen and the Chris.

OWEN SMIGELSKI: Thanks, Keith. I think the concern that we're having here about having a unique contact or the ability to correlated bad faith with multiple domain name registrations for UDRP purposes is that that was never a thing before Temp Spec. It seems to be this discussion, and there was also in Phase 2 as well, too, about features that seemed like a reverse WHOIS search.

Let me just remind everybody, that was never a function of WHOIS. There were some third parties that improperly scraped WHOIS and provided some outside tools, but that's not something for us to solution. If you want to find bad faith in UDRP decisions, you can search the public available UDRP decisions, but let's not conflate the contactability of an individual through a domain name

registration with the ability to determine bad faith or cybersquatting intent here. That's outside of our scope, and it's not anything that we should contemplate or even attempt to do. Thank you.

KEITH DRAZEK: Thanks, Owen. Chris, you're next.

CHRIS LEWIS-EVANS Thanks, Keith. And hello, everyone. Just on that. I think we're talking across each other a little bit here. And what we're talking about here is purposes, not functions, of the system. So, what we're looking at here is what is the legitimate purpose for processing this data. And there are purposes other than contacting the registrant, and a number of those purposes will not have direct effect on that registrant. So, that's, I think, where we're talking across each other.

There are going to be purposes that do have direct impact on the registrant. And those have some of the higher risk attached to them, I would suggest than those that don't which, obviously will have that lower. So, I think while we're thinking about this, maybe we could think in those terms rather than attaching functions that aren't part of this. Thank you.

KEITH DRAZEK: Thank you very much, Chris. Brian, you're next.

BRIAN KING: Thanks, Keith. I thought that was well said by Chris. We're not trying to … I think we're all aware that there was no reverse WHOIS previously. And I can be brief because [Mark] made the good point in the chat. It's common that a trademark owner would identify hundreds or thousands of potentially infringing domain names and then pull the WHOIS for those as part of an investigation and prioritize their activities based on if any registrant was in a pattern or practice or had a number of infringing domain names.

So, that's gone now. Right? The Temp Spec wiped that out, the ability to get that data [inaudible]. What we're looking at is if there's a possibility that doesn't run afoul of data protection law that some identifier can enable that type of activity. So, that's what we're looking into here, I guess. Just to be clear. Thanks.

KEITH DRAZEK: Thank you, Brian. And I'm going to pause here. If anybody else would like to get in queue, the queue is open. I'll just take a moment to remind everybody, please set your chat function to All Panelists and Attendees. And I'm going to turn back. I know there's been quite a bit of activity in the chat, but I'm really encouraging folks to put your hand up and speak to the issue. This is an important discussion, and now is our opportunity to hash it out.

Okay. Margie, go ahead.

MARGIE MILAM: Hi. The other use case that I think is relevant for this discussion is also in the DNS abuse world where you may identify a domain name that's being maliciously used for malware, and the ability to identify other domain names registered with that same contact to be able to stop the malware from proceeding is exactly why we have this issue of asking about having some sort of unique designator, or whatever you want to call it, to be able to enable that.

KEITH DRAZEK: Thank you, Margie. Milton, you're next.

MILTON MUELLER: Yeah. So, I think Steve did us a favor by separating these two concepts of the contactability and the correlatability. The problem I have with correlatability is that if the identifier may not be the person's name. But if, indeed, it identifies every domain name registration this person has made, it is in effect a … That kind of correlation is a personal identifier. So, if that is published on the web, I understand the value of that for cybersecurity researchers as well as for law enforcement and for trademark people. But it's also extremely valuable for the bad guys in a number of ways. So, unless that date is not published, I think it's completely off the table as something we can do and comply with GDPR. I thought would have already been decided, actually.

KEITH DRAZEK: Thanks, Milton. And look, I think that is the key question here for this group under the Phase 2A work, is the question of feasibility;

and feasibility specifically in light of GDPR. Right? And so, I think Steve's intervention early on was sort of an important distinction. Obviously, there may be some use cases or some value, but in the context of the work of this group, we have to figure out whether what's been proposed is feasible under GDPR. And I think the responses from Bird & Bird on this—and Becky, feel free to jump back in here at any point if you'd like.

But I think we are seeing that there is, I think, a pretty clear challenge around the feasibility of this under GDPR as it relates to privacy. And contactability is one thing, and correlation is clearly another at this point.

Would anybody else like to get in queue on this? Milton, go right ahead.

MILTON MUELLER: Just a quick comment. So, for trademark owners, their key for wanting a search and wanting identification is going to be the actual domain name and whether it infringes or whether the content on the domain …

So, if these domains are correlated … Let's say some type of squatter registers 16 different variations of Facebook, you're going to get the correlation anyway. For cybersecurity researchers, of course, it's very different. The command-and-control infrastructures are not going to register identifiable domain that say, "We are the command-and-control infrastructure for XYZ."

So, the correlatability has greater value there, but I don't see how, again, you can publish that data for those few cases of

infrastructures for cyber attack without also publishing what is, in effect, the personal e-mail of every registrant in the Domain Name System. I just don't … I think you have to separate those two things, and you can't do that.

KEITH DRAZEK: Thanks, Milton. Margie, you're next.

MARGIE MILAM: A couple observations. And I haven't really thought it through, so I'm just putting it out there. There is value in this sort of identifier even if it's not published. In other words, if the cybersecurity expert would make a request based on, say, the one domain name that's obviously being used for malware and then on request able to get the [fulsome] list, that's still a better situation than what we see today.

And that's part of that problem, is that today you're basically in the blind, if you will, unable to fully appreciate the breadth and scope of the domain names that are being used in a particular malicious attack. So, I just would like to have the group not immediately reject the idea, but think about the ability to help protect again security incidents and see whether there's a way to consider it even if, perhaps, it's not published.

KEITH DRAZEK: Thank you, Margie. Volker, you're next. And I see that there's also some chat going on, on this subject, and some dialogue taking place. Feel free to bring that to the phone, folks. Volker.

VOLKER GREIMANN: Yes. I understand why correlation is helpful for many parties, and I absolutely have sympathy for that. The problem is that the same tools of correlation are also available to bad actors. People are getting spammed because of their domain name registration. People are getting doxed because of multiple domain name registrations that they might hold.

There are not theoretical cases. These are people that have happened and are still happening in some certain cases. One of our members has been inundated with robocalls because of data that has been available in WHOIS for a while.

So, there are issues with that. So, unless we can fix those issues and exclude the bad actors and allow only the good actors access to that kind of data, I don't think we have something that can be discussed here, that can lead anywhere. Ultimately, I'd rather have 100 domain names that are abusive than 2 customers that are negatively impacted by any disclosures or any harmful effects of this kind of usability of the system.

The second point that I wanted to raise. A lot of registrars, this one included, that are worth their salt when they're looking at abuse have an interest in doing this kind of correlation themselves. And they have that data. They have access to that data because, frankly speaking, it saves us money if we do that. If we get a

number of requests that are in a similar pattern, we start looking if there are not other domains that match the same pattern and take action proactively against those domain names as well. Because, obviously, I'd rather turn off 100 domain names in one fell swoop than receive 100 tickets over time that deal with those domain names.

That kind of thing saves us money, and therefore maybe we should provide more guidance for registrars on how to do that, that are not able to do this themselves or have not, basically, the right tools available to them; or offer them educational materials why it's in their best interest to do this kind of action themselves. And obviously, that is not visible. It appears in no statistics on abuse fighting, but that's something that a lot of registrars actually do.

And therefore, if this is handled by the registrars, a certain need for third parties to do this kind of stuff goes away. And I'm not going to try to cost people their jobs, but effectively, that is what it boils down to. If registrars do this right— and there are all kinds of incentives for us to do so—then certain parties, certain providers, cease to provide any additional benefit. Thank you.

KEITH DRAZEK: Thank you, Volker. Hadia, I'll turn to you next, but I just want to note that we'll probably need to move on from this topic on our agenda here in the next 5 or 10 minutes. And this isn't the last time we'll have an opportunity to discuss this, but I just want to remind folks that we do have the Bird & Bird memo, the guidance on this. And I think, really, what we're talking about here is the

feasibility of unique contacts under GDPR. And then we need to make sure that we're addressing that specific question as we prepare for the initial report.

Hadia, go ahead.

HADIA ELMINIAWI: Thank you, Keith. So, I raised my hand to say that, actually, Margie's idea of having a registrant-based e-mail contact that is not being published is worth exploring. So, I think it is worth looking into what would be the benefits of having such a registrant-based e-mail address that is not published, and the feasibility also of this. So, that wouldn't be in violation to GDPR. But again, let's look if this would be useful, and how possible it is. Thank you.

KEITH DRAZEK: Thank you, Hadia. Would anybody else like to get in queue? So, I guess what I'm also hearing is that there's some discussion here about unique identifiers. And I think there's a distinction between a unique identifier and a unique e-mail identifier or contact. And I think we need to make sure that we are talking about and considering the same thing as we figure this question out and the response and where we want to include or incorporate anything in the initial report.

I know there's been some discussion about the benefits of having the ability to correlate registrants across registries and registrars, but again, are we talking about an e-mail address that potentially is personally identifiable? Is it something else? Does that even

matter? I think these are all important discussions, but we need to remain focused here on the question before us in our charter and what we're trying to accomplish over the next four or five weeks.

Brian, go ahead.

BRIAN KING: Thanks, Keith. So, you raised an interesting point there. Given the way that the EPP works, in that before a domain name is registered, a set of contact data is registered with a gTLD registry, and then the EPP sends a create command that connects the domain registration to that set of contact information that's already been registered with the registry. I mean, it happens in milliseconds, but in the order of operations, the contact set is registered first. It could be done at registry level.

It could be done, meaning an anonymized identifier could be established at the registry level and then have the domain name tied to it. And then the aggregate could be done at the RSP level as defined in the Subsequent Procedures Working Group. So, as we see consolidation in the industry, it could really have a unique identifier per registry service provider, narrowing down to … Verisign could do it one way and Donuts could do it another way and CentraNet could do it another way.

It would be tough to conceive how you could have one identifier across all gTLD domain names, but it could certainly cover a lot of ground if you did it that way at the registry level. So, food for thought there. Thanks.

KEITH DRAZEK: Thanks very much, Brian. And look, I think what we're acknowledging or recognizing here in this conversation is that there is legal feasibility under GDPR. There is the technical feasibility in terms of, as Brian sort of introduced, the EPP commands that are used, the interaction between registrant, registry, and registrar. And let's not forget that there are resellers in there occasionally.

So, there are couple of different aspects to feasibility, but again, what we're tasked with here is trying to determine whether unique contacts and unique e-mail contacts are legally feasibility under GDPR. And then I think the technical feasibility is related, but perhaps secondary at this point.

I'm going to reopen the queue here if anybody else would like to get in. Let's give it another five minutes max if needed. And then we will move on to our next agenda item. And again, we will have more opportunity to discuss this, but thank you.

Brian, go ahead.

BRIAN KING: Thanks, Keith. Yeah, just to kind of conclude. I think where we're landing on the charter here that's on the screen is the bottom left quadrant. It seems to be where folks are coalescing, and we might be able to find consensus so that whatever anonymized identifier is tied to the registrant. And it would be easier and better for us, I think, if we lived in the top left quadrant there with that begin published.

But, hey, through the SSAD or “available upon request” would still be a helpful way to do this. So, negotiating against ourselves, perhaps, but in the interest of trying to find consensus, I think the bottom left quadrant is where we can probably find some consensus. Thanks.

KEITH DRAZEK: Thanks very much, Brian. Much appreciate. Volker, go ahead.

VOLKER GREIMANN: Yeah. Almost there with Brian, but I think he misspoke and meant the bottom right, of course, because as I outlined before, there are so many risks associated with the bottom left one that would need to be take care of as well. and I have not heard any single proposal that would basically protect registrants from abuse of that kind of functionality. So, the bottom right it is.

KEITH DRAZEK: Thanks, Volker. Brian, do you want to get back in? I want to make sure that we’re not talking past ourselves and that we’re all saying what we mean and meaning what we say. So, Brian?

BRIAN KING: Sure. Thanks, Keith. I think Volker’s being a little cheeky there. We would prefer to be in the top left, and I think some registrars or others may want to live in the bottom right. So, the proposal is that we meet in the bottom left. Thanks.

KEITH DRAZEK: Thank you, Brian. Okay. Would anybody else like to get in queue on this? I think there's more work that we need to do here on this topic, but we probably need to take this to the list and to schedule some further discussion on this for a future meeting. Let me pause and see if anybody from, either, staff would like to interject here. Or, Becky, if you've got any wrap-up words for us on the feasibility of unique contacts, you're welcome to weigh in. But I just want to pause and see if anybody else would like to speak to this.

Okay. Not seeing any hands. Nothing further from Becky. And I guess, again, we need to get back to question of whether what we're talking about here is guidance or a requirement, at some point. But let's table that for the moment so we can move on.

All right. Thanks, everybody, for your input and engagement on this one. More work to be done, clearly, but I think now that we have the Bird & Bird memo, we're in a position where we can take the next step on this one.

Okay, let's move on, then, to item #4 on our agenda which is the topic of legal and natural. And, again, what we're trying to assess here is whether voluntary recommendations and/or changes to consensus policy are needed or are warranted. And I think, at this point, we will turn to the document that folks have provided input to. Again, thanks, everybody for your input and for concluding and contributing to the homework assignment.

And so, let's just get right into it. Again, the question here is whether any updates are required to the EPDP Phase 1 recommendations on the topic. And I'm going to get out of the way of this discussion here and hand it over to Melina if anybody would

like to get in queue. I would encourage folks to present or summarize briefly your input. If there are any questions or comments that folks have for clarification, feel free to use this time.

But, Melina, let me hand it to you. Thanks.

MELINA STROUNGI: Thank you, Keith. Do you hear me well?

KEITH DRAZEK: Yep. Hear you great, thanks.

MELINA STROUNGI: Great. First of all, I would like to thank everyone for their efforts and time devoted to the process and in the document. I think I need to make a small intervention as we're approaching very fast to the May deadline. So, we may want to be very wise on how to make use of our remaining time.

So, Keith, just to build on your earlier point, I think it is really good to remember certain standards of good behavior. Even in times where we disagree with each other, I think it is I really important to try and remain respectful. And I was sad to see that …

I acted in good faith, for example, when Volker had asked to explain why WHOIS data are important for DNS abuse, and I spent time drafting, coming up together with statistics, figures, reported problems. And within a few minutes, he dismissed

everything as alleged facts, even doubting that the DNS abuse exists, that sky has not fallen.

Are those perpetrators for child abuse cases registrants? Yes, Volker. Perpetrators, indeed, may be registrants. Children abuse cases are real. They're not make up. Complaints are real. Phishing and malicious activity are real. DNS abuse is a real issue. So, it is your right to say, "I simply do not want to differentiate. End of story." But please do not allege that such an important issues as DNS abuse is not existent. I find it disrespectful for all these people from all over the world who are really working hard on this.

So, on a way forward, I really wish that everyone tries to be more respectful and more polite towards one another.

Now, having clarified this, I was thinking, "What is the best way from us to benefit from the remining time that we have in Phase 2A?" Some contracted parties are not convinced that we should make a differentiation requirement. Volker's position has been quite clear on this. He often brings examples on how things are in Germany. He has clearly stated that he will only differentiate if this is a legal requirement under German law. I don't know. So, I perceive this that he prefer to be regulated than self-regulated. It seems so.

This is fine, and I really respect Volker's decision to be regulated. This is, however, only one voice. We are here to make global policy for all contracted parties, so I think it would be very useful to hear, today, also other contracted parties' voices. I recall some very nice comments from contracted parties which go at the heart

of the issue. They are asking a very important question. “Why should be differentiate? It seems to benefit everyone else but us.”

So, contracted parties do acknowledge the benefits that the differentiation would have for the wider community. But they are asking, “Okay, but what’s in for us?” This is a very valid point. This is a very constructive point. So, I suggest we focus this meeting, indeed, to explore together what will be the benefits of making a differentiation requirement. I can name a few.

For instance, by differentiating, we can diminish the number of access requests that you receive. We know that in the past, and I believe this is a point also made by [Marby,] there were concerns that when receiving an access request, you may have to do the balancing test. And there’s a lot of unclarity, a lot of stress on how to carry the balancing test correctly, whether or not a request is valid to disclose personal data or not.

Making the differentiation a requirement would relieve lot of such stress and uncertainty. It would really diminish the number of requests you would have because, according to the data we have, the majority or registrants are legal persons. They're not natural persons. So, this means that it would make your everyday life easier.

Another advantage is reputation. There is currently a lot of implications that the current practices are lacking transparency. So, really, differentiating would be a very positive step towards transparency.

Another important benefit would be self-regulation. This is a great opportunity for you to influence things. We're at a very critical moment now where a certain proposal has been made. And before making it into a law, you have a great opportunity to take control and influence things. You have the opportunity for your voice to be heard.

I want to share with you the following information. While you are fully committed to the EPDP multistakeholder model, you should be aware that from the messages and questions we receive from the legislators, we may not exclude that the current requirements may be even more prescriptive or more strict than what is currently stated in the NIS proposal.

So, what is best? If May approaches and no consensus has been reached, I think this will be a pity. It will be a missed opportunity. So, I would like to ask contracted parties the following. Could all these benefits make you consider making differentiation a requirement? How about other benefits or financial incentives? I think it would be very productive if we can discuss on possible ways, financial incentives and other ways to make it more appealing to them to differentiate. Thank you.

KEITH DRAZEK: Thank you, Melina. And thanks for your last question there about what could be done whether it's incentives, or what might shift the consideration for contracted parties. And I think that's a reasonable question to ask. Thanks for your intervention.

Volker, I'll turn it to you and then to Milton.

VOLKER GREIMANN: Yes. Thank you, Keith. First of all, I did not want to appear dismissive to Melina and her arguments. If she made any arguments regarding statistics of abuse that have increased over the past three years, then I have not seen that. I must have overlooked it. I'm checking my e-mails now, but I'm still not seeing that. Yeah, but it wasn't intentional. So, that as a preface.

Obviously, we prefer self-regulation and, as you have probably seen, I have made a very concrete proposal of how we would see publication to go ahead which is consistent with existing European legislation which is already implemented in many member states as de facto disclosure process for publicly available information. There is no one in Germany that would state that the information in the trade register or in the land register is not publicly available, yet you cannot get it in an automated fashion without telling someone who you are and paying a nominal fee for that.

I see no problem with implementing this here, as well. This is de facto in EU law. This is what member states are doing, and I think following that example would benefit us because that would mean that we wouldn't reinvent the wheel. We have the benefit of strengthening SSAD for other purposes as well, lowering costs for other requests. There are so many benefits to my proposal that I don't really understand why this is not being accepted or at least followed up on with more enthusiasm.

And speaking of regulations coming from the EU, I have just one question which may be beside the point but still interesting to me. Why are you not proposing the same kind of regulation for

hosting? There is quite a difference between what registrars and registries are supposed to do compared to what web hosts are supposed to do with their registration data.

I don't see any requirement to put hosting companies on the spot to require them to publish their customer information in some kind of database. Why not? They have the content. There's the infringement. That's where you should go. Why come after us?

KEITH DRAZEK: Thank you, Volker. If anybody would like to respond to Volker's questions, feel free to get in the queue. I have a queue building. Milton, Mark SV, and then Alan.

MILTON MUELLER: Yes. So, I do want to respond, in some ways agreeing with Melina's somewhat pointed message, and disagree with certain elements of it. What I think we need to pay careful attention to is the belief that we can settle this within ICANN's self-regulatory framework. I think this is a very important point.

I'm not terribly pleased with the implied threat that if we don't resolve it here in a way that certain governments don't like, that they will supersede us. But, in fact, that is indeed a threat that we need to take into account. And I don't see any reason why we can't try to find a consensus solution within the framework of ICANN which will be global in effect and uniform across all jurisdictions. And I think that's something that we should strive to do, so I totally am on board with Melina on that particular issue.

The other thing I'd like to say, and will probably irritate all of you, is that the stakes of this are probably less than many people believe. There are so many ways of getting information in the digital environment. You can get my home address in so many ways from so many data brokers. The historic WHOIS data is being commercially marketing all over the place in, indeed, all kinds of databases.

And Volker raises a good point that there are all kinds of other Internet services that are also points of abuse or crime or attacks which, in many cases, might be much more helpful. And we shouldn't try to load everything onto DNS.

So, let me conclude by saying I have tried to explore a space for agreement, and I articulated those principles. Principle one was that there should be some kind of differentiation between legal and natural. And I thought that Volker's idea of, yes, we differentiate but then we put everything behind the SSAD and then we have automated disclosure for members of the SSAD, was a very good idea that we should be taking seriously because I think it gives almost everybody what they want.

Automated disclosure means that you will get all the legal person data quickly and efficiently, and it won't be published for any bad actor to use. And if they do turn out to be bad actors, we can kick them off the SSAD. So, what's wrong with that? That seems like a pretty good middle ground solution for people to explore seriously. Thank you.

KEITH DRAZEK: Thanks very much, Milton. And I think the point that you've made right at the end there, if I heard it correctly, is that there is a proposal on the table that is probably or perhaps as close to a compromise solution that we may find. That there is an acknowledgment that differentiation is worthwhile or doable, but the question is about access to that data. And I think that's an important consideration whether we talk about publication or providing data on request.

We do have an SSAD recommendation that is currently with the Board. Obviously, it's going to go through an ODP (Operational Design Phase) Review. It's not done. It's not finalized. It's not in place. But I think it is something that we need to consider as a possible path forward.

Let me stop. I see Alan has his hand up, and I'm going to go Alan. And then we're going to go back to a more orderly review or presentation of the various points that were submitted by the different groups. So, we'll go back to the chart, the table, and the Google Doc where everybody has provided input, and we'll go through, more methodically, a very brief presentation from each group as to the input. So, a three- to five-minute summary from each group as we go through to set the stage for further conversation.

With that, Alan, go ahead.

ALAN GREENBERG: Thank you very much. Two things. Number one, I strongly support Milton's proposal—certainly his principle #1—that is clear that a

legal/natural distinction must be made. However, I haven't heard that agreed to by the contracted parties. If there is general agreement, let's get that on the table and make it really clear because what I'm hearing is that some contracted parties may identify things [where] each piece of data is public, but not do the legal/natural distinction for the registration itself and for the registrant. So, I think we need some clarity on that.

Number two, the discussion on the SSAD, I feel, is a complete red herring. If we're going to use the SSAD which has all sorts of complications association with it and we put some pretty stringent rules in—in Phase 2, in terms of what registrars must go through to make decisions—I don't understand, once one knows which data we can publish and not, why a simple vanilla RDAP server does not give the same thing.

In both cases, it's going to end up going to the registrar through an RDAP interface, presumably, and I don't know why we're talking about using the SSAD when the communication paths can be replicated without all of the complexity that we built into the SSAD and without all the cost; and more important, without the multiple-year delay before it actually exists.

So, we're talking about a mechanism of how to do it instead of what is allowed in the policy. So, this is a PDP looking at policy, not building a mechanism. So, I really wish we could focus on the questions at hand and not go off on extraneous other areas which may or may not be implementable in the long term. Thank you.

KEITH DRAZEK: Thanks, Alan. So, just in quick response. I think we're not trying to design spec for the system, necessarily, but I think that in order for something to be feasibility and implementable, we have to consider how we might achieve these things under GDPR. Right? In my view, you can't completely separate the discussions of a policy with the implications for implantation and these questions that are being asked.

And apologies if I got ahead of myself or misspoke on the topic of differentiation. I see there's some feedback for me in chat there.

ALAN GREENBERG: Keith, may I reply to that?

KEITH DRAZEK: Yeah. Go ahead, Alan. Thanks.

ALAN GREENBERG: Yeah. Yes, the registrar will have to decide, "Is this request for data that I can release or not?" But that doesn't have to be done through the context of the request coming from the SSAD. The complexity is all on the central side, either both an SSAD request and a simple RDAP request. Right now, if I go to whois.icann.org and do a request, it gets translated into an RDAP request and it comes back with some data which may have information in it or it may not, depending on a decision the registrar has made on what to release—the registrar or registry.

That doesn't need the SSAD to work, and it works today. So, I really think it's a red herring to be talking about the details of the distribution mechanism and not the policy as indicated by Milton's principle. Have we agreed that the legal/natural differentiation should be made? I haven't heard that, and that's a [risk]. That was the question in our charter. Thank you.

KEITH DRAZEK: Thanks, Alan. That's well said and a good point. So, Thomas, Volker, and then I do want to go back to an overview of each of these respective inputs. Thomas.

THOMAS RICKERT: Thanks very much, Keith. And hi, everyone. I thought that we had a very constructive communication on the way with the distinction between personal and non-personal data. Let's just remember and try to analyze what we did. A lot of folks are doing the distinction between legal and natural because they think that legal data, per se, is not to be protected. And we found out that part of the data of legal entities is actually personal data.

So, we were talking about it a two-step approach by which we asked the registrant to self-identify as either a legal or a natural person. And if they say they are legal, then we still ask whether personal data is involved or not. So, basically, it is all about the distinction between personal and non-personal data. And maybe we do ourselves a service in the spirit of converging to consensus by focusing on the first point.

And I think if we did so, if we back that up with a proper mechanism to provide consent, then I think we would achieve the same compliant result as if we were going through additional hoops that cause problems in our consensus finding.

KEITH DRAZEK: Thank you Thomas. Volker, Melina, and Laureen. Go ahead.

VOLKER GREIMANN: Yes. Thank you, Keith. Alan makes a couple of good points in that he's right in many aspects that, obviously, some aspects of what I'm proposing go beyond what we are tasked to do. However, that should not stop us from at least considering what I'm proposing because in many ways, it's solves a lot of the issues that we are discussing. Instead of having a piecemeal solution that addresses some of the issues and others are not addressed, this proposal basically serves to resolve all the issues, provide a compromise that allows access to certain points of data which [inaudible] would probably still have to be detailed in further discussions.

But if we have a mechanism in place how we can agree and how we can envision this disclosure to happen, the question of what is going to be disclosed is going to be a lot easier. So, essentially, what I'm saying is, let's not try to have a broader look at things and make sure that basically we do not see the forest for the trees. We are focusing on the very small trees, but we actually need a solution that fits the purpose.

And, yes, he's right. SSAD is a couple of years out, probably. I can't imagine certain scenarios where it happens next year, but that's [inaudible].

But I don't want a solution that's sub-optimal that works for a couple of years and then think that there might be a better way to implement it through SSAD and then have to redevelop it again. Let's focus on what is practical, what is implementable, what is reasonable to implement—economically and technically as well.

And if that takes a little more time to become a reality, then that is probably going to be the case. But if we have a solution that in the end satisfies more parties than any stopgap solution that might be a minimum consensus but basically does not address any of the concerns and makes no one happy, then I'd say wait a year or two and get a better solution in place. Thank you.

KEITH DRAZEK: Thank you, Volker. Thomas, I think that's an old hand if I'm not mistaken. Let me know if it's not. And then I have Melina and Laureen. And then we're going to go back to … I will draw a line at this point, and we're going to go back to the discussion of the question before us on the screen and in the agenda which is the difference between recommendations versus consensus policy.

So, Melina, then Laureen.

MELINA STROUNGI: Thank you. And thank you, everyone, for your points. Just to note that, indeed, we have the option to wait for two years. But just to

bear in mind that maybe, in the meantime, we will have legislation in place and there we will not have room to influence anymore the process.

While really, if we benefit from the time now until May to come up with something that pleases, ideally, everyone in this group—or at least most of us—it would be a significant progress and it could really influence the legislation process while the other way around, it might be too late anymore and then you are left with whatever legal requirements there are at the time.

It may be different for members states, different for each country. Some may be stricter than others. Some registrars may be found at a disadvantage as compared to others. So, I really want to avoid this scenario and hopefully come up with at least some basic … Because, indeed, I agree with Volker's point that some things go beyond this Phase 2A. We cannot address all the details and the technicalities, and we don't even have the time to do it even if we wanted. So, at least I think it would be beneficial to start by agreeing on some basic principles such as the ones proposed by Milton.

I also want to make a point regarding Volker's proposal on the SSAD. It's not that we didn't take it into account or that we are not willing to take it into account. Let's agree that, okay, we have different interpretations on what publication means. That's fine. In any event, though, even if we use the SSAD for disclosure, you cannot skip the step of differentiating between legal and natural entities.

Even in the scenario where you decide to go with disclosure by the SSAD, you cannot skip this first step. There is a reason why privacy legislation makes this distinction. If you notice in the recitals of the GDPR, it doesn't say that the GDPR does not apply to data of legal persons. It says that it does not apply to personal data of legal persons. The legislator acknowledges that there are certain data of legal entities that may be personal, and it's a conscious choice to make a distinction between legal and natural entities.

What we've proposed is basically to always have the first level of differentiation between legal and natural and treat all data of natural persons—well, as personal as they should be and be fully redacted. While, in your example, if you skip the first step, you lose the safety net, let's say. So, let's assume you do not ask the registrant, "Are you a company or are you a natural registrant?"

Let's assume you have a natural registrant who is not knowledgeable of GDPR and self-identifies some of their data as non-personal data while in reality, they are personal data. And then you get a disclosure request via the SSAD, and you automatically disclose this data because they are flagged as non-personal. What would have happened then? You will have accidentally disclosed personal data of a natural registrant. In my view, the liability of contracted parties in that scenario could be much, much, much, much higher than the solution that we are proposing. Thank you.

KEITH DRAZEK: Thank you, Melina. And Laureen, you're next. And then we're going to move back to the other section of our agenda.

LAUREEN KAPIN: Sounds good. I wanted to follow up on some of the comments by Thomas and Melina, and make sure I'm understanding the scenario. Thomas had talked about giving consent if a legal person is involved. And I may have misunderstood, and Thomas could respond in the chat if I have misunderstood.

My question is, shouldn't the issue of consent only come into play when we're talking about personal data? And as a necessary correlation to that, when we're talking about legal entities and their data which is not personal data, shouldn't consent be nonapplicable? And shouldn't there be no barriers to that information just being published in the available registration data information?

I fully understand the need to protect personal information, and indeed I don't think there's anyone in this working group that would disagree with that. What I don't understand is the inclination to protect information that is not protected under the law and which is not personal information. And that's where I really would welcome some very specific discussion of why there needs to be extra protections grafted to deal with the non-personal information of legal entities.

KEITH DRAZEK: Thanks, Laureen. I see that Thomas has typed—

LAUREEN KAPIN: Great. I'm happy to hear that, or see that.

KEITH DRAZEK: Yeah. He's typed into chat but also put his hand up. So, Thomas, in response to Laureen, go ahead. Hadia, I'll turn to you then. And frankly, at this point, we've only got 15 minutes left on the call and it may not be conducive to go back to the question of the distinction between voluntary versus requirement. We may have to schedule that for our call on Tuesday because we've got … Every group needs to provide its summary, its overview, and input. And we simply won't get to that today.

So, Thomas, in response to Laureen. Then Hadia.

THOMAS RICKERT: Yeah. Thanks for the opportunity, Keith. And, Laureen, actually no consent is required where the data of legal entities not containing personal data is present. In fact, there would be risk in asking for consent where none is required. There is a Spanish supervisory authority which has actually sanctioned the company that was using the wrong legal tools, or the wrong legal basis.

So, I've said this on other occasions as well. We should make sure that where, let's say, data of legal entities is publicized, that we actually do not ask for consent in any shape or form. Only where personal data is required, we need to make sure that we do this in compliance with Article 7. And where the data is not

obtained from the data subject itself, it becomes a little bit more complex and then we would need to invoke Article 14.

So, there are legal mechanisms in order that, but under no circumstances should we ask for consent where none is needed.

KEITH DRAZEK: Thank you, Thomas. Laureen, would you like to respond?

LAUREEN KAPIN: Yes. In my view, if we can separate out these two scenarios … I understand that there are complexities and we have some disagreements on how to treat the personal data of legal entities, but might be agree on how we can treat the non-personal data of legal entities, if we could at least move forward on that, I think it would be quite productive.

KEITH DRAZEK: Thank you, Laureen. I'm going to turn back to Hadia. And then, Volker, I assume you want to respond as well. Hadia, go ahead.

HADIA ELMINIAWI: Thank you, Keith. I just wanted to note that any guide we provide needs to be based on the information we have, not, of course, based on our wishes or what we would like to happen. And currently, we have legal advice that shows if contracted parties are to publish data based on whether the data includes personal information or not puts them at a higher risk than if they differentiate between registrant types first.

Also, we have a study, the ICANN study, who looked at ccTLDs that differentiate. And, yes, we can say that ccTLDs are not like gTLD registries. But nevertheless, we did not find any of the registries that actually publish legal persons' data not differentiating between registrant types. So, that's one point.

And then I would like to quickly build on Milton's proposal and intervention which I thin is very positive, but there are a couple of points here. One, in order to automatically disclose the data, we will need to differentiate between the registrant types. Second, currently SSAD allows requests only from accredited users, so for SSAD to be used by nonaccredited users, a change in policy would be required.

Finally, adding cases to SSAD should not be a problem because we have the evolution mechanism. However, the evolution mechanism will not solve the policy issue in relation to who uses SSAC. Thank you.

KEITH DRAZEK: Thanks very much, Hadia. My understanding from Phase 2 SSAD recommendations is that the intent is for accreditation to be available to anybody who wants to access SSAD. But obviously, there are still details to be worked out there. Happy to be corrected if I have that wrong.

Volker, you're next. Go ahead.

VOLKER GREIMANN: Yes. Thank you. In a way, that is correct. We might need another PDP, but I have no doubt in my mind that if we chartered a PDP that basically had an agreed outcome where all parties would be more or less aligned on pretty much the details—and those could be worked out, outside of ICANN or as part of a pre-PDP group or what have you—then the actual PDP could be conducted in record time. Maybe not a day, but record time, nonetheless. Let's see how the Transfer PDP goes where that version happens, but I guess that one will probably be one of the fast ones, hopefully.

But that being said, I think policy being required for something is not necessarily a bad thing. It's something that we should, as a community, commit to and be happy to do because if there are policy that can achieve consensus, then by all means let's get it done.

KEITH DRAZEK: Thank you, Volker. Milton, you're next.

MILTON MUELLER: Sorry, Keith. We are never going to get to that last agenda item. Are we?

KEITH DRAZEK: On Tuesday, next week. Thanks, Milton. Go ahead.

MILTON MUELLER: So, let me just begin by saying that one of the reason I've decided to be more flexible about this issue is that in the real world, and not in the world of law, the distinction between person and non-personal data is increasingly artificial and blurry. That is, if you give me a bunch of so-called non-personal data like telephone numbers that you call or even where your packets go or all kinds of infrastructural information about what's happening, I can find out how you are and what you're doing—all kinds of things about it.

So, I think, yes, we want to respect the terms of the GDPR, but I think we have a little more flexibility to do so in ways that can, again, meet the demands of the different stakeholders here if all of them are willing to come to a convergence point.

So, here's the problem that I think we're running up against. It's probably correct, in Melina's reference to this Interisle Consulting Group. Maybe in some kind of formal sense, only 11% of the domains belong to purely natural person registrants. But in fact, there's this huge gray area of quasi-legal persons who are small businesses, people in their home office, and so on. And they may not want to be treated, informationally, as an [impersonal] legal person whose data should be completely open.

And that's why the second principle that I articulated, that it is putting the registrant in control of their self-designation as legal vs. natural and then having the two-step process, if they want to be considered a legal person, also allowing them to not publish certain sensitive information such as an e-mail address or a home address for a home office, this has to be in there.

So, that's why you have to go down the list and recognize that acceptance of each principle is a compromise and a balancing act for all of the stakeholder groups. So, I think that is very important to understand, that there is a very big gray area between legal and natural in which they might be formally or legally person but they're really at somebody's home office and they've just given themselves a name as a corporation.

And in many cases, they won't mind to have that information published. And in some cases, they will. So, we have to put the registrant in control.

KEITH DRAZEK: Thanks, Milton. Volker, I'll turn to you and then we probably need to move to wrap up in light of time. I'll make some closing remarks, but Volker, go ahead.

VOLKER GREIMANN: I agree with everything that Milton said. With regard to this so-called study that mentioned the 11% number, I think that study was deeply flawed in many aspects. It was paid for by self-interest parties that wanted a certain results, and that's the result it delivered. It clearly showed that they were not able to categorize over, I think, 60% of the number of domain names that they studied. And basically, the 11% is only of the ones that they were able to categorize. So, it's just a very small minority of domain names that actually became part of this.

From our own domain database, and other registrars in the group also look at theirs, this is a number that certainly does not bear

out. The number of personal registrations is probably higher than the number of legal entity registrations.

And to the point that was made earlier with regards to the differentiation between legal and natural persons, it's just sadly the fact that we cannot look at a certain data set and say whether it contains personal information or not. The only person that can tell us is the registrant.

So, I'm perfectly fine with having the differentiation, as Milton suggests, made by the registrant because that is the entity that knows whether their information is personal or not. Simply making the differentiation between legal or natural does not get us there. It's a step on the way that can help, and many registrars might be willing to do that as a first step on a voluntary basis, but I don't think we should mandate that.

I think, ultimately, being of no use for making the actual differentiation other than the preparatory step that can be helpful in certain circumstances does not really register it as something that should be required. It's something that can be recommended as a voluntary cation, but going beyond that, I have my doubt that we can get there. Thank you.

KEITH DRAZEK: Thanks, Volker. Stephanie, last word. And then I'm going to wrap things up. Thank you.

STEPHANIE PERRIN: Thanks. This is the crux of this whole argument. I, similarly, just like Volker … There are two issues here. The attestation of whether they're legal or natural—and I don't think that many of these folks in the gray area are capable of making that distinction, and I believe that the threshold of work—as I've, I think, put on the e-mail … We're really arguing about who's going to do the work of deciding, of explaining to the registrant whether they're a legal person or not. And this is a non-trivial question in countries that don't use the term "legal person."

And I just think that a focus on person information is so much more useful. It's still difficult. You still have to explain to people in much greater detail than we do now what data is personal and what isn't. For instance, the person registering the domain is unlikely to be well versed in data protection law, and may not realize that employees whose contact data they're releasing have data protection rights in many countries.

So, these are the things that we have to provide detailed guidance on, and I hope we get there soon. Thanks.

KEITH DRAZEK: Thanks, Stephanie. So, thanks, everybody. I'm going to wrap things up here shortly. Look, this has been, I think, a good conversation but I do feel like we're, in some ways, restating things that have been said before. I think some of the discussion today is actually reflected, captured, and has been incorporated into the write-up document. And so, we didn't get to that specifically as far as an agenda item, but I feel like that's what we

dealt with today primarily instead of focusing on the earlier topic of the distinction between guidance versus requirements.

So, look, good conversation but I really encourage everybody to focus on the write-up document and to identify any deficiencies, conflicts, any areas of confusion, anything that we need to work on together on the write-up document so we can start developing initial report language around the guidance language that we're talking about, the voluntary practices for registrars who choose to differentiate at this stage.

We do need, and we will circle back to the discussion of the difference between voluntary guidance and new consensus policy requirements on Tuesday during our next call. So, everybody please come prepared to talk about and to present your input to the table.

And I guess with that, I'm going to ask if there's AOB, any other business? Any final comments? Anything from staff before we move to wrap up?

Again, just to reiterate, our next meeting is Tuesday at 14:00 UTC. So, we're going to two meetings a week, moving forward over the course of the next month as needed. But they are on the schedule, and folks should be planning to participate twice a week on our plenary calls. And, again, as always, it's critical that folks do homework, contribute to the documents in the interim.

I don't see any other hands. Thank you all for your contributions today, and we will talk again on Tuesday. Thanks, all. Go ahead and wrap up the call.

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

[END OF TRANSCRIPT]