JULIE BISLAND: For the recording, this is Julie Bisland. Good morning, good afternoon, good evening. Welcome to the DNS Abuse Mitigation PDP 1 Working Group Call, taking place on Monday, the 20th of April, 2026. We did receive apologies today from Ching Chiao and Nitin Walia. Statements of interest must be kept up to date. Please raise your hand or speak up now if you have an update to share.

All right, all members, participants, and alternates will be promoted to panelists. Please watch your screen for the prompt. Observers -- oh, we have a hand. Farzi, go ahead.

FARZANEH BADIEI: Sorry, this is not a SOI, I think. I just joined an organization as a part of Digital Medusa work, which is called the Freedom of Future of Speech, which is based in Nashville. Thank you.

JULIE BISLAND: Thank you, Farzi. All right. All documentation and information can be found on the DNS Abuse PDP 1 Working Group Wiki space. Recordings will be posted shortly after the end of the call. Please remember to state your name before speaking for the recording. And as a reminder, participation in ICANN, including this session, is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct. And with that, I will turn it back over to you, Paul. Thank you.

PAUL MCGRADY: All right. Thank you, Julie. Let's get started, everybody. Welcome. I think we just did that. We're going to have an update on ICANN86 planning next, I think, unless there was something more to the welcome I was supposed to remember to do. Let's move on to the next slide. Oh, there was more for me to do. Here we go. ICANN86. I guess we felt welcome enough. So, we are having a prep week webinar on Wednesday, May 20th. This is to inform the community of our progress so far.

The idea behind these prep week webinars is we were spending a lot of time back in the day taking an entire session to update the community. Instead, we've kind of moved them forward so that people are better prepared to understand what it is that we're all talking about while we're there. We have four DNS abuse sessions. Two are on Monday, June 8th. You can see the dates and times there. If you can go ahead and lock them in. One on Wednesday and one on Thursday.

So, those are for us to get work done. So, please make it a priority to be there if you can. Let's move on. We have our strap. Do we do it again? I hope so. Strapwerson. Our strapwerson is back, Charter question number two. Just touching base on this one briefly. Let's move on to the -- You'll remember the charter question number two. Just this is just a quick review. What criteria should be used to define association between domains? What elements can be considered to establish such association? And then we go on to the strawperson.

We've added some new language here in green to reflect the working groups comments on the strawperson in our calls and on the list. So, I think it's worth reading through again. It's been a minute. So,

association between domain names should be determined using a flexible, non-exhaustive set of criteria that allows registrars to identify domains that are reasonably linked to the same abusive activity, account, or actor.

When determining association, registrars may take into account what is reasonably available to the registrar and differences in registrar business models the specific elements considered in any given ADC even within a single registrar may vary depending on the particular circumstances. Such association may include but is not limited to -- we have two to's there, we probably should fix that -- the following factors as applicable and as available.

Domains associated with the same account, customer, registrar, and customer are other potential common connection points. Domains exhibiting common patterns or indicators of coordinated activity, including naming conventions, shared infrastructure, for example, name servers and or campaign characteristics identified through internal analysis or external reporting. Domains linked through information reasonably available to register during its operation, including information derived from internal analysis and or external reports that provide indicators of what to look for in a campaign.

And I don't know if that is all. I apologize, I'm in a hotel in Illinois, and I don't have my second and third screen. Here we go. The policy should not prescribe a fixed or exhaustive checklist of association criteria, but shall be supported by non-binding guidance, examples, or advisories that can be updated over time to reflect evolving abuse patterns. This is in recognition that different registrars have access to different data and

technical systems and that abuse patterns evolve over time and that prescriptive requirements may become outdated.

The determination of association should allow for flexibility across different registrar business models and data availability and must be capable of being justified to ICANN Compliance as reasonable under the circumstances. At the same time, the framework should reflect that there may be a minimum or baseline expectation of checks using information reasonably available while preserving flexibility and how registrars implement those checks across different business models, recognizing that while account level association may serve as a useful baseline, it is not always determinative due to reseller models, shared data, and privacy services.

Okay. I think that takes us, if I remember correctly, takes us to the end. But if not, staff, please let me know or flip the next screen. Nope, that does. Let's go back up. I don't want to belabor this because we have talked about this pretty exhaustively. And the green language was meant to deal with everybody's concerns. But let's open a queue so that people don't feel we rushed through it unnecessarily. Also, let's not belabor it unnecessarily, but let's hear from all y'all. Okay, we have Reg and Farzi. Go ahead, Reg.

REG LEVY: Thanks. This is actually a pre-strawperson concern or question. When I opened this meeting this morning, it asked for my email, which it typically does not do. Is that a new requirement from ICANN or from Zoom?

PAUL MCGRADY: I don't know the answer to that because I had the same experience and was wondering if something had changed. And I was already coming in under the gun.

REG LEVY: We can wait for ICANN to weigh in.

PAUL MCGRADY: Okay. Reg, and by the way, this is a good example. One of the things I have to do is keep control of the queue, so if you have something additional to add, let's make sure.

REG LEVY: Right, yeah, can ICANN please weigh in on this?

PAUL MCGRADY: Yeah, Reg, this is what I'm talking about, right? We have to maintain the queue. So, when I'm talking, if you don't interrupt me, I'll do my best not to interrupt you, okay? All right. So, since I don't know the answer, Julie, your hand's up. Can you go ahead and tell us what's going on?

JULIE BISLAND: Yes, sorry. So, that was my fault. I was messing around with some settings. I forgot to change it back. I will fix that so that next week you are not expected to do that. My apologies.

PAUL MCGRADY: Thank you, Julie. All right. Farzi, go ahead.

FRAZANEH BADIEI: Thank you, Paul. So, while we think the language of flexibility might be appropriate in this context, we believe that there has to be some sort of transparency in the methods that are used in order to do the investigations so that the registrants and the end user and others know what sort of methods registrars use as much as possible, and we're not saying that they should disclose any kind of a method that can be abused or overcome by the, I don't want to use this term, like the malicious actor. But we think that there should be some baseline for transparency. Thanks.

PAUL MCGRADY: Farzi, before you go, help us understand more specifically what you mean by that. I mean, that sounds good, right? Does that mean transparency in how the advisories are built?

FARZANEH BADIEI: No.

PAUL MCGRADY: Okay, go ahead.

FARZANEH BADIEI: So, for example, it says such association may include but is not limited to the following factors as applicable. So, it would be good in the transparency reports to say that you what sort of factors they considered in that year or in that like within that six months. Also, domains exhibiting common patterns or indicators.

They can also say in their transparency report that what sort of factors they have considered including named conventions, was it shared infrastructure, was it campaign characteristics or all of them, and any other factor that they have considered. I know it's more work, but when we give flexibility and then there needs to be some kind of transparency on the method that they use.

PAUL MCGRADY: Thanks, Farzi. So, I think that that is a suggestion for an additional element in this, which is a transparency report from the registrars. Okay, great. All right let's capture that idea. Marc, go ahead.

MARC TRACHTENBERG: I guess just reacting to that initially. I don't really have any concern with the registrar being required to provide what factors they looked at, but I think that the registrar shouldn't be limited in what factors they can look at and there's no way to limit that. The register has the ability to look at whatever they want to when doing the ADC or conducting their business.

So, I think having the transparency requirement of what they looked at, probably is something for a different element because this goes to the question of how does ICANN track compliance with this, right? Because again, as I mentioned in the last call, this is internal. It's not transparent or visible at all to external parties or reporters. They don't know whether the registrar is conducting their ADC or not.

And so, this, I think, goes to a different question or a different element. But I can get on board with transparency. My point though is that I think this is going too far to taking into account the registrar business model. The RAA is registrar model agnostic and so should this be. Registrars have the option to do whatever business model they want, but the obligations are the obligations and they can meet them different ways. Just like in the RAA for the abuse mitigation obligations at 3.18, if you have a reseller model, you have your obligation as a registrar to conduct your investigation when you receive the report.

And to the extent there's actionable evidence, you have the obligation as a registrar to take reasonable mitigation efforts. Could you do that through a registrar? Sure. I mean, through a reseller? Sure. But the obligations are on the registrar and that should be the same here. And maybe in guidance from ICANN, it can take into account these different models, but in the rule itself, I just think it's got to be registrar model agnostic.

PAUL MCGRADY: Thanks, Marc. All right, we have Volker.

VOLKER GREIMANN: Yes, and I would like to give a small counterpoint to Farzi because as much as I sympathize with that, I do not want to be in any position that I give threat actors a guideline or a guidebook how to avoid our detections. And even in case where we take down a domain name because of these violations, because of certain pointers that we found, or because they had associated domains, we will usually not tell them what exactly led to the takedown, because then they will know what to avoid next time around, and we do not want to give them that kind of advice.

This is the same with the kind of people that contact us regularly and ask, I have a website that does this, this, and that, and we usually get fake reports. And would you take that down? And I'll tell them to look at our terms and conditions and our abuse policy, and reading makes them smarter. Because we will not tell them whether we will take that down. We will decide when we get the report. Thank you.

PAUL MCGRADY: Thanks, Volker. And yes, I think that we need to capture Farzi's idea to see if it fits into any of our charter questions. I don't think it fits here because right now, we're talking about association, not about reporting. But it's an important thing to grab. It's also important thing to grab Volker's comment about not building a roadmap. And it may be work that we don't even do. We'll have to go back through and look at the charter questions again or maybe work that we do. But I don't want to spend too much time on that. It's important we should talk about it, but it's not the subject matter question number two. Okay. Gabriel and then Brian.

GABRIEL ANDREWS: Just want to throw support behind what Volker just said. He took words out of my mouth.

PAUL MCGRADY: All right. Thanks, Gabriel. All right, Brian, and then Michaela.

BRIAN CIMBOLIC: Sorry about that. I thought I expected Gabe to be longer than two seconds. So, I'm coming off you. Hi. So, just to note, I think that this is sort of out of scope, frankly, particularly for this question, but overall. Transparency reporting is not currently required under the RAA. And as to whether or not there should be transparency reporting, that's a super valid question, but that's a much bigger question than the Associated Domain Check.

Currently, if a registrar suspends a domain, it's not under any obligation for transparency reporting on that. And the Associated Domain Check, really, it seems as though we're going down a path in which a registrar sees a malicious registration, checks, finds evidence of other domains engaged in DNS abuse, and then individually suspends those names under the existing obligations of 3.18.2.

So, it kind of feels like transparency reporting as it relates to Associated Domain Check is sort of distracting and not core to the question of what we're doing here. So, I think if we want to have a conversation on transparency reporting in general, I think that's a great community-wide

discussion, but I don't think it's particularly helpful as it relates to this PDP.

PAUL MCGRADY: Thanks, Brian. Yeah, and for clarity, when we come up with interesting ideas that we think require or should, requires is the wrong word, but that the community would benefit through discussing further, but they don't fit in our charter, we actually have a mechanism to capture interesting ideas that came up, but were not in our charter.

And part of our job is to feed that back to the GNSO Council small team on DNS abuse to see if they want to do something with that, including having those community conversations or they could do their own PDP on transparency, I don't know. But we're not the council. We're just us. All right, Michaela, go ahead.

MICHAELA SHAPIRO: Yeah, I'll keep it short and sweet. Michaela from the NCSG. I'm just following all of this discussion. So, agreed, a community-wide discussion on transparency. So, echoing Brian would be fantastic and happy to take that further. To your point, Paul, about whether this fits into this question or a later question, I would want to draw attention to question five of the charter, which is about if there is an adverse impact on registrants, are there corresponding remedies?

And to me, one thing that stands out there is how are you supposed to gauge whether there has been adverse impact if you're not aware, or how can you perhaps try to challenge or try to seek recourse for when

there is an adverse impact on your domain name if you don't have transparency around the grounds for which your domain was taken with the mitigation action. So, just thinking about maybe perhaps we need to be a bit more prescriptive and how we discuss what transparency means here.

And I would draw attention to where Reg very brilliantly through something in the chat that I highlighted about a difference between transparency the person who's affected and transparency to other parties, I personally think that's a very strong distinction that I would want to see us discuss further perhaps. But this could also come up in a later stage if needed in question five. So, happy to take that further. Thank you.

PAUL MCGRADY: Thanks, Michaela. Don't go away. So, I have a follow-on for you, which is a transparent report on a specific incident seemed to be different than what Farzi was talking about, which was more of a six-month or a one-year retrospective on the various tools used, basically what was the foundation or the fundamentals of how registrar went about it. Do you think those are two separate things or in your mind, are they the same thing?

MICHAELA SHAPIRO: Well, I don't -- and Farzi can perhaps respond to that better than me, but my sense, and again, Michaela, for the record, I don't think she was overly prescriptive in how we do this. I think it's just the point is that there's no wording about transparency anywhere in the strawperson up

at the moment. But I see Farzi's hand and I don't want to preempt you, Paul, but is it possible for me to pass on my time to Farzi?

PAUL MCGRADY: Well, I like to put people in the queue, but this is a short queue. We'll remember it when Farzi comes around. But let's go ahead. Anil's up next, then Marc, and then we'll hear from Farzi.

ANIL JAIN: Thank you, Paul. Anil, for the record. Here, I just want to put a small thing that out of the -- we are now finding out what is the reasonability of deciding the associate domain. But results out of ADC, in case there is a result that we have to take down that domain, I personally feel that we should have sufficient regions, and those regions should be legal regions so that we can defend in front of lawful agencies that this is possible.

So, at the same time, when we discussed in the last call also, previous call also, that it is very, very important that the regions which we have defined, there are very critical regions where the action is required immediately. Then there are regions where more or you can say additional support is required to be seen because this is a balance between rapturing the reputation of the registrant whose domain is under ADC and finally to be dropped, and the business. which registrar and the ceiling agent has to undertake in future also. So, these are my comments, maybe related to question number two and further question also. Thank you, Paul.

PAUL MCGRADY: Thank you, Anil. All right, we have Marc, and then Farzi disappeared, but I hope she comes back because I would like to get clarity on the nature of the reporting. Is it per incident? Is it per six months? Is it per year? All of the above, so that staff and I can take a look at it and determine if it fits into a charter question, if not what to do about it. If it doesn't, or more importantly, if it does, how to slot it in and make sure we don't forget it. Marc, go ahead.

MARC TRACHTENBERG: I think I'm just trying to better understand what -- I definitely agree there's a difference in transparency between transparency generally and or to ICANN versus transparency to the registrant, but I'm trying to understand what the adverse impact is on the registrant from a practical perspective of being potentially misidentified in an ADC where the registrar thinks that some additional domain names are associated and just what is the impact there. I saw Jothan's comment some people could say, well, some additional domain names could get suspended.

Okay, well that's an issue under the RAA. The registrar has certain obligations with what it does for domain names and to the extent that that a registrar thinks maybe that a domain is associated with another one, it doesn't take any action, there's no adverse impact on the registrant, and to the extent that the registrar thinks that the domain names are associated and they're not but has actionable evidence of domain abuse and then takes down the domain name. Okay, even if they weren't actually associated, the registrar is meeting its obligations

under the registrar accreditation agreement and mitigating an abusive domain name.

So, what is the adverse impact? What is the harm? We keep talking in these general terms, but I'm just trying to understand from a practical perspective, what really does that mean? What adverse impact practically could there be on a registrant? If we can identify that, we can discuss it. But I think to have these speculative things, it's hard to discuss, especially not seeing what they reasonably could be.

PAUL MCGRADY: All right. Thanks, Marc. We'll hear from Farzi and then we need to move on because we seem to be consistently not talking about charter question number two, but other things that are that are either further down the line or good ideas to capture to pass on. But Farzi, I would love to hear from you about the nature of the reporting, because I thought from your initial intervention that you were thinking about some sort of six month or one year transparency report as opposed to a per incident thing, which is -- Farzi, go ahead. Yeah.

FARZANAHE BADIEI: So, it is industry practice. I don't know if the domain name industry pays attention to other tech actors, but it's industry practice to do transparency reporting every six months and a year. Actually, Two Cows does voluntary transparency reporting on law enforcement and some other registries do transparency reporting. It is not a new technique that we are suggesting.

Transparency reporting is very -- and like after 30 years we should think about changing our practices. If we are asking for monitoring and doing ADC check, which some of the methods could create blanket surveillance, then we need to talk about those methods. And if we don't know what those methods are, then we cannot do our research on them, we cannot understand the implications on the registrants and the broader internet ecosystem.

So, transparency reports is not to create more paperwork for registrars. It's just to have more visibility into what is happening when they say they do ADC check for the sake of the Internet, the domain name registrant, and the end user. So basically what we are suggesting is something really simple. It can also be voluntary.

We can, of course, discuss transparency. And the EU is the champion of transparency reporting in Digital Services Act and other laws. So we can talk about it, of course, we can talk with the community. But in the PDPs, we would like to see transparency and accountability mechanism in place. And also, to respond to Marc, some of these methods could have adverse impact on the registrar. And if we don't know about them, we cannot measure that impact. And also, I wanted to respond to something else, but I'm just going to go down now.

PAUL MCGRADY: Okay. All right. Thank you.

FARZANEH BADIEI: Oh, sorry. Actually, Gabriel is one of the few people that supports us in this transparency discussion, and we are very appreciative of that. He did it in RDRS and he's doing it now here. And I know that he's saying it should be voluntary, but we are really appreciating that, Gabriel.

PAUL MCGRADY: Thank you. All right. We're spending so much time talking about something that doesn't fit in question number two, we're not going to get to the rest of our agenda. So, I'm going to draw the -- Gabriel, his hand was up. Gabriel, if you want to come back, I'll draw the line right behind you, but I'm going to draw it fiercely because we do need to move on. Brian, and then Martina, and then Gabriel, if you come back.

BRIAN CIMBOLIC: Thanks very much, Paul. Hi, everyone. Just a note, so I am broadly supportive of transparency reporting. I, however, don't agree that it belongs here. Keep in mind, if a registrar takes action on a domain under 3.18.2 currently, it has no obligation to have transparency reporting currently. I don't understand why we would have transparency obligation as it relates to a subset of names that the registrar acts upon.

That would be incomplete information, it would be confusing, and I don't necessarily think that that would be helpful. Again, I think a broader community conversation around transparency reporting is a good thing. I think we should engage in that, but I think that is a separate and different conversation from here. So, I think we should move on. On the actual question two, I just want to note, I think that

it's good. I think that it allows for the strawperson. It allows for flexibility.

I like the may include, but it's not limited to the extent there are different factors that a registrar may or may not be looking at. I think that that should all be acceptable with the caveat that I do think that we need some sort of we've talked about an advisory.

I think it's important without spelling out this is okay, this is not okay, I think that an advisory would play an important role is showing when a situation, an example where a registrar did a good job with an Associated Domain Check, as well as hypotheticals where the registrar didn't rise to the occasion, where it says it did something, but it was not reasonable enough of an Associated Domain Check, just because we want to make sure that whatever comes out of this policy is enforceable.

PAUL MCGRADY: Thanks, Brian. All right, we have Martina and then Gabriel, and then we're going to move on.

MARTINA BARBERO: Thank you very much, Paul. And three very quick points. One on the fact that, in fact, for the GAC, this conversation about transparency at the global level is something that we have been trying to push since the contract amendments of a few years ago. So, this is a high priority for the GAC. We'd be happy to engage in a discussion on overall rules, because as Brian say, we struggle to see the value of defining subset

rules from transparency here without having a global framework on how transparent reporting on DNS abuse should be addressed.

That's point one. Point two, I understand the concern about maybe the way that ADC can be used for overarching investigations. And I understand that we might want to have a way to draw a line. But in the AI regulation of the EU and the SNDM that were mentioned by Farzi, very often the access to transparent information is not for everybody, it's mainly for researchers and for the public sector.

So, maybe one way to accommodate a bit this need for transparency on the ADC is to think about whether the SSAC or security researcher can sometimes have a look at what's going on or give this access to ICANN Org in a way to mitigate this concern, but without making fully public the type of associations that the registrars are doing, because that would be against counterproductive and would give harmful players information that they don't deserve to have.

And finally, on this question in particular, the GAC appreciates the language. We just have a question on the baseline, which is referred to in the rational. Because I think the language here is a lot about me, and we relate to that, but then we speak about the minimum baseline in the rationale.

So, I'm not sure we have eviscerated entirely this topic, but I just wanted to raise that because I know there were some colleagues who had concerns, and in general, we wanted to see how to articulate this flexibility versus giving ICANN Org a bit of ground to stand. And in that respect, I suggest that, well, I support Nick's suggestion to maybe ask

compliance if this type of language would be enough for them to have some tips in the enforcement stage.

PAUL MCGRADY: Thanks, Martina. We will take that suggestion back with us and ask ICANN Compliance sooner rather than later about that. I think that in my mind, the baseline was, you can't just say, oh, well, because of my business model, I don't have access to any data at all that's helpful and I can't do this. Well, if that's a bridge too far, and that's not what folks who have been advocating for flexibility are saying, but we do need to think about all possibilities. So, we will grab that question and take it back. Gabriel, go ahead.

GABRIEL ANDREWS: Yeah, thank you, Paul. This is Gabriel for the records. Mostly just raising a hand because I was called out by name by Farzi. And thank you, Farzi, for recognizing that. We have been making a good effort to listen to and constructively respond to the request for high-level transparency. I note that in the past, you're right, that high-level transparency is something that the GAC has been supportive of as Martina just alluded to, and I think Brian called out as well, that I think we'd be supportive of looking into how to do that in a systemic manner in the future.

You've heard my caution on this, that I am supportive of the type of high-level reporting that I see put out by companies like Google or Microsoft, where they every six months will put out a report that talks about how many times they responded to law enforcement action. I

could envision a report where every six months you talk about how many investigations were conducted in response to evidenced abuse reports that were given to them, so long as you don't set an expectation that they talk exactly about how they conducted those investigations, because that's where you get into the risk of really educating your bad actors, as Volker has highlighted in the past.

And so, high-level reporting, sure, that's great for transparency. Just let's mitigate that operational risk and let's talk about this perhaps in its own forum, as I think was suggested by others. And I think you'll continue to find us willing partners. Over.

PAUL MCGRADY: Thanks, Gabriel. Okay, great. We're going to draw a line there and move on to the next thing. Here's a bit of homework for those who are interested in the topic of transparency reporting, please take a look through the charter questions, and if you believe it fits into one, put that out on the list so that staff can capture it so that when Nick and I have our conversations with staff, we will be able to understand everyone's views about whether or not it rests here.

If it doesn't rest here, then it will fall into the important ideas that came up that the GNSO Council should consider doing something with, which we'll be sending them at the end of the PDP. Or maybe we'll send them earlier, I don't know. Maybe we'll send them as they come up. But in any event, if we can have the advocates for this concept do that on the list, that would be fantastic. All right. We are moving on to strawperson charter question number three. All right. Here we go.

Defining investigation. What constitutes a reasonable investigation by a registrar? What investigation steps are required or recommended? Are the criteria for investigation proportionate and necessary? What is the impact of this investigation on domain name registrants? All right. And this is preliminary language based upon the working group's discussion. So, this is the part where everybody should be unhappy with it and make changes and advocate for things, okay?

So, this is not in the category of stable but not final. It's still very fluid. A reasonable investigation by a registrar must consist of reviewing information reasonably available to the registrar to determine whether additional domain names may be associated with the same abusive actor, sorry activity, actor, or campaign. And I think that may be the concept of the baseline, you've got to do something.

A reasonable investigation must be proportionate to the circumstances, including the nature of the abuse, domains registered for malicious purposes, the available evidence, and the scale or characteristics of any identified campaign. In the parentheses, we have another reminder that we're not talking about compromised domain names. This is just registered for malicious purposes.

A reasonable investigation must not require registrars to access or generate data. that is not reasonably available to them, recognizing that registrar capabilities, business models, and available data may differ across and within registrars. Registrars must check at least one reliable internal data point and use additional technical or abuse intelligence signals where needed available to identify associated domains to a malicious domain.

That's sort of a weird. I think we have to work on the grammar there. The obligation to perform an ADC should not be conditioned on the registrar having completed mitigation action in respect of the domain name that triggered the ADC that may be performed in any of the following orders, depending on the registrar's view of what is likely to result in the elimination of highest volume of malicious activity.

And here's the order. Prior to taking mitigation actions, in parallel with taking mitigation actions, or where the registrar has taken or is in the process of taking appropriate mitigation action. Staff, is there more to this strawperson on page two? Yep. The trigger for ADC may arise from a single domain name from which actionable evidence of DNS abuse exists, recognizing that the purpose of the ADC is to determine whether additional associated domains may be involved in abusive activity and the absence of multiple reported domain names does not preclude the existence of a broader abusive campaign.

Registrars must apply association criteria in a reasonable and proportionate manner, considering the risk of over-association, including scenarios where domains may be linked through reseller models, privacy proxy services, or shared data that does not reflect common control. The need to avoid reliance on assumptions that all domains sharing attributes are not necessarily controlled by the same actors.

The importance of ensuring that association is based on indicators that are meaningful and actionable rather than speculative. The importance of accessing data only when deemed necessary to perform the ADC. Usage of minimum information reasonably available and necessary to

determine whether domain names are associated and avoid collecting or processing additional data not needed for that purpose and the potential impact on domain name registrants. All right. And then we have a rationale. There's a lot here guys.

All right. There was a strong concern that requiring mitigation actions to occur for the triggering domain name before conducting an ADC could delay investigations and reduce effectiveness. Several participants noted that it is not operationally feasible to act on domains that have not yet been identified and that ADC may be necessary to understand the scope of use before final mitigation decisions are made. At the same time, the group did discuss whether including a single reported domain name should always be sufficient to trigger the ADC and how to balance this with concerns about workload and proportionality.

The discussion also highlighted the importance for working group members and the impacted parties flexibility in sequencing before, during, and alongside mitigation, and the need to ensure the standard remains practical across different registrar models, avoids unnecessary delay, provided that the sequence does not undermine the effectiveness of abuse mitigation or alert bad actors, and can be defended as reasonable and enforceable by ICANN compliance, all while remaining anchored in existing RAA language.

And that's probably the biggest run-on sentence I've seen in a long time, but we'll work on it. For the avoidance of doubt, as noted in the ICANN Advisory on compliance with DNS Abuse Obligation, actionable evidence means that the information that is readily available to the registrar must

be sufficient to enable the registrar to make a reasonable determination as to whether the registered name is being used for one or more form of DNS abuse.

Registrars are encouraged to proactively monitor the registered names that they sponsor to identify potential DNS abuse. A registrar's assessment of actionable evidence will vary depending on the circumstances of each case. I think that's it, unless staff tells me there's more about the rationale. Yep, that's it. So, let's go back up and open a queue on this, both the preliminary language and as well as the rationale, if people want to tackle that, and we'll spend a good chunk of time here. So, Reg, go ahead.

REG LEVY: Thank you. I'd like to remove the word reliable because I feel like it creates ambiguity. One internal data point, I think, is reasonable. I'm also concerned about the fact that use additional technical or abuse intelligence signals seems to be part of the must, and that seems to require that for every domain that we mitigate, we need to pay a third party to give us additional information about that domain.

And so, I think that additional technical or abuse intelligence signals either should be a separate sentence, so it's not part of the must, or just struck entirely, because we're not in here to provide extra business for retail block lists.

PAUL MCGRADY: Thanks, Reg. So if it read, registrars must check at least one internal data point, period. Registrars may use additional technical or abuse intelligence signals. Would that address your concern?

REG LEVYY: Yeah, that sounds great.

PAUL MCGRADY: All right. Thanks, Reg. All right, we have Marc, and then Volker.

MARC TRACHTENBERG: There's just like so much to unpack here. I don't even have nowhere to start on this question. It's just absolutely ridiculous. I guess I'll just make the two points I kind of made in the chat which is seems like we're going backwards on this question to address what was maybe addressed in question one of what the trigger is, and now the trigger is saying one domain name may be enough to trigger the ADC when I thought we had kind of landed on it is that one domain is sufficient, which I think is extremely clear in the charter and the only reasonable way to proceed.

But also here, I have no problem with reasonable, but I would make the same comment I made before, which is this language should be registrar agnostic. If different registrars have different business models, they can make the case for why what they did with the ADC is reasonable or not, but we don't need to bake this into the language itself. Take out all this stuff about recognizing registrar capabilities,

business models, and blah, blah, blah, and just leave it for a reasonable investigation.

PAUL MCGRADY: All right. Thanks, Marc. And by the way, everybody, this is also going to go in what is in the collaboration document, and your part of your homework is going to be going into this document and let's capture the ideas and concepts now, but it's not your last chance at this. So, you'll have a chance to go in and make comments into that document and we will capture them and refine this and bring it back. So, if you don't get in the queue today, and I never know how these are going to go.

But if everybody doesn't get in the queue today on this, then you'll have another opportunity. And Marc, you said the question's ridiculous or the strawperson's ridiculous. I'm not sure which one you're referring to, but I happen to think that the particular question is actually four questions. And there's a lot there stuffed into question number three. But let's charge ahead and deal with it and get it refined and ready. Volker, and then Gabriel.

VOLKER GREIMANN: So, supporting everything Reg said. With regard to what Marc said, I think having some limiters and some more descriptive guidelines here is helpful because that also guides compliance when they are basically adjudicating whether we meet our obligations or not. But one part that I think I heard that I didn't really like here was that Compliance could also come and ask us why we did take a certain domain name down, whether we did apply the change correctly.

I don't want to be in a position where I have to answer to compliance from both sides. Why didn't you take it down? Why did you take it down? It has to be one or the other for compliance because otherwise, we're in a legal bind that we do not want to be in. That part, why we did take something down, that's already very nicely packaged in just one little word that we as registrars know very well, and that's liability. Thank you.

PAUL MCGRADY: Thanks, Volker. Okay, Gabriel, go ahead, and then Martina.

GABRIEL ANDREWS: Yeah, so I wanted to respond just to a single part of this. So, this is not the sum of any feedback that you may have, but just in real time. I am reading the line that says that the registrars must check at least one reliable internal data point. And I put this comment in the margin in the document as well, but I have a concern that as written, that it might dodge the requirement to check whether or not the threat actor has multiple customer accounts.

And what I mean by this is consider a hypothetical bad actor that has like 10 or 100 different accounts with a registrar. If the registrar has one reliable internal data point that they choose to look at all the domains on a single account that's reported to them and they don't take any other additional steps to look at to see any of those other additional 99 accounts and the fact that they might share the exact same customer name, customer payment information, customer IP login history, even if everything exists to link additionally 99 additional accounts, if their one

data point doesn't cross that account threshold, then I worry, in that case, are they compliant? And I don't know the answer to that based off of this language. Over.

PAUL MCGRADY: Thanks, Gabriel. Martina.

MARTINA BARBERO: Thank you very much, Paul. And maybe on top of what Gabe said, just to comment on the one comment I put in the document, which is that the second sentence and the language there suggests that the ADC can happen at different points prior to taking a communication action, in parallel, etc. But this is not consistent with the draft Strawman language for question one, which still mentions that the ADC is triggered and takes place after action has been taken on a malicious domain.

So, I think we need to have support because that's a GAC point. We want action to be taken, not after necessarily, but like language to question three, it's what we would like to see. But then we need to correct the language to question one to make it sure that it's aligned, otherwise it doesn't make sense.

PAUL MCGRADY: Thanks, Martina. That's an important point and staff will capture that and we will talk about how to make sure that the documents we produce are internally consistent. Anil, go ahead, and then we have Volker.

ANIL JAIN: Thank you, Paul. Paul, once we are able to reach to the stage of ADC, so whatever background work registrar has done, that is the basic reasonable investigation which registrar has done. That is perfectly all right. Now, coming to the flexibility in the various methods of investigation, I suggest here if this working group or PDP can formulate a table, which will include both technical aspect as well as non-technical aspect to be framed and we hand over to the registrar to do this reasonable investigation. This will help two things.

Number one, a registrar who is not very knowledgeable, at least he'll get a toolkit to investigate and come to the conclusion of ADC. Number two, it helps in transparency also whenever it reaches to the level of taking down the domain and then coming the legal obligation. So, technical indicators means the DNS data, name server configuration, registration timestamps, et cetera.

Or maybe some investigation which is a result of consulting the DNS abuse intelligence resources, maybe outsider, which can be taken. And the non-technical things, we have already discussed in when we are dealing in set of question number one and two. I stop it here. Thank you.

PAUL MCGRADY: Thank you, Anil. Volker, go ahead.

VOLKER GREIMANN: Yes, just very briefly in response to Martina's comment there. I think it's important that we do not mandate when the associated domain names check has to occur, simply because of the fact that sometimes the associated domain name check is part of the investigation that we use to determine whether the one domain name that we got reported is actually worth a takedown.

Sometimes there's a cluster, and having that cluster finally takes the report over the threshold of warranted takedown because then we see that the evidence level has been reached that we can make the determination that it's absolutely illegal use. Whereas if it's just one domain that is acting alone, it could be all kinds of things. It might be abused, might not be abused, might be compromised.

But if there's a cluster that matches the pattern, then the ADC very much is part of the investigation that allows us to do the initial takedown. So, I think we should be very agnostic about when the takedown has to occur. It can be before, during, or as part of the investigation, even after, but we shouldn't mandate that. Thank you.

PAUL MCGRADY: Thanks, Volker. Yeah, it sounds like you and Martina agree that question number -- if we end up landing on this language in question number three, we have to make question number one make sense. So, we have to go back and look at that. Farzi, go ahead.

FARZANEH BADIEI: Yeah, so this goes back to what we initially started. And we framed it as severity of harm. And there was a lot of conversation that, oh, no, we don't know what it is and stuff like that. Okay, so, we put that argument aside. We want to talk, instead of using this loaded term of like harm and severity of harm, we want to use the term signals. What sorts of signals are out there other than the domain name that points to a potential abuse?

And this can be one reliable internal data point and it can be like use of like, I know Reg doesn't like this, but additional technical or abuse intelligence signal. And this is, I think, that people in some registrars are doing already. And this is what we mean by not taking action based on just one report on one domain name and doing it more holistically. So, at the moment, we like that there is one reliable internal data point, but we can discuss the wording as well. Thank you.

PAUL MCGRADY: Thanks, Farzi. Okay. Our queue seems to be at an end. So, let's move on. But remember that part of the homework is going to be going in and commenting on this to make sure that the issues, staff's going to do, as they always do, a terrific job capturing comments from the chat and from verbal interventions, but also anything that can be done to suggest specific language changes to address concerns is very, very welcome in that collaboration document.

All right, we're moving on to deliberate Charter Question 4. What data access and privacy safeguards are necessary to protect registrants and registrars during associated domain checks? And we have early input

themes, but we don't have strawperson language because we've not talked about this. So, this is the real free for all opportunity for question number four. Because from these conversations and the interventions in chat and on the list will come the strawperson.

So, early input themes are: there is universal agreement that any ADC must comply with applicable laws and data privacy safeguards. There is broad agreement that investigations should be targeted and evidence based. Multiple groups converge on the idea of balanced and proportionate responses. Groups tend to differ on how prescriptive the policy should be from detailed obligation-heavy policy to high-level principles with registrar discretion.

There were additional comments on reporting requirements with a divergence on whether and how much data should be shared by the registrars. The registrar's stakeholder group is more cautious in that no precise information should be shared with reporter or ICANN in contrast, the IPC would require registrars to share associated domain names that the registrar determined where actionable evidence was found. And then we have the early input documents.

And when we say reporting here, I do believe we are talking about the per incident reporting rather than the six month or one year industry reports that Farzi was talking about. And so, we should keep that in mind. I think that's our only slide for charter question number four, if I remember from prep time. So, this is the free-for-all. Let's go back up to the question so we can have that in front of us. What data access and privacy safeguards are necessary to protect both registrants and

registrars during associated domain name checks? Go. All right, Volker, go ahead.

VOLKER GREIMANN: None. Basically, the registrant is protected by the terms of our agreement and the laws of the registrar, where the registrar is based in. If the registrar makes a mistake, he's liable to the registrant for any damages caused, period.

PAUL MCGRADY: Marc.

MARC TRACHTENBERG: I agree with Volker. I mean, the boundaries of the contractor there, boundaries of the law are there. I don't think anyone's suggesting that this doesn't have to be compliant with law. I mean, all the registrars have to comply with applicable law. So, that's kind of it's table stakes. I mean, that already exists.

PAUL MCGRADY: All right. Thanks, Marc. Anil, and then Farzi.

ANIL JAIN: Thank you, Paul. Anil, for the record. This is a very interesting charter question because there are different laws which are available. One is the agreement of registrar with ICANN. Then there are GDPR, which are applicable to a good number of countries where the data protection is

available to registrant as well as to the registrar. And there are local data privacy laws which are available from country to country.

So, basically, one has to be very, very careful when they are doing the ADC that this must be protected at all. At the same time, the registrar should only access and correlate the data that is strictly necessary for the investigation. And that availability of the data should only be during the time of investigation and it should not be permanently available. These are my initial comments on this. Thank you.

PAUL MCGRADY: Thanks, Anil. So, that's strictly necessary as standard and guardrails around the timeframes. And Anil, the third big idea that I heard from you, in addition to those other two, is that there is more than one law out there. It's not just GDPR, but every country has its own privacy laws, and that's a distinction. So, we need to capture those three big ideas and also capture the Volker's big idea backed up by Marc of the contracts, find the way it is, and let's not mess with it. So, those are four big ideas. Farzi, give us another big idea.

FARZANEH BADIEI: Yeah, you are not going to stop talking about this topic by saying let's not overthink, Brian. So, totally agree with Anil on the points he made. And also, we want to think more about how this kind of ADC practices, because it's evolving, it has an impact on data protection. Another thing that we want to raise is that, yes, applicable law is great, but there are some people in some jurisdictions that don't have data protection and privacy protection.

And we need to rely on actual data protection and global data protection standards. They exist. OECD has one. There are a few others. And whatever Anil said with regards to availability of data at the time. But we have many more opinions on that, and we are going to get back to you on under wording. And also, like, we need to do a data protection impact assessment, according to our charter as a whole to all of the recommendations.

PAUL MCGRADY: Yes. All right. Thanks. Marc, and then Michaela.

MARC TRACHTENBERG: I just want to respond to Anil and just kind of strongly objective is strictly necessary. Anyone who's done investigations knows that there's no strictly necessary. You follow the investigation where the investigation takes you based on the evidence that you see in front of you. To say strictly necessary, no one's going to know that before. And I don't know how you demonstrate what was strictly necessary. The registrar should have the ability to do the investigation that it thinks is necessary.

And as far as how long they retain the data, it's data they already have. It's in their system. So, I don't really understand what the concern is here. As far as the point about you know different privacy safeguards and laws exist in different countries, yes, that's true under applicable law. And so, of course, like in everything they do, the registrars have to comply with applicable law as do registrants and reporters and everyone else in the ICANN community bubble, as well as everyone else

in the entire world. So, this is just in the background, everyone always has to comply with the law or risk consequences.

PAUL MCGRADY: Okay. Sorry, I thought you were done. I didn't mean to interrupt you. So, before you go, if not strictly necessary, is it another necessary? Is it reasonably necessary? What is it? And you can say, I don't know yet. I want to think about it and put it in the collaboration document. And that is a fair response. Did I lose you, Marc? All right.

MARC TRACHTENEBERG: I'm sorry, I didn't realize that was a question for me.

PAUL MCGRADY: Yeah, yeah. No, yeah. Yep. It was one of those before you go, Marc.

MARC TRACHENBERG: All right. Sorry, I missed that part. There's like a chat going on and like other conversations.

PAUL MCGRADY: Got you, yeah. So, let me say it again, just because you didn't have warning that I was going to ask this, which is if it's not strictly necessary, is it some other kind of necessary, like reasonably necessary, or is necessary or is necessary the wrong word in your mind? But more importantly, what would it be? What the standard?

MARC TRACHTENBRG: I think necessary is problematic. Who knows what necessary is? That's a hard word to define. I think reasonable while also can be challenging is much better, and that's the standard that I think people have generally agreed on using consistently through different parts of this PDP or the policy that we're creating and how we're answering the questions, and I just think that that is better and less prescriptive, the investigation should be reasonable in scope.

Like we keep saying reasonable, that seems to me to be the right word the right standard and what that ultimately looks like. I think maybe defined by advisories from ICANN or other things, but we shouldn't be too prescriptive here. The goal of this is to identify more DNS abuse. That's the goal. I mean, we don't want to do it in ways that adversely impact registrants or other people, for sure. We haven't heard any ways that that could happen yet, but if we do hear some, then we should address those.

But let's make this reasonably lightweight but also enforceable and meaningful. And I think we all recognize that behind the scenes, there's gonna have to be some ICANN compliance guidance here like there is in all the other obligations just like for DNS abuse. So, let's put as much in here as is reasonable. So, there's baseline obligations that are definable and understandable and auditable and leave some of the specificity maybe to some guidance.

PAUL MCGRADY: Thanks, Marc. I don't want to put words in your mouth, but it sounds like Marc is advocating for a reasonably appropriate standard rather than -- so, Anil, is it strictly necessary? I think, Marc, you sound to me like you're at reasonably appropriate, and maybe that does it. If I got it wrong, Marc, and you have better language, please do put it into the collaboration document. Oh, now I've done it. I've got Thomas in the queue. All right. So, I'm not calling on you now, buddy. You're number three. Michaela and then Brian.

MICHAELA SHAPIRO: Yeah, I'm sorry. I think I came before you, Thomas. Is that okay?

PAUL MCGRADY: Yeah, I confused everybody by saying his name. Sorry, Michaela, go ahead.

MICHAELA SHAPIRO: All good. Michaela, for the record. No, I'm also similar to Marc, I'm actually struggling to keep up with all the moving parts. But just to say this is less about the specifics of that language, but just to keep reiterating what others have said about ensuring that there are safeguards in here to allow. I think at a basic level, I completely understand and empathize that investigations will need to go where they need to go to address the issue at hand.

That being said, in any kind of investigation, when it comes to any kind of abuse, whether it's within the ICANN and domain context or not, there are still parameters that you must adhere to. So, this isn't a free-

for-all. Finding that exact language I know is tricky, but perhaps instead of being overly prescriptive, I think that's where having these safeguards will come to address some of those concerns. Where the NCSG stands is about ensuring that there are limits to the data.

For example, we can limit investigations to data already collected in the course of domain registration. And you have a principle of avoiding expanding that data collection, retention or sharing beyond what is already required under the contractual legal frameworks that we've already referred to. That being said, if it were to need to be expanded, this is where, again, proportionality and reasonableness would be the standards that we would want to push for.

But at the moment, we don't necessarily want to see that happen, but understand that others may disagree with that approach. So, we just want to ensure that while registrars, of course, have an interest in trying to address DNS abuse, these are not necessarily going to resemble law enforcement investigations because they are not law enforcement actors.

I don't think registrars would want to be in that role, but again, happy to defer to them on this call. So, let's just ensure that we're consistent with data protection standards as Farzi and others have already mentioned. So, I'll stop there. Thanks.

PAUL MCGRADY: Thanks, Michaela. Brian, and then Thomas.

BRIAN CIMBOLIC: I hate to be in the way between a group and Thomas's insight. So, just to note, so I agree that I think necessary, and I certainly don't agree with the concept of strictly necessary, but I even have some heartache over the phrase necessary. What we don't want to do is currently, just like registries, different registrars have different appetites and different practices when it comes to DNS abuse.

Some will just respond to reports, some will proactively search out DNS abuse. And so, there's different approaches to this. What we don't want to do, I think, is discourage registrars that take a really comprehensive approach to DNS abuse. If a registrar currently is doing associated domain checks and is doing so looking at the customer account, but also looking for related strings at similar registration times and looking at other information, well, I don't want to create a situation where if it did one check, then it's prohibited from doing other checks.

Again, all of it has to be consistent with data protection laws, has to be consistent with applicable laws, has to be consistent with its agreements, but what we don't want to do is say, well, you did your first check, you found something, everything thereafter is not necessary. So, I think we don't want to cage a registrar. If a registrar has a higher risk appetite and is happy looking at other data that It already has, I agree with Michaela, this shouldn't be an exercise in gathering more data, but it has three or four different steps that it does internally already to look at associated domain checks.

I think that if the policy ended up in a position where that registrar is somehow punished or discouraged from more comprehensive associated domain checks, then I think that would be a really bad policy

result. So, I think reasonably available or reasonably appropriate is a good place to start.

PAUL MCGRADY: Thanks, Brian. All right, Thomas.

THOMAS RICKERT: Thank you so much. I think that probably we're experiencing different language being used in different jurisdictions because we would not use the reasonably whatever language where I originate from. So, in my jurisdiction, necessary would be perfectly fine. Ultimately, we're talking about new purposes for processing the data. And if you need the data, if it's necessary to fulfill the purpose, however far that might need to go, you may process it. But after that purpose is fulfilled, it's not necessary anymore.

So, for me, I would be perfectly okay with the necessity standard, if you wish. Also, I think what we're seeing here is what we already saw when we did the EPDP on registration data. We've been talking about ICANN purposes versus purposes of the individual companies. So, I think that maybe we should clarify that companies can do whatever they can or must do under their local laws and arrangements and what they have, but that we are limiting our policy to the purposes that the contracted party needs to fulfill to meet ICANN standards and not get in trouble with ICANN compliance.

And as far as that goes, I think it's sufficient to talk about necessary, it's sufficient to make a reference to the applicable laws. As Brian

mentioned earlier, let's not overthink this, but I think one aspect that we need to think about a little more is retention periods because it's one thing to do the investigations and to do things with the data that you already have in your system. The other thing is what do you do with the intelligence gathered there from? And I think that we need to create different types of results of the associated domain checks.

So, if you get this trigger moment, if you start your investigation and it turns out that there's nothing, then you should probably be required to delete the result of that internal search immediately. Because otherwise, somebody might get somebody's name or account might be part of an investigation multiple times, and even though nothing materialized, at some point something sticks. So that can be stigmatizing.

And then we have the cases where something happens and where potentially a registrar takes mitigation action, and then the registrar needs the results of that investigation for two purposes. One is to be able to defend themselves if they've done something and somebody complains against what they did, and then the auditing part, i.e. ICANN might want to look at what the contracted party did in a specific case.

And I think that we probably need to, and I think we can't do that on the spot, but we need to think a little bit more about how long the data needs to be retained maximum, maybe it's three months, maybe it's six months, but after then it needs to be purged from the system, not the underlying data, but just the result of your investigation so that you're not getting in trouble with the ICANN compliance. But I would actually

create these three buckets to talk about retention only and leave everything else to the applicable law.

PAUL MCGRADY: Thanks, Thomas. I think just some initial reactions to that is, we can't get too prescriptive, like, for example, a requirement for immediate deletion, because what if one jurisdiction has a rule about retaining that sort of thing, right? But I get your point. I'm hoping staff captured all of that, and they certainly will go back through the recording if they didn't, because there's a lot there. We need to talk about that. Marc and then Martina.

MARC TRACHTENBERG: Yeah, just responding briefly to Thomas. I still think necessary is problematic and the reasonable scope is better and seems to have general agreement, at least in the chat. I don't know whether that is reflective of what the participants actually think, but I would certainly advocate for that.

The other point I wanted to make is, I think that I heard maybe from Michaela that the registrar should be prohibited from looking beyond the data they have collected. Maybe she didn't say that. I'm not sure. I don't want to put words in her mouth, and maybe others said it, but I just wanted to clarify that I don't think that a registrar should be prohibited from looking beyond the data they have collected because that would prohibit them from looking at the website that's posted on the domain name, which could be a very good indicator that they're

related, right? Or looking to see that they have the same MX records or something else.

And I'm not saying that they should be required to look at that stuff, but they should be able to, and this goes to I think Brian's point of not limiting what registrars can look at in their reasonable investigation. So, if they are a little more ambitious, they can find more than DNS abuse. And I think actually it could protect registrants. It'd be good in some situations to look beyond. So, for example, if you're a registrar and you have a large number of registrants who are probably using your default name servers, or maybe you have a large number of registrants that use Cloudflare because so many people use Cloudflare now.

And so, you're doing your investigation, you're seeing all these domain names related and you see, oh, they all have common name servers. Well, that's probably not enough there. So, you probably want to look a little bit further or maybe you don't have to, but you might want to, to say, okay, all these domain names are on the same name servers, but that doesn't necessarily mean they're related because everybody uses Cloudflare. So, maybe I want to look a little bit further.

I can see that the domain name is similar in structure to the domain name where we have reasonable evidence or actionable evidence of DNS abuse. So, maybe I want to take a look at the websites to see, okay, yes, these are all the same phishing website. So, I think they're related.

Or maybe if the domain where you have actionable evidence is being used for phishing, now the registrar looks and says, oh, I'm checking the

MX records, I see that all these other domain names, which have a similar structure, that aren't the same but are similar, and were registered around the same time, they have the same MX records, the same email provider. That gives me what I need to feel comfortable that they're related. The registrar shouldn't be prohibited from doing that.

PAUL MCGRADY: All right. Thanks, Marc. And there was several big ideas in Thomas's intervention, but one of them was that nothing we're doing here should prevent a registrar from using the data that they have to protect their own systems. And that may be a different analysis and that may start with a report of a malicious domain but may not end there and it may not be all about ICANN either. And I think staff should capture that. Martina and then Volker.

MARTINA BARBERO: Sorry, I was also trying to follow the chat. This is so interesting as a conversation, but just on the retention and maybe responding to Thomas, I think we have the parameters of applicable laws at the jurisdiction level, we have ICANN contracts, we don't want to reinvent the wheel here and add another layer of other different retention policies. I think then it's reference to Area A where actually relevant because I think we want to make life for implementation as clear as possible and avoid over-complexify this matter.

So, I'm not sure I would want to invent a different retention policy than the one that already exists. I see your point, Thomas, maybe for

investigation that yields no results, but then still, it might be that the register is asked by ICANN Org two years down the line. something about how they've addressed DNS abuse in the past two years, and they want to show examples, I don't know.

So, I'm not sure we want to add another layer of retention data policies to whatever already exists, because I think it would make it even more nightmare-ish to be compliant for registrars. But I may be wrong.

PAUL MCGRADY: Thanks, Martina. We have Volker and then Farzi.

VOLKER GREIMANN: Yes, agreeing with both Marc and Martina here. On the one hand, we absolutely do not want to be limited in the tools that we can use to root out DNS appeals on our platforms. Some of us use third-party services that enrich the data or reports that we get. Some of us scan our databases against anything that has been reported and do not wait for reports in all cases. So, that should be always allowable. And in the context of ADC, it shouldn't be any different.

And with regards to the other comment, I think we should absolutely not be in a position that we have to generate new data points as a mandatory policy to show compliance. I think the data points that we do collect and that we do base our decisions on should be sufficient, but we don't need to engage in large paperwork actions that basically take us away from the task that we want to accomplish here. Thank you.

PAUL MCGRADY: Thanks, Volker. Farzi.

FARZANEH BADIEI: So, Paul, I have two clarifications. So, first of all, when we talk about data protection, of course, if it's a matter of profiling and you can put things together and kind of like identify the domain name register and stuff like that, that is dangerous as well. But we are explicitly here talking about collection of personal sensitive data, like what is considered as like your name, your email address, your mailing address, and stuff like that.

So, when we say that data collection, we are not saying that don't go and check the name server. And this is not what we argue in the data protection argument. Another thing that I wanted to just mention that to the group, like we really appreciate the exchange, but some sometimes our comments and interventions, they receive some kind of comeback and responses that are blunt and overbroad about us, what we think, and our solutions, that it doesn't go unnoticed, and we appreciate the exchanges. We just want to mention that, please clarify first if we think that if a certain thing that you think we said is actually the thing that we believe, and then we can discuss it. Thank you.

PAUL MCGRADY: Thanks, Farzi. An important point for all of us, I think one of the things we're doing very well in this group is that we are not assuming bad motives. I don't see a lot of that in our verbal interventions or in the chat, to the extent I can keep up with the chat. But Farzi's point is well taken, which is as we go to summarize the views of other people so that

we can react to them, let's make sure that we say, if I'm understanding so-and-so correctly, I believe he or she is suggesting the following and leave room for correction.

I think that's a good civility thing. So, good call out. Our queue is done on this. So, I'm not going to belabor it. Other than to say thank you, I thought this was an excellent conversation. I thought the two conversations, the two topics before were excellent. I think we are in our groove and we're getting stuff done. I am very happy with us today. Oh, Anil, go ahead. And then we'll move on to AOB, unless somebody's dying to get in. But if you are, do it now. Anil, go ahead.

ANIL JAIN: Thank you, Paul Lennon for the record. I just want to mention here for the benefit of all the members of PDP that the registers are not same in size and also in capabilities of collecting the data. For example, there are small registers who are dealing only with few domains and there are very big registers. We are aware about those. So, the big registers have more capabilities in collecting data and even going beyond the required data also.

The second here is that there are registrars who are actually doing work for individual registrants, and there are registrars who are doing only for bulk registrants. So, when a registrar is doing for a bulk registrant, then the intention may not be to capture detailed data in this. So, when we are framing the norms for collecting the data for reasonable investigation, I think these aspects are required to be taken into consideration. Thank you.

PAUL MCGRADY: Thank you. Okay, Volker is next. I'm going to draw the end of the queue there so we have time for our last two slides. Go ahead.

VOLKER GREIMANN: Yes, and I appreciate the comments from Anil because it allows me to highlight a little thing that might otherwise get lost. I think, yes, absolutely, every registrar is different, every registrar is, in a way, its own little island because they have created their own business model and carved out their own niche.

But we should try to stay away from any generalization that, for example, larger registrars may have more data or maybe better equipped, staffed, resourced than small registrars are. I know a lot of larger registrars, especially in the wholesale business, who will probably have a lot less data than some of the boutique registrars who have white glove services for their customers, whom they each know individually and have met personally.

A lot of brand registrars are probably in that position. And even though they're small, they will have a lot more data available to them than large registrars might. So, we shouldn't generalize just by size. I think the business model also plays a very large role in how a registrar is able to resource this and go about the checks. Thank you.

PAUL MCGRADY: Thank you, Volker. All right. AOB, I have none. Does anybody have any AOB? Nope. Okay. So, next steps, Review of the Strawperson on

question two and three. Two, I think is further along. Three is still a big old mess. So, take a look in the collaboration document, make your comments, make your improvements, make sure that we capture the big ideas from today. We had a lot.

Staff will work furiously to update that collaboration document so that your review is good. We probably should flip one and two, but we will get that going. But you guys, make your comments as you go. Don't wait for staff. Three, working group to review the collaboration tool and provide feedback on charter question. It says four and five.

We didn't really get to five on substance, but we do have the early initial inputs in there. So, you can take a look at those and start to work on charter question five. And then we should just all prepare to discuss next steps based upon our action items above. Nick and I will meet with staff later this week and get ourselves ready to keep swimming.

Thank you, all. Please be active on the list, please be active in the collaboration document um, and like I said I'm really pleased. Today was such a great call. We did so much good work and we were civil and thoughtful and we had big ideas. I love it. Thank you all. Have a great day.

[END OF TRANSCRIPTION]