ALAN GREENBERG: Thank you. Welcome to the second day of the face-to-face meeting of the RDS WHOIS2 Review Team in Brussels on the 17th of April. I'd like to ask staff to do a roll call right now to start with, and then we'll do a recap of what happened yesterday. I'm assuming there are no changes to the statement of interest from yesterday. If I'm wrong, please let me know.

ALICE JANSEN: Thank you, Alan. This is Alice Jansen, ICANN staff. Shall we start with Erika for the roll call?

ERIKA MANN: Erika Mann.

CHRIS DISSPAIN: Chris Disspain. Thank you, Erika.

SUSAN KAWAGUCHI: Susan Kawaguchi.

ALAN GREENBERG: Alan Greenberg.

LISA PHIFER: Lisa Phifer.

LILI SUN: Lili Sun.

CARLTON SAMUELS: Carlton Samuels.

DMITRY BELYAVSKY: Dmitry Belyavsky.

JEAN-BAPTISTE DEROULEZ: Jean-Baptiste Deroulez, ICANN Org.

UNIDENTIFIED MALE: [inaudible], observer.

SARA CAPLIS: Sara Caplis, ICANN Org.

ALAN GREENBERG: Thank you. I'll note Stephanie Perrin and Cathrin Bauer-Bulst are not here yet, but I presume they will be arriving shortly and will be noted in the records of the meeting.

The first item on our agenda is a brief recap of what happened yesterday. This is a very brief one and this was done by staff overnight, and as I go through it, I'd like to ask for thoughts from particularly the

team leader, but anyone else if this is not an accurate summary, but it is a summary not a detailed record.

On recommendation 15 and 16, the plan and annual report, we're considering a recommendation to improve methodology when documenting implementation steps and milestones. More effective reporting structure is needed. Outcome-based reporting, not activity-based reporting, develop and track progress against the work plan and not just against the action plan. Sorry, I'm trying to … I'm having trouble with my Skype to actually have it scroll without missing things, if you'll give me a moment. That was the completion of recommendation 15 and 16. Does that sound like a fair summary?

UNIDENTIFIED FEMALE: Yes.

ALAN GREENBERG: Any other comments? Okay, thank you. Recommendation 1, strategic priority. Where is the strategy for WHOIS that was made a priority? Who owns the strategy? Who tracks and provides oversight for that strategy? What does success look like? High-level guidance to measure success against metrics is needed. ICANN took actions, but not those envisioned by the WHOIS recommendation. Notably, the Board Working Group or EWG are not the committee WHOIS1 recommended. I think that last part needs to be clarified because there was a committee that was looked at as a community committee, including the board, but there was also reference to the compliance reporting to the board and

that's not the action that we need, so we need to make sure that we're talking about the community committee.

I guess I have a question before I'll ask whether this is satisfactory. I don't know – how do you measure whether treating something as strategic is a success? If you use my example of why didn't – if it was so strategic, why wasn't someone watching related to privacy issues in WHOIS? Well, that one has blown up on us, so it's easy to track. But, if it hasn't blown up yet, the absence of something is very difficult to document. So, I think we need to think about that a little bit. It's easy to find fault, but if there's no real methodology one can use other than this being no disaster yet, does that mean you're doing a good job or you're lucky? So, I think we need to think about that a little bit. But, in any case, strategic priority is a roughly good summary. I think it needs a little bit of work, but … General agreement? Sorry?

CARLTON SAMUELS: [inaudible] committee.

ALAN GREENBERG: I don't believe it said the compliance should report to a board committee, but there is reference to the board there and a reference to the board participating in this cross-community committee, so we need to just make sure that's clarified.

Recap of recommendation 2, single WHOIS. There is no single WHOIS policy. The board did not have the power to produce a single WHOIS policy, but took actions it is empowered to take, i.e., initiate a PDP,

develop process framework, and in the absence of a single WHOIS policy actions were taken to provide consolidation and navigation. Although improvements could be made to that, it would still not be a single policy.

Broader than this recommendation is the question: to whom should the recommendation be directed? Consider horizontal, cross-community, or top-down, bottom-only recommendations. I think that's a general statement that we need to consider. I'm not sure it's really tied to that recommendation. Is that reasonable, Carlton? Yeah. Okay. Anyone else?

Data accuracy, recommendations 5 to 9. Susan and Lili to confirm questions for ICANN compliance. Findings and issues, recommendations will be handled by the two subgroups to avoid duplication. There's no real recap here of the findings, however. I think if I can try to summarize on the fly, the findings were that a lot of work has been done. The reporting is not necessarily really clear on what the outcomes are and I think there was, certainly from Lili, a level of dissatisfaction of the ability to really use the data to draw conclusions. Lili is looking at me with a confused look on her face and I'm looking at her with a confused look on my face. Maybe my summarizing on the fly is not adequate and we need to go back and come up with …

Certainly, I'm not satisfied based on what Lili has found that we can say they did a really good job of this. They certainly did a lot of work and we have a lot more numbers than we had before, but I'm not sure that the data has been presented in a way which makes it easy for the community to understand what the situation is regarding data accuracy. Please, Lili.

LILI SUN: Actually, specifically for data accuracy topic, I believe we can draw the conclusion that it failed to meet the objectives of the WHOIS1 recommendation, but actually to what extent can we achieve? We need to put a question mark.

ALAN GREENBERG: I guess I have a level of dissatisfaction of just simply saying it didn't meet the requirements without being a little bit more specific on how they should've either done the work differently or presented the work differently. Carlton?

CARLTON SAMUELS: It's about how they did they work and the presentation of the work. It's two things. The first thing is that they had a framework of how they were going to put it in, so they have an infrastructure that they implemented to [inaudible] data accuracy. Then, once the data was processed and the accuracy derived from the data, there were certain elements that were left unexplained. For example, that [consent] 25% or so, that does not explain what happened. If you look at the numbers, about 60% or 65% and then there's another 15-20% and then there's [inaudible] the rest of it. We don't quite know what is the situation with that piece of data.

So, in my view, the mechanism or the infrastructure is put in place, but in the analysis of the data, certainly the outcomes were still … There still needs some explanation of the outcomes and the remediation.

ALAN GREENBERG: Any further comments? Recap of outreach materials are available but not up-to-date and are labeled appropriately. The note says insufficient targeted outreach. I think there's been lots of targeted outreach, but not necessarily targeted outside the ICANN community. I still have a level of dissatisfaction. If we say that, I think we have an obligation to explain a little bit more where we believe they should have targeted it. But, I'm not sure how relevant it is given that whatever the world is a year or two years from now it's going to be different and I think there's going to be a huge amount of outreach that will be necessary to explain the far more complex world we'll be at that part than we are today. So, Carlton, please go ahead.

CARLTON SAMUELS: Yes, without the outreach, we can say that we see from some of the strategic planning from the stakeholder organizations, ICANN stakeholder organizations, that they're looking at different groups outside of ICANN to target. You are quite right that those might change within the year or so, but we can safely say that there now is at least some recognition that outside groups should be targeted and there is some thinking into what those groups should be. That might change over time.

ALAN GREENBERG: I think the last recommendation, given that it simply said target groups outside but was not very specific, I think was a little bit … I won't say negligent, but it made it very hard to implement that, especially in a

world where there was no ability to go back to the review team and say, "What did you mean?"

That finishes up the summary. Alice has something to say. Alice, maybe we want to quickly reread the strategic priority one now that Cathrin is here, if Cathrin is ready to focus.

CATHRIN BAUER-BULST: I'm ready.

ALAN GREENBERG: Okay. The recap on strategic priority is where is the strategy for WHOIS that was made a priority. Who owns the strategy? Who tracks and provides oversight for that strategy? What does success look like? High-level guidance to measure success against metrics is needed. ICANN took actions, but not those envisioned in the recommendation with regard to the Board Working Group or the EWG that are not the committee that was recommended by the WHOIS recommendations.

My comment is I have a little bit of problem saying how do we measure success in something being strategic in that you can't really tell to some extent whether you did it properly or you were just lucky that nothing bad happened along the way. Again, I don't like making recommendations that I can't tell them how we go about implementing it. Other than that, I think it's a pretty good summary, Cathrin. Are you comfortable?

CATHRIN BAUER-BULST: Yes. Thank you, Alan. I'm comfortable with that.

ALAN GREENBERG: Thank you. And thank you to staff for pulling all these together overnight. Yes, Alice, now back to you.

ALICE JANSEN: Thank you, Alan. We had sort of put data accuracy and compliance in the same bucket. We did the [inaudible] conclusions in the data accuracy, but we skipped compliance and maybe we want to … Yes. Thank you.

ALAN GREENBERG: And no one noticed. I'm not quite sure where to go. I was actually imagining that we would have a significant number of recommendations in compliance, and we may end up having some factoring in Lili's data, but the recommendations that Susan gave were very, very generic and I can't actually repeat them right now. Are we happy to do that or do we want to be more specific in terms of compliance?

SUSAN KAWAGUCHI: I agree. I brought up two recommendations, one of which probably fits more in Lili's bandwidth than the compliance. But, I also think that we need more information from the compliance team, that last report – the second report I got from them was pretty uninformative. The first one was much more informative and it was just a lack of time to schedule

another time with them to go back and talk and make this meeting. So, there's a lot more work to do there, which I have a plan to do that.

Then, I think it is a discussion. I didn't want to come to grand assumptions on recommendations without some discussion of the whole working or the whole review team. I could come up with all kinds of recommendations if you'd like right off the fly, probably, but I think it's better if we have an in-depth discussion and really decide what is a priority.

One of the things that I struggled with, too, in the report, it asks for our ranking on the recommendation, which I think it's too soon to do that. There was a reference to five recommendations, so I don't know if that was just a number pulled out of thin are. Are we really thinking we're only going to have five to ten recommendations?

ALAN GREENBERG: Lisa then me in the queue.

LISA PHIFER: Let me answer that first, and then actually I had wanted to be in the queue to respond to the compliance wrap-up as well. So, the question about five is merely a technique for prioritizing. If you could only do five, which would be your top five? So, instead of forcing us to rank one, two, three, it's just saying what would bubble to the top?

But, with regard to recapping on compliance, there were two objectives that the compliance subgroup is trying to address and the read-out yesterday covered findings for the implementation of rec 4, but we still

need findings for the other objectives that then lead to the recommendation that you put forward. The inverse is true for rec 4 implementation. You still need to consider whether there are any recommendations based on those findings. We have sort of a partial read-out and two action items in addition to the one regarding reconciling overlap between the two teams.

ALAN GREENBERG: Thank you. A couple of things. In terms of one or two recommendations versus a whole laundry list, I think what we identified yesterday in another context is if you give a long list, then it will be perceived as this is exactly what they must do as opposed to a more generic one. Perhaps with one or two examples, but make it very clear that those examples are not limiting. So, I strongly favor something more general in putting the responsibility on them to flesh it out, but make sure it's clear that they do have to do that.

Other review teams at times may have a recommendation, but three or four sub-parts to it. One could argue whether that's three recommendations or one.

Lastly, I think we came to a very strong conclusion that they are never going to address issues like accuracy if they simply are looking at a case-by-case basis and that they're going to have to generalize and look for patterns and rely on outside experts or outside groups that do a lot of pattern recognition. I think that one is a very clear recommendation that we have to make really clearly. If we have a problem with 40% of all

registrations, we're not going to fix it by picking one by one from random samples.

UNIDENTIFIED FEMALE: Yeah. When I was doing the work, I really envisioned us coming to conclusion on – so there's three elements or three sections of the rec 4 and I'm not sure that the resource is an issue. They seem to be pretty well resourced at this point. They definitely were not the first time around. But, I definitely think … I agree with you that there's a recommendation out of the first part on providing reports and data and doing something with that data. The second is the reporting structure, so I think there's definitely two strong recommendations coming out of that and it could be we may find that there might be [inaudible] elements to those recommendations.

ALAN GREENBERG: I think we have Cathrin in the queue next? Carlton?

CARLTON SAMUELS: So, [inaudible] part of it recall we also had a conversation about the role of the reputation companies and sharing data with them [inaudible] key part to make sure that that is involved.

UNIDENTIFIED FEMALE: Yeah, I agree.

ALAN GREENBERG: That was my reference to external groups. Cathrin?

CATHRIN BAUER-BULST: On the [reputational fees], we also cover the issue that Jamie raised with users and about not being able to take action against registrars such as [inaudible] names because formerly they comply with the obligations that they have to respond to the compliance team and that's maybe something we could also [inaudible] with a third recommendation that they need the right framework to be able to take action. If everybody knows that there's a bad actor and compliance is not able to do anything because they don't have the framework legally, then that's an issue in my view.

More generally, I wanted to – we're getting I think into the overall discussion of how we deal with the first part of this review. I think we will need to think about what our objectives are as the review team in issuing these recommendations, because of course, for much of it, we're just doing the [inaudible] on WHOIS as it used to be and then we probably don't want to just complain about things that went wrong, but [inaudible] to fix going forward. Of course, compliance doesn't fall into that bucket, but I think that should be one discussion we should maybe already reflect on now individually and that we should get into [inaudible] talk about the overall implementation and possible recommendations. What is the objective of this review team in terms of where it wants to steer things and how can we [inaudible] achieve that?

We might still want to highlight where implementation was incorrect, but if it's no longer useful to attack that particular issue because of the

way the WHOIS has changed, then it's probably not useful to make a recommendation on that. But, then, we could think about again the meta level of how can review teams ensure or how can they better track that their recommendations were actually implemented and do we need another process that looks specifically at that two years down the road and not five years down the road?

ALAN GREENBERG: And linked to that – again, I'll certainly support the fact we don't want to say go back and do the work properly because you didn't do it right last time if it's not relevant. On the other hand, we are seeing a pattern in much of this that, from ICANN's perspective, they said they did something and we're not agreeing. Therefore, the process they have for determining whether in fact they're meeting the recommendations has to be refined somehow whether it's with the equivalent of an implementation review team for them to get outside opinion as to whether they completed it or not or something else. We're certainly looking at this with a more critical eye than they did in their self-analysis and I think that's problematic. Susan?

SUSAN KAWAGUCHI: I just wanted to note that we have a couple of agenda items this afternoon to do this overall assessment, so to make sure that we haven't forgotten this point, we've put a note to ourselves to bring this back up then.

ALAN GREENBERG: Yeah. Sorry. We've gotten carried away.

SUSAN KAWAGUCHI: I'm going to carry it a little further. When I've been reviewing all the reports and looking at all these issues, I'm not seeing things going away completely with GDPR. I think we still have a duty to enforce on accuracy. It'll be much different, but I think the accuracy will still be an issue and I'm not sure how that data becomes apparent to ICANN, and that's, thinking down the road, I think we need to do. But, all of this work in letting the compliance team know that the reports and everything, which yes, they have tons more data than they did in 2010 through 2012. It didn't satisfy that recommendation because it doesn't really give us information to understand the issues and for them to understand the issues. And I don't think that's going to change. It'll just be on a smaller scale because we won't know what's going on, but there will still be a need for reporting and people being made to sort of make that data accurate. I mean, we [BCIPC] lost the argument that there is a component of GDPR that requires accurate data, but I think ICANN should stand on that and just say, "Yes, we require accurate data." That's fine, but eventually somebody is going to see it.

ALAN GREENBERG: Thank you, Susan. Two comments on that. Certainly, my response to Cathrin that we need to look at what's still relevant was not necessarily saying that a lot of it isn't relevant anymore. Just to caution that, as we go through it, if it's not relevant, let's not push. This is not a make work

exercise unless we're going to get something out of it. But, I agree with you. I don't think there are many areas where that's true, but so be it.

In terms of post-GDPR, well, one of the interesting questions is: is accuracy something that is of sufficient importance that ICANN should have access to this data? Because it's not clear that ICANN will have access to the data if we just let the world unfold. And that's one of those really critical issues. Can we say we are having a reliable, usable DNS if we cannot demonstrate that the data is moderately accurate? I personally think that's imbedded in our mission. The Article 29 people don't seem to think so, but we could argue about that.

So, I think going forward, we are going to look at the world as we think it will unfold, even if we don't know exactly how it will be at the time we issue our report. Carlton, were you trying to get in? No? Cathrin, go ahead.

CATHRIN BAUER-BULST: Yes. Thank you, Alan. Just to clarify, my point was that we are now determining where implementation is not up to what we think the standard should be and there's a recommendation that might come out of that related to how implementation should be done and monitored. Then, there's a separate process about designing the recommendations going forward, which doesn't necessarily relate to all the areas where we've discovered that there's an issue with implementation. But, I do agree that much of it still remains relevant.

ALAN GREENBERG: Further comments before we go back to the regularly scheduled agenda? Erika, please.

ERIKA MANN: Listening to you, I wonder whether there is actually, particular to what Cathrin said, there is really a difference because even if WHOIS would go dark, it wouldn't mean that the data shall not be collected accurately and stored accurate. It would only mean that it's not visible to the public.

So, you can look at it in two ways. Either who then is going to collect and source the data becomes sloppy and is not storing data accurately any longer, but this would be then a serious problem because then nobody would ever have received correct information or be able to receive correct information. So, I would say a large part of what we do is still going to be relevant. The [inaudible] will change or might change, or might change for some players, for the [inaudible] players, [inaudible] customers. But, that's [inaudible]. The rest would still remain maybe even more accurate and the accuracy needs to increase probably even, because if you can't see the [inaudible] factor becomes so small because it's only those which really go after something and will use law enforcement that you can track and trace.

ALAN GREENBERG: Cathrin?

CATHRIN BAUER-BULST: Yes. Sorry, I really don't want to belabor the point, but just to be clear, let me give you an example. We discovered yesterday that the outreach to the general consumer probably hasn't been done and also talked about that it's probably pretty difficult to do, so we might determine in our report that this part has not been implemented properly, but if we decide in the new WHOIS, there will be no access to the registrant information for the general consumer, then there's absolutely no purpose in recommending—

UNIDENTIFIED FEMALE: [inaudible].

CATHRIN BAUER-BULST: Or for anyone, but regardless—

ALAN GREENBERG: We don't know how it's going to turn out right now.

CATHRIN BAUER-BULST: But, then, there's absolutely no purpose in declaring that we need to have outreach to the general consumer because it won't be useful anymore. Then, we don't need a recommendation that says you didn't do this properly, but we might still want to have a recommendation that says there were a number of points that weren't implemented properly – one, two, three, four, five – and on that basis, we recommend that a certain process should be established to follow-up.

ALAN GREENBERG: If I can elaborate, I think all Cathrin is saying is if – and that's an if there – if general users anywhere do not have access to WHOIS information, there is no point in telling ICANN to go publicize it with them. On the other hand, if some class of users still have access outside Europe or whatever, then obviously it's still a requirement.

ERIKA MANN: I agree, Alan.

ALAN GREENBERG: Let's not do make work.

ERIKA MANN: No, but my point related to different factors the same because I think Cathrin is right. We need to evaluate the relationship, but just regard to certain topics like accuracy, I would argue the fact that the internal control factor might even need to increase.

ALAN GREENBERG: Look, we're going to have a lot of time, spend a lot of time, in detailing recommendations and I think if people around the table disagree, there will be plenty of opportunity for that. And if we're all agreeing with … No, no, no. Look, we don't know how the world is going to unfold right now, so hypothesizing on if it goes this way … We can spend a lot of time hypothesizing if ICANN doesn't have any access to the data, how

are we going to ensure accuracy? It's going to be a really good question, but we don't know how it's unfolding right now, so let's not spend time debating it. Stephanie?

STEPHANIE PERRIN: I don't want to belabor this point, but I don't see how ICANN is going to lose access to the data because they're the data controller, and unless they totally revise how they manage all their contracts, where they give themselves access to data, the same thing will pertain. It will just be not public.

ALAN GREENBERG: We've heard other ways that this can unfold, but it's not a discussion that we need to have right now. If we are complete, the next item on the agenda is …

ALICE JANSEN: Alan?

ALAN GREENBERG: Apparently, it's not the next item on the agenda.

ALICE JANSEN: Do you want to go over the meeting objectives for day two briefly just to clarify?

ALAN GREENBERG: I'm not sure I want to read what are effectively the same words as yesterday. We'll be spending part of the day looking at recommendations we haven't looked at yet. Same basic methodology as yesterday. We will also have some additional time today to again follow on the discussion we've just been having in terms of trying to synthesize where we're going in a more global sense than just recommendation by recommendation. We're already running somewhat late right now, so I don't think I'm going to belabor the details. There's nothing significantly changed from the overall methodology of yesterday. I think what we did yesterday worked pretty well so far.

With that, I will go on to recommendation 12 to 14, internationalized domain names. Dmitry?

DMITRY BELYAVSKY: Next slide, please. There was a block of three recommendations related to international data. The recommendation 12 requires … There is a typo. The recommendation 12 required [inaudible] of a group within six months to terminate the data requirement. Recommendation 13 required incorporation for the final data model to the registrar and registry agreement and the [inaudible] placeholders in case the recommendations are not worked out. And recommendation 14 required the metrics to develop – a required development of metrics to maintain the data. Next slide, please. And next.

So, after [inaudible] the document, we have the following findings. Board tasked working group to specify the requirements for the

international data registration and this principles and recommendations were worked out and adopted by the board.

So, the recommendation 12 seems to be fulfilled. The recommendation 13 required including the final data model or placeholders if the data model is not implemented, so we can find [inaudible] in the both registrar and registry agreement, but in both cases, this requirement [inaudible] the registrar and registries to implement new protocols, if any, only in case if its implementation is commercially reasonable. In fact, if it doesn't [inaudible] registrar or registry to do anything. But, formally, the recommendation 13 is fulfilled.

And the protocol, which is designed according to the requirements [inaudible] recommendation regarding translation and transliteration but it's not implemented yet in fact, though ICANN start [that] pilot program.

According to recommendation 13, the metrics that should be used for the international data, well, we think that the metrics provided by data accuracy measurements is relevant to the international data, though it requires – it may require the persons to understand the corresponding language to use the methodology. But, formally, the recommendation 13 is fulfilled, too.

So, the recommendations are phrased in such ways that they were fulfilled, but in fact, we don't have any international data available to check whether it was. Thank you.

ALAN GREENBERG: Comments? I'll put myself in the queue. I guess what we do next, the words I would tend to use are since the work was done but none of it is implemented on things like translation, transliteration, we really are not in a position to take action today. What we need is what I would call a watching brief of this needs to be monitored as we eventually go to a new RDAP based system that is capable of handling IDN to make sure it is implemented meeting the original targets. I'm not sure we really … I'm not sure it makes sense for us to make a recommendation to the board to say keep an eye on it. That's sort of a demeaning statement. Presumably, they're always keeping an eye on things.

But, on the other hand, I don't think we really want to leave it as, "Thank you very much. You implemented it. We don't need to think about it anymore." So, I'm not quite sure how to go forward. Dmitry?

DMITRY BELYAVSKY: I think that the most significant point is that there is in fact no obligations for the registry or registrars to do anything because of commercial limitations. I don't know, can we do anything with it? But, I think this phrasing means that in fact neither registrars nor registry are obliged to do anything. I think this should be noted, but that's all.

ALAN GREENBERG: Certainly … I haven't been involved with this recently, but I was involved a bunch of years ago and issues like translation, transliteration, which are necessary to be able to functionally use the WHOIS data in some cases, but it was completely unclear who would pay for it and it's not necessarily an inexpensive process where it's not always obvious

whether in any given case it's translation or transliteration that you actually want because both of them yield completely meaningless results sometimes.

There's a lot of questions to be resolved, but I don't think we're at the point where we can raise them. Dmitry?

DMITRY BELYAVSKY: I can say just about [inaudible] practice of translation and transliterations. Most registrars provide [fields] in native language and in most cases the registrants can either take their transliteration provided by the registrar system or can correct it using, for example, documents, legal forms, so less burden is on the registrant and … Well, the [inaudible] burden is on the registrant and the technical burden is on the registrars because they have to provide transliteration software. But, it works more or less well [inaudible], but I'm not sure if it will work, for example, in China. Thank you.

ALAN GREENBERG: One of the problems is today we are dealing with a seven-bit ASCII WHOIS. We must provide something that can be put into the WHOIS. Once we're with an IDN-based WHOIS, we don't necessarily have that requirement and the native script may well suffice, but not necessarily be useful to anyone, which is why the whole issue of translation, transliteration came up because what is in the WHOIS may not be a usable [context]. Comments, questions? Lisa?

LISA PHIFER: I've been thinking about how to ask this question. It seems this may be an example of where the recommendations were fairly specific, like updating the contracts to require support, but that wasn't really the intent of the recommendation. The intent was to have a system that provided translation, transliteration. So, maybe one thing to be learned from this is to state the overall objective more abstractly and then supported by specifics. In this case, the specifics were carried out, but perhaps the overall intent was not.

ALAN GREENBERG: Is that a forced versus [inaudible] analysis? Yeah. Go ahead, Susan.

SUSAN KAWAGUCHI: This is not something I'd spend a lot of time on, on the first WHOIS Review Team. I'm just trying to remember back. We thought with [inaudible] new gTLDs there would be many more IDNs, and some have launched. But, maybe there's free translation tools now that exist that didn't six or eight years ago, whenever we talked about this, that could be leveraged. It could be that we could make some suggestions in the next recommendation on this. But, it seems like RDAP is the key to this, right? Go ahead.

DMITRY BELYAVSKY: Yes, but no. RDAP is the key because it allows to provide data on a speaker's native language, but it's still a problem to provide it understandable in ASCII world [inaudible].

ALAN GREENBERG: RDAP has the capability of having multiple formats. The question is which formats do we use? If you go back to one of the original analyses of translation, transliteration, they give some marvelous examples of when it makes no sense at all to do a translation because … There are many company names that have no meaning. They're just arbitrary things that sounded good at which point you have no choice but to do a transliteration. Other places, it makes complete sense. The same is true for street names and city names and things like that. It requires a fair amount of knowledge and typically eyeballing it and a knowledge of that language to decide which is which that makes some sense, and it wasn't at all clear how one does that in a more generic sense.

I like Dmitry's examples of what's done in Russia. You do a first stab and let the person look at it and that works really well if that person understands Latin script and can read it, and it has no meaning whatsoever. So, if you're dealing with Arabic and Chinese and that person does not read a Latin-based script, they're not in a position to judge: is this a good interpretation of what I wrote or not? It's a challenge. I think all we can say is the work was done to the extent it can be done, given that we still do not have an RDAP-based WHOIS system and until it is, we're going to have a lot of work to actually implement that and you never quite know when you go to implement these things if you have all the details until you try. I think that's about as good as we can say and I don't think we can charge more work, except to note that this is not finished until it's actually finished and someone is going to have to keep a good watch on it. Anything further?

Where are we? Recommendation 11, common interface. Miss Susan.

SUSAN KAWAGUCHI: Common interface. So, this is really Volker's, but since he could be here – he's the rapporteur on this one. So, it is recommended that the Internet service is overhauled to provide enhanced usability for consumers, including the display of full registrant data for all gTLD domain names, whether those gTLDs operate thin or thick WHOIS services, operational improvements should include enhanced promotion of the services to increase user awareness.

So, as I'm sure you're all aware, the Internet service internic.net prior to … Well, probably not even. I'm sort of stumbling on this in trying to remember. But, anyway, the internic.net would provide at least a thin WHOIS for all the dot-com and net which were, in those days, more the primary domain extensions. Still are, but we have all the new gTLDs, too.

The challenge that we were seeing personally and people were complaining about is you couldn't always figure out which registrar a domain name was registered with and you'd have to go to the thin WHOIS, pick up the registrar if it was there, or if that registrar was providing that service instead of their reseller. You would really take a lot of investigation just to do a simple WHOIS lookup. I can remember bringing several examples to the WHOIS Review Team and saying, "Okay, you figure this out. Look at this. You tell me." And it would be 15-20 minutes later, they're like, "Oh, we got it now." Well, that's ridiculous.

So, in reading this today, I'm like, oh, we should've never probably said overhaul the internic's internic service. What I think the implementation of this was to develop a whole new interface, a common interface. I'm not sure if they did anything with the internic service. It still returns the same results.

So, we were trying to answer several questions. Has the creation deployment of the WHOIS [inaudible] the direction of the board met this recommendation, considering the old internic's internic service still exists unchanged. Does the WHOIS query service provided through the micro-site, the common interface, provide clear and reliable access to full registrant data for all gTLD domain names? What promotional efforts has ICANN undertaken to increase user awareness of the common interface? Does the common interface provide clear instructions on how to notify ICANN, the sponsoring registrar, and/or the registrant regarding data accuracy? So, we used a lot of the common tools here or resources that we've used for other things here.

So, we requested statistics on the use of the common interface, up-time, requests for help using the tool and what usage data is tracked by ICANN. We requested that from the team or department that implemented and maintains the common interfaces and asks if there was any challenges with implementation and maintenance of the interface.

We basically didn't get a whole lot of information. They don't track much. So, once again, we have a policy or recommendation that went into effect and a service that's being provided and it's much better than the old system in that you can actually look up most of the … That you

can look up any of the gTLDs new or legacy and receive information most of the time, but there's nothing there to really provide guidance on how well this works, how often … They do say that sometimes fields are returned blank, and there was a fix for that. So, in general, it was just not enough metrics and it seems to me we don't want to burden ICANN with having a deep analysis on something, but we do think that there is a recommendation here that we could develop that the original recommendation was sure that anyone looking up a WHOIS record could do that easily and from one source instead of having to go to every registrar around the world.

But, because we're lacking metrics to ensure the tool provides the data or that it provides it in a consistent manner, it's just not acceptable. So, there's a few suggestions. Again, I didn't write up an actual recommendation, but there could be service-level agreements put in place to ensure the interface works reliably.

Then, specific metrics. How many times are fields returned blank? What challenges does that provide? Is that because it's missing in the WHOIS record? That's an accuracy problem. And is the data displayed consistently across all the TLDs? Do all the gTLDs return the results consistently? And is there a problem with specific gTLDs that we should be looking at? How big or small is this problem? Without some basic metrics, you don't know if this is a problem.

Anecdotally, I've tried on several times to look up different domain names just in my day job and I had problems with dot-science, dot-live, dot-film, and there was a fourth one. I went back a few days later to look them up. Is it just me? Was it my user error? I have no idea

because there's no metrics. So, the recommendation is sort of define metrics and/or SLAs to be tracked and evaluated to determine consistency of results of queries and use of tools. That's just a draft recommendation.

ALAN GREENBERG: Anyone? Then, I'll take the first shot. You're implying that in a case like the dot-science you were looking at, the implications are they couldn't get through to the registry to give you the information?

SUSAN KAWAGUCHI: Or registrar.

ALAN GREENBERG: From the registrar. Well, dot-science is a new one, is a registry.

SUSAN KAWAGUCHI: [inaudible].

ALAN GREENBERG: Okay. But, as far as you understand, they don't track the inability to contact the registry, so they have no statistics at all. If something is a failure, they just return, "Sorry, we didn't get it," and don't even count that? That's about as shoddy a programming as I can imagine.

SUSAN KAWAGUCHI: Yeah. They said it was very difficult to go through the [inaudible].

ALAN GREENBERG: Alright. One other thing. The recommendation said overhaul internic. I believe they wisely chose to ignore that and build a new system.

SUSAN KAWAGUCHI: I do, too, yeah.

ALAN GREENBERG: And for that we can take off our hat and say thank you. But, you can still go to internic and it still returns the same feeble information you had before. There's no message there that this is a – in common parlance – this is a depreciated service. That is, we recommend you don't use it anymore. Nor does it actually just refer to the other one. So, it still exists for people who don't know about the portal and no indication that this isn't where you should be. That, again, I think is rather shoddy. If you come up with a new service, you should have some way of referring people to it. Lisa?

LISA PHIFER: So, I want first to clarify the point about not tracking failures. So, my read of the implementation briefing was that they have that information in logs. What they don't do is track any metrics associated with it. So, to go back now and dig it out of logs would take some effort, and I believe what Susan is suggesting is that there be some more proactive tracking of metrics and perhaps a comparison against SLAs to ensure that common interface is in fact reliable.

I wanted to ask a couple of questions. The original impetus behind this recommendation was lack of commonality in query interfaces at the time of the WHOIS1. I was wondering if, with transition to thick WHOIS, and with common labeling and display, if you felt like the need for common interface was still the same as it was when the first review team recommended this.

SUSAN KAWAGUCHI: Yes, until and if – of course GDPR may change all of this, but until dot-com, net, and jobs or whatever goes thick, the same challenge exists. The other confusing issue is the ability for registrars to rely on resellers to provide WHOIS, which still exists in the RAA, that they can rely on their resellers and not provide WHOIS lookup.

So, in the thin registries, that challenge still exists because you can find a domain name, look up the registrar … You can get the thin WHOIS if it's a dot-com or net, for example. You look up the registration in the thin because you have to find the registrar first to go to. You can use paid services which help, but a lot of those are only like 85-90% of registrars. At least that's what it used to be four or five years ago. Even domain tools doesn't get 100% of all of the … If they're telling you they do, they don't. And maybe they're closer to 95 or something or even 99, but there's always going to be some registrars that are not going to play nicely and give that information over, and domain tools, again, park that for GDPR but those kinds of services could go away.

So, you would go look up … And sometimes the registrar would be listed. Sometimes it's the reseller. But, you didn't know who was

actually providing the WHOIS service, so then it was a mystery. Literally, it would take 20 minutes to sort of figure out the puzzle. “Oh, I got them now.”

I did that for a living. I was looking … Up until I left Facebook, I usually did at least 100 WHOIS queries a day, so I was pretty used to it, and without relying on domain tools or something or another service, then it just was very cumbersome and here we are trying to educate users to know who they’re doing business with, the whole outreach thing. That was quite a challenge to even understand what a WHOIS record was and find it. So, until we get all the registries are thick registries, I think that’s a problem.

ALAN GREENBERG: I’m sitting here with sort of a level of astoundment at some of the things you’re saying and some of the things you’re not saying, going back to the logging versus tracking problems. ICANN is not the largest organization in the world. We may look at 400-something employees and say it’s loaded and large. But, on the other hand, it’s not a really big organization and compliance is one of the key parts of ICANN.

The concept that ICANN is running a WHOIS system which is regularly recognizing you cannot get to a registry’s WHOIS or you cannot get to a registrar’s WHOIS and it’s not logging those for compliance to look at, I find unbelievable.

SUSAN KAWAGUCHI: No. I'm not saying the report says that they're recognizing that. They did indicate that there was sometimes blanks in the fields returned. But, they don't know. They don't really know. And, actually, I don't know. Did I do something wrong when I plugged those in? I don't know. I'm just working away and going, "I can't get it here," and go somewhere else. I was trying to use the tool because of this subgroup.

ALAN GREENBERG: You were told they were logging things, but not keeping actual statistics. Well, if they're just logging it in a historical log, then they're not notifying compliance either that there's a failure to [inaudible] and that's the part that blows my mind. You have a ready source of information about failure to comply and we know some registrars are not providing WHOIS and you're not taking advantage of that information. That is the part that blows my mind.

SUSAN KAWAGUCHI: Well, there we are. Compliance is reactive. They're not proactive. And I think that may be a major recommendation that we make, an overall recommendation for compliance that would also work for common interface for data accuracy is compliance … You have to change your model for compliance. You have to be proactive.

ALAN GREENBERG: And if ICANN is running another non-compliance service that could provide valuable information to compliance, it shouldn't be hoarded. It should be shared.

SUSAN KAWAGUCHI: Yeah. So, back to this. I don't have any … To me, if the Internet service still exists, I don't think that's a negative, but maybe there should be some sort of indication that you'll get a better result—

ALAN GREENBERG: I'm not sure we're going to make a recommendation out of it. We should certainly note it. Lili?

LILI SUN: Actually, to be honest, before I went through Susan's draft report, I didn't even know the internic.net. Yeah, I didn't even know that. I thought that whois.icann.org. After I went through your report, I [inaudible] two portals for the WHOIS lookup. To be honest, the whois.icann.org seems to be more user-friendly. Yeah, I just checked once just now. It seems that the internic.net, they hide the personal contact information. So, it seems like, yeah, it's already GDPR compliant. But, for the whois.icann.org, it still shows the personal contact information. That's the only difference now.

ALAN GREENBERG: That's because for dot-com and dot-net, all it's doing is querying the registry and it's only showing the thin data. All the other registries hold the thick data, all of it. It shows whatever it gets from the registry and those registries and dot-jobs are the ones that only have thin data in the registry. It's not hiding data. It's just not getting it and it's not doing the

next step, which is what Susan was talking about of figuring out who the registrar is and going to the registrar for the additional data.

SUSAN KAWAGUCHI: internic.net has been around forever, but I'm glad that you knew about the other one because it is much more efficient.

ALAN GREENBERG: Unless of course you're watching ICANN's tutorials, which they only tell you about internic. Any further comments on common interface? We have a break at 10:15 and it is 10:15 exactly. Enjoy your break, 15 minutes.

We are reconvening on part two of the morning of our second day of face-to-face meetings on the 17th of April. That is the RDS WHOIS2 Review Team. We will look at recommendations on privacy-proxy providers. Susan?

SUSAN KAWAGUCHI: Thank you. This is rec 10, proxy-privacy. If you've read the … Well, I'm sure you've all read the recommendation, but this recommendation gave some latitude on how to sort of oversee privacy and proxy providers and to regulate them. If you look down, we ask that … The Review Team 1 asked to review existing practices because there was good, or at least one good, proxy-privacy service provider that would actually respond and reveal, which sort of stands until today, that GoDaddy does this routinely through domains by proxy and other ones don't. The review team suggested a possible approach, which was an

accreditation system and provided goals, which I think this may have led to … Well, this has not been implemented yet, but it's in the process of being implemented. But, I think the way this … In reviewing all of the other – some of the other – recommendations, as I'm reading this one again, then I realize this one sort of spells out more of what we intended.

So, the goal of the process should be to provide clear, consistent, and enforceable requirements for the operation of these services and to strike an appropriate balance between stakeholders with competing but legitimate interest, and we even outlined privacy data protection law enforcement and the human rights community. We also suggested that you could use a mix of incentives and graduated sanctions to encourage proxy-privacy service providers to become accredited and to ensure that registrars do not knowingly accept registrations from unaccredited providers. ICANN should develop a graduated and enforceable series of penalties for proxy-privacy service providers who violate the requirements with a clear path to decreditation for repeat serial or otherwise serious breaches.

So, it's a pretty detailed recommendation. Then, the 2013 RAA introduced a specification privacy-proxy somewhat based on this recommendation and the work has been going on since then. So, there was a PDP for PPSAI and currently the IRT is working on this problem.

The subgroup reviewed the report – and I'm sorry, I didn't introduce the subgroup members for this was Volker, Cathrin, Stephanie, and I. Volker really is the rapporteur, but since he's moving I took this on. So, the review should encompass the work completed both through the RAA

specification and the PPSAI PDP and whether the agreed-upon details adhere to WHOIS1 recommendation 10. We looked at all of the documents – I keep scrolling. I'm probably [inaudible] you. Based on the analysis, so I'm on slide 103. I think it's 103. Nope. It's 103. I just pulled up the main document. It's the chart. There we go.

We broke up the parts of the recommendation, clearly labeling WHOIS entries to indicate the registrations have been made by privacy or proxy service. That was addressed in the PPSAI report, providing full WHOIS contact details for the privacy-proxy provider which are contactable and responsible. That was in the PPSAI. Volker indicates here that details of the standard report processes are still being debated, but there's definitely a consensus that this would be done.

Adopting agreed standardized relay and reveal processes and timeframes. These should be clearly published and proactively advised to potential users of these services so they can make informed choices.

Law enforcement relay and reveal processes were not detailed in the PPSAI PDP Working Group report, but that work has been continued in the IRT and I think Cathrin is still continuing, right? There's no agreement complete.

CATHRIN BAUER-BULST: Yes, the work still continues and there's a couple of sticking points in particular on the timeframe for response where law enforcement has set a 48-hour period as their target and the privacy-proxy service provides say that's not feasible for possible smaller privacy-proxy service providers.

SUSAN KAWAGUCHI: So, that is to be done, finished. We'll see where that comes out. Carlton, there's a draft right now?

CARLTON SAMUELS: Yeah. There's a draft for the [inaudible] framework in the PPIRT.

SUSAN KAWAGUCHI: Yeah. So, part of this is defined under the 2.4.5 of the RAA, so that work, we'll see. That's one of the hurdles that has to be overcome before this is actually implemented. Registrars should disclose their relationship with any proxy-privacy service provider. That's in the PPSAI partially defined in the 2.3.

Maintaining dedicated abuse points of contact for each provider. That is a separate policy that was implemented and this IRT has agreed that that fulfills that.

Conducting periodic due diligence checks on customer contact information.

Volker drafted this part. Review has shown no such checks are currently envisioned. Implementing such reviews may violate the reliance of the underlying registrants on the privacy of the data. I don't agree with that. I didn't want to change it because it was really his. But, it would be problematic to collect inaccurate data and return inaccurate data, which is going on today. I would say in my personal experiences, it's almost 50% when I was at eBay and then at Facebook requesting, and the only

one that reliably had a process was GoDaddy and domains by proxy, but I would say about 50%. That's an anecdotal statement there. But, the data was either incomplete or inaccurate and it was usually really obvious that it was inaccurate.

GoDaddy had an okay process that if you said … Sometimes they would just suspend the proxy and/or suspend the registration because it was so obvious this information was bad. Other times … They always included a caveat with returning the information to us that we requested, that if you think this is inaccurate let us know, and I would write back and go, "This is inaccurate. This is not … Tom T in China is not enough information to do what I need to do."

So, I think that I need to go back to the IRT and look to see where we really are. Stephanie, did you have a …

STEPHANIE PERRIN: I should first say I did absolutely nothing – none – of the work on this. Let's just be clear. Similarly, while I'm on the IRT, it conflicts with another group, so all I do is monitor and watch what's going on. It's hard to keep up.

But, I'm just clarifying that when you were … Your sample for deciding that 50% were inaccurate, which I'm not questioning, that's a sample based on … You're investigating them, so the odds are pretty good that they're engaged in bad behavior of some kind anyway, right? No?

SUSAN KAWAGUCHI: Well …

STEPHANIE PERRIN: It's not really random. So, they're engaged in something and I want to contact them. That doesn't necessarily … The enforcement that I did routinely for almost 20 years between the two companies didn't necessarily include negative behavior. Some of it was definitely fraud. Some of it was just people don't understand trademarks and don't understand … They're a fan of the company and you need to explain that. But, there was nothing necessarily harmful – intentionally harmful, let's put it that way. I would say probably about … And I manage probably somewhere between 15,000 to 20,000 enforcements a year between four brands when I was leaving Facebook. I would say about 30% of those was we wanted to contact them to make them understand, "No, you can't name your ancillary service you developed Facebook Whatever or WhatsApp Whatever." It may be a great service. We have no idea because we don't look at that. But, you need to change your branding and create your own brand.

So, to me, it's not necessarily. This is something literally in 2000 when I started doing a lot of that – I did that previous to eBay, too, whatever another company. It did not seem … I felt, as a company, a major brand – and I don't know how relevant any of this is, really – but my strategy and philosophy in that enforcement was is you get to those people quickly because they didn't understand and were not educated about, so they didn't waste a lot of their own resources. Don't let them develop a whole business model that they think they can rely on to feed their family and spend money. We tried to get that out really quick.

Now, the bad guys, they don't care. But, there was a certain percentage. I would say roughly 30% that was just, "Hey." And they would respond and go, "Oh, I didn't have any idea," or, "You're a big, bad company. You can't make me do this." Then, I'd educate them some more. Sometimes I'd say get your own IP attorney because I've got lots of them. Sometimes that was where I had to default to.

But, for the most part, they were like, "I had no clue. I just assumed because the registrar let me." Of course the registrar let them. The registrar can't make that evaluation. To me, it was more of a friendly outreach. Not everybody would have viewed it that way, but that is …

STEPHANIE PERRIN: Funny they would even know to use a proxy service. You ever register a domain with GoDaddy?

SUSAN KAWAGUCHI: A little hard to get out of it sometimes.

STEPHANIE PERRIN: Yeah, yeah. And it's real money.

CARLTON SAMUELS: Review conduct [inaudible] customer contact information. You've been following the IRT. One of the requirements for the accreditation is that you have to … This is when you take out the proxy service provider's contact information in lieu of the customer. The registrar is obliged to

change the record because the record is inaccurate now if the proxy service provider is deaccredited, and required to suspend the domain name if the [underlying] customer does not change their proxy service provider relationship.

So, at some level, there has to be a periodic check by the registrar to ensure that the proxy service provisioning is intact. I'm not sure I agree with Volker on that at all because the rules already say that you must check periodically to see if the proxy service provisioning is still intact.

SUSAN KAWAGUCHI: Yeah. Like I said, I didn't agree with that.

CARLTON SAMUELS I'm agreeing with you. I think Volker is wrong on that one.

SUSAN KAWAGUCHI: Unfortunately, he's not here to defend himself, so we'll just say Volker is wrong.

CHRIS DISSPAIN: Say he's wrong, take it out.

SUSAN KAWAGUCHI: Exactly.

ALAN GREENBERG: That means we will note which of the number ones he is wrong on. No, no. I'm just noting each of these items is numbered number one.

SUSAN KAWAGUCHI: I didn't do that part.

ALAN GREENBERG: I'm not blaming you. I'm just saying if we're going to bring something up with Volker, we need to be able to point to it. All I was asking.

SUSAN KAWAGUCHI: Okay, moving on. Maintaining the privacy and integrity of registrations in the event that major problems arise with a privacy-proxy provider. That was included in the PPSAI report for maintaining data escrow.

Providing clear and ambiguous guidance on the rights and responsibility of registered name holders and how those should be managed in the privacy proxy. Partially defined in some of the RAA. He puts a question in here. How effective are these rights and responsibility regarding the effectiveness of proxy registration and the protection of rights of others? I'm not sure, actually, what he's getting at there, so if anybody else on the team. It's the last one.

CARLTON SAMUELS: I'm not sure what he means because there's two things. One, if you have a proxy service provider who is using their contact data to shield yours and they lose the accreditation, they are required in the

regulations now to give you at least 30 days' notice that they are going to be deaccredited and the underlying customer has the right to opt for a new service provider or failing that they did not opt for a new service provider in that 30 days, the registrar is required to suspend the registration.

If you opt to have a new proxy service provider and that proxy service provider is staying with the registrar, then all you need to do is tell that registrar who the new provider is. If you're going to be a different provider, it might include transfer of the domain name to another registrar and the incoming registrar is required to accept a proxy provider, so long as the proxy provider is accredited. Isn't that the way it works? So, there's a whole set of responsibilities in transferring proxy service coverage between registrars.

SUSAN KAWAGUCHI: I thought this one actually … Because it says rights and responsibilities of registered name holders. So, if this is relating to the underlying contact information which is the underlying registrants … That's shielded, but you still have a responsibility for the, for example, domains by proxy and that's just the service I'm most familiar with. With their [inaudible] of you have responsibilities and agreed to responsibilities in their [inaudible] that are not mandated by the RAA to not infringe a trademark, not to commit fraud, not to … So, I think that's … This may be getting to both of those points, your point and mine.

There's always this ambiguity between the proxy provider going, "Hey, I'm just a proxy provider," but they won't get out of the way all the

time. Domains by proxy does. They won't get out of the way and provide the information, but the registrant is actually a bad guy in committing some sort of fraud or abuse, so you can't get a hold of them because you can't get the proxy provider to do what they should do, to do the right thing. So, I think that is what this aims at.

I haven't checked this in like a year, but domains by proxy, for example, has always had the option of not receiving any e-mail relayed through the e-mail address of record on the domain registration, which to me, is a complete violation of your responsibilities as a registrant, but you could say, "Nope, don't send me any e-mail that comes to that proxy e-mail address." I have a screenshot from several years ago I'd have to look for, but I haven't checked it. They could've changed that in the last year or so, but that was one of the things we were trying to get at for the WHOIS Review Team was, "No, no, no. Just because you choose to protect your information, that's great." Everybody has a right to do that in certain cases. But, you don't have a right to not respond in some cases or at least receive e-mail. But, they were protecting them from spam. Well, there's a lot of spam filters. There's a lot of other ways of protecting spam and not receiving anything to the admin e-mail address of a domain registration just seems to be counterproductive and an abuse.

ALAN GREENBERG: Yes and no. The registrant of record is the proxy provider, so they have an obligation to respond even if the original registrant doesn't.

SUSAN KAWAGUCHI: But, they don't.

ALAN GREENBERG: That's a different matter. So, it's completely reasonable for them to offer an option to the original registrant, whatever they're called, as long as the registrant of record responds. But, it has to be one or the other. You're saying it isn't and I'm agreeing that that is a violation. You can't force to pass it on, but somebody should be responding.

SUSAN KAWAGUCHI: I would say that this recommendation intended to force them to pass it on. Yeah.

STEPHANIE PERRIN: I would say that that last bullet – and obviously I can't imagine what Volker had in his mind, but for the layperson to understand their rights and responsibilities, particularly vis-à-vis law enforcement and access to their data, that's not easy. They have certain rights under different data protection laws. I think the proxy providers have a requirement to explain all that to them.

When we were on the review team, I was startled to learn that actually sometimes registrants didn't understand whether they were actually the name holder or whether it was the service that was the name holder and they were just using it, borrowing it as it were, and they had no real rights; and therefore, their trademark rights might be diminished. All of this stuff has implications.

A quick skip through the providers, at least the last time I did it, which was quite a while ago, nobody was really providing decent information about what was going on and that matters. Obviously, it matters to crooks, but it matters to innocent people, too, and it certainly matters to people like human rights defenders just how easily the data is obtained by hostile governments. I think that probably could support a fairly robust recommendation with regards to transparency.

ALAN GREENBERG: I have a question not on the details, but where we are in this overall process. What is the prognosis for actually implementing the results of the PDP and having privacy-proxy providers that are accredited and working under the new set of rules? What's the timeframe people are envisioning?

CATHRIN BAUER-BULST: The current temporary arrangement, to my understanding, runs through March 2019. The aim is to have the new framework implemented and operational by then.

ALAN GREENBERG: So, we're going to be reporting before it becomes operational. I'm just thinking about how do we make recommendations to something that still may not be firm at the time that we're writing our report, then? Clearly, we're talking about writing our report at the latest third quarter of this year. That puts us at a rather funny situation. By the time it's published, and certainly by the time the board responds to it, we will

have an infrastructure in place which we may or may not have understood where it's likely to be going and certainly will not have seen it. So, it puts us in an interesting position for writing any further recommendations.

CATHRIN BAUER-BULST: I just had another small point on the last number one following on what Stephanie was saying. I fully agree that informing the registrant about the rights and responsibilities is a key task of the privacy-proxy service provider and I was just thinking through the feasibility of the different kinds of rights and where they stem from to provide the right information.

For example, if you look at the European data protection rules, it will depend on which jurisdiction you are in how the remedies work, for example, and not so much on the jurisdiction of the privacy-proxy service provider. So, it might even make sense to have a more centralized overview somewhere that provides guidance based on the jurisdiction of the privacy-proxy user, that then the privacy-proxy services might be able to refer out to in their own instructions and several people could cooperate on keeping updated, because otherwise, we might be asking a bit too much of them in terms of providing universal information for all their users regardless of where they come from.

By contrast, I think it should be fairly easy to have a standardized document that describes the rules and responsibilities that arise out of the ICANN context itself and out of the registry and registrar

accreditation agreements and other such documents. So, just maybe to think about differentiating there in terms of what burden we impose also on the privacy-proxy services.

ALAN GREENBERG: Anyone else?

SUSAN KAWAGUCHI: I think that would be a good recommendation, actually, and something that might be feasible to implement once … Without going back to – this would just be [inaudible] to the common interface. Here's the information about privacy-proxy.

STEPHANIE PERRIN: That would certainly solve the problem that different law enforcements have different requirements vis-à-vis the disclosure to individuals about whether in fact their data has been accessed. So, you can have it all in one place. It's a lot for a registrar, as you point out, to know.

SUSAN KAWAGUCHI: And to keep it up to date I think would be really difficult. Okay, so we'll go onto the next slide. These are some issues we did not develop recommendations. It looks like maybe we discussed one we could flesh out.

So, issue number one – and I'll just give you my … I don't agree with this, but this is definitely Volker's proposal here that current funding

proposals for accreditation program create concerns of ICANN failing the goal of onboarding all providers of such services due to inflation of costs. ICANN Org staff seems to be unable to justify proposed accreditation fees, which may endanger the entire program.

So, I think the accreditation fee is $4,000 and that may be yearly. I haven't paid that much attention, so if the three of you can remember. The registrars are concerned. I understand the bottom line is tough sometimes for a registrar, but the reality is, in my opinion, is there are expenses to running this program in accrediting individual registrars and enforcing all the compliance and the contracts and that may be a justifiable price. I don't know if anybody wants to argue for Volker's stance there. Poor Volker, he's not here.

CARLTON SAMUELS: If you look at all the things that are required based on what the IRT is putting out there now, it seems to me that fee is lowballed.

SUSAN KAWAGUCHI: I would agree with you.

CARLTON SAMUELS: Do you have to do the checks? Then, you'll have to do all of the processing, then you have to do the constant checking to see if they're in compliance and you have to be prepared to respond to allegations of non-compliance. All of that is in the framework. You have to decide. That is a whole lot of churn there. I don't know what the number is, but

that number seems to be, to me … [inaudible] period of time, so yearly fee, annual fee, or whatever it is. I don't know.

ALAN GREENBERG: Two questions. I find the wording he has here curious. ICANN Org staff seem to be unable to justify proposed accreditation fees, which may endanger the entire program. Well, I think what he means is they are unable or unwilling to provide justification and a level of fees may jeopardize the program, presumably, not the inability of presenting them.

My inclination, without having followed this closely, is $4000 doesn't sound like an awful lot if you're actually going to run this kind of program. I can conceive of the second year being slightly lower, but probably not a lot.

But, I have a question. When we started talking about privacy-proxy, we were saying we were not only going to enforce it against or have the rules for those who are providing a formal commercial service, but Joe Lawyer who happens to register things in his name on behalf of his clients would have to be accredited as a privacy-proxy provider. Is that still the way it's playing out or are we looking only at real commercial services?

CARLTON SAMUELS: The way it panned out is as long as you are providing the service, then you have to be accredited. As long as you're putting your name is in

front of somebody, it's aimed to shield, then it's a service you provide and you must be accredited.

ALAN GREENBERG: Same lawyer who incorporates a company in his own name but also would register the domain name at the same time prior to the company being launched would have to be according to these rules, scrupulously a privacy-proxy provider.

CARLTON SAMUELS: Right.

ALAN GREENBERG: Okay. I could certainly see a different fee level for different classes of privacy-proxy providers, but not necessarily even treating a small registrar different from a big registrar. Chris wanted to say something, then Susan.

CHRIS DISSPAIN: Yeah. I don't want to get intensely legal about it, but in reality, it's the reason why you're doing it. If you're doing it because you are providing a service to the client, you're basically, as their lawyer, getting all the ducks in a row so that they can then become registered as the registrant of that domain name. You're not providing a privacy-proxy service. What you're doing is providing an agency service and that's a different service, so therefore you don't need to be a proxy service provider. You just need to make sure that you transfer the name across when it's

necessary. You're not breaching any rules and you don't need to be accredited to do that. It's a completely different service.

ALAN GREENBERG: The reason I mention it is when the initial discussions were held, the answer was, yes, even if you're a lawyer doing this for three clients, you need to be a formally accredited service, which made no sense, but that is the words that were being used when I was last involved a long time ago. Cathrin?

CATHRIN BAUER-BULST: Thank you. Just to suggest that if there is an issue with the fees, one thing that we might want to consider is to recommend that there be sliding fees based on the number of privacy-proxy registrations that a company has, so that there would be higher fees if you have hundreds of thousands of registrations and lower fees if you're a lawyer just doing this ten times a year for your client whose trademark you're protecting or something. That might be something we could consider, and then maybe we can knock $1000 off the $4000. I'm not sure how they calculate it. The added bonus could be that you have an overview of how far, how many registrations there. I mean, I guess that could also engender … I'm just thinking this through as I talk. Could also provide an incentive to underreport the number of registrations you have, so you could also do it in reverse, that you knock off a certain percentage of the fees if you have below a certain number of registrations a year.

ALAN GREENBERG: Stephanie and then Carlton.

STEPHANIE PERRIN: I was just wondering how this whole decision of having a flat fee instead of a per-registration evolved because it does seem to me that a per-registration might be a little fairer. You might offer the service and then only have ten registrations, in which case you'd be getting, say, $400 as long as the price doesn't double, triple, or quadruple. Just wondering.

ALAN GREENBERG: Carlton and then me.

CARLTON SAMUELS: The reason that I thought it was a flat fee because it wasn't the subject for the registration and the accreditation is not the underlined registrant is the person providing the fee. And all of the things that have to do to accredit, I have to do it regardless if you have ten or 10 million customers. And the fee is for accreditation and the management of that accreditation process. That is why I strenuously objected to having a per-user fee because it is not the underlying user that is the focus of the exercise. It is the provider. And all the things I'm doing is a fit and proper test for the provider. Not has to do with the client. The provider. That's why I am on the side that says it's the provider that I'm concerned about accrediting, and everything, all the administrative exercises that I would do is directed at that provider, not the [inaudible] clients that they have.

ALAN GREENBERG: Thank you. I'll point out that Volker's wording in here is the justification, and indeed, Carlton, I think you're right. If the costs are purely associated with the accreditation, then they have to be attributed to that. On the other hand, in the real world of commerce outside of ICANN, there are many, many examples where the pricing is determined to, number one, make you a profit if you're a profit-making organization and to be acceptable to the community. So, if ICANN has a certain revenue they need to have to run the service, then you could price it as $1000 accreditation and three cents per registration. That would end up generating the right amount of revenue and be more acceptable to the wide range of clients. It's not fair, but it may be the commercially viable solution.

I personally am more interested in making sure it works than making it fair. The people who are going to pay more for it clearly will not agree to that. The people who pay less will say, "Sure, why not?" That's a decision that has to be made. We stand to have lunch an hour and a half early.

SUSAN KAWAGUCHI: I just wanted to agree with Chris on his analysis of an attorney or a law firm providing. It's not really a proxy registration. I think one of the challenges with this program is going to be identifying all the different proxy providers around the world where we really have – ICANN will have leverage is with existing registrars that are providing a proxy service is that they are then required to be accredited. It will be easier to identify that they actually have accreditation services or a proxy

services and so it'll be easy to target them and say you need to be accredited.

Also, I think the fees for that accredited were they started out using the same fee level as becoming a registrar. So, because there's credit checks, there's all kinds of background checks, there's expenses.

Not to channel Volker here, but one of his arguments is if these truly are going to be existing registrars and not standalone proxy services that have no business dealings or relationship with an existing … If they are only – for the most part – registrars that have a service, then that registrar has already gone through those checks. So, there could be some duplication of efforts and I think his pushing back has made them think about that and staff has come back.

But, in the case where maybe they do, in this new world of GDPR, people, maybe this is a service that is launched separately from the registrars and people want a higher level of service to protect their information. Sort of like this cured credential program. What did we call that in the EWG? Yeah. Something like that. Then, if there's no current relationship with ICANN, then those fees are all … Those make sense to me.

ALAN GREENBERG: Chris?

CHRIS DISSPAIN: Yeah. I only just wanted to draw a distinction between … If I want to just hide my details, it's pretty easy for me to hide my details, right? We

used to find in Australia I think something like 30% - and I'm just dragging these figures from the back of my brain, but something like 30% of new small business registration in com.au were registered in the name of the web designer on behalf of the client and the client usually didn't even bother to think about that and there would only ever be a problem if the web designer didn't get paid and then suddenly would say, "It's my name," and it wasn't because we had reasons why you had to be eligible for the name, right?

What this is supposed to be doing, I think, is the opposite of that which is I specifically want my information to be hidden by someone who provides that service and will only reveal that information under an agreed set of guidelines which I have – and therefore, I'm going to pay for that. And if we're expected to run some sort of a system that deals with accrediting and maintaining accreditation of those people, then clearly that has to be paid for and it can only be paid for on a work done basis rather than a number of names you have on the management basis, [otherwise] it doesn't make any sense. Thanks.

SUSAN KAWAGUCHI: Just one quick comment. That is the worst thing that any small business can do.

CHRIS DISSPAIN: Oh, I know.

SUSAN KAWAGUCHI: I have unraveled so many of those it's ridiculous. People hold them hostage.

So, issue two, impact of GDPR data redaction requirements on proxy services are yet unknown, but significant impact is expected as personal data becomes hidden by default without use of privacy services.

Yes, but we don't know what the GDPR is yet. Anybody have comments on that one?

ALAN GREENBERG: Lisa, do you want to go? I was going to say when you look at ICANN's proposed model and we're now in a situation where we may well be hiding the information about the proxy provider. If we're treating legal persons as natural persons, then you can't even find out there's a proxy provider there.

CHRIS DISSPAIN: Yeah, let's have everyone treated the same way, then. Makes perfect sense.

ALAN GREENBERG: Says the formal statement from a director of ICANN.

CHRIS DISSPAIN: Now, you know that that now forces me to say that I was not making a formal statement.

SUSAN KAWAGUCHI: Okay, so issue three is just a recommendation that they implement a suggestion to the … I'm not sure if it's a recommendation.

CHRIS DISSPAIN: Sorry, Susan. [inaudible]. Lisa just asked a perfectly sensible question to me, which is, "And so, what is the issue?" Issue two is what. That's just a statement. I'm not clear what the issue is.

SUSAN KAWAGUCHI: The only thing I gleaned out of this, and we'd have to ask Volker, is I think it may go back to issue one that they incur this cost and then all of a sudden their proxy services, they have no business.

CHRIS DISSPAIN: Again, to be clear, inasmuch as – we keep saying we don't know what's going to happen with GDPR. One of the things that we do know is that there is GAC advice that you shouldn't treat personal name registrations in the same way that you would treat corporate name registrations. I'm paraphrasing. There's also GDPR. Sorry. There's Article 29 advice that even if it is a corporate registration, the personal data should still be redacted. But, the fact that corporate – if you assume the other advice ends up being followed, then recommendations about privacy-proxy services are obviously relevant because that will apply across corporate registrations and corporations may well [inaudible] organizations, whatever they're called – may well want to buy that service. So, I still

think it's relevant. I'm just not sure what the issue in number two is meant to cover.

ALAN GREENBERG: The issue we and perhaps privacy-proxy services are spending a lot of money on something which may or may not be relevant in the current format right now. So be it. Well, let's go home then. Stephanie?

STEPHANIE PERRIN: Is it reasonable to recommend or comment that the entire fee structure should be reexamined after a year of implementation? I can understand the concern … I think I'm well up on GDPR and privacy issues generally, but I couldn't guess whether people will now become hysterical about their domain privacy and all want privacy-proxy services on top of their GDPR protection or they will all, on the other hand, think they're protected even though they aren't and drop their privacy-proxy services. Chris is looking extremely confused.

CHRIS DISSPAIN: I understand the point you're making, but [inaudible] fees.

STEPHANIE PERRIN: My point is that on Volker's recommendations, I mean the principle argument being that ICANN staff are unable to provide a cost rationale for the $4000 each accreditation fee. And if indeed the volume drops, then this is not a profit-taking measure or they will have to triple the price of proxy services. That I think is a reasonable concern and it is

reasonable in a well-managed organization to go back and … Alan is looking like I'm proposing eviscerating dodos on the beach and having a barbeque. This isn't a crazy idea. You don't know what the costs are going to do. Revisit in a year, for God's sake.

ALAN GREENBERG: You misread my look, but I'll let you finish.

STEPHANIE PERRIN: Well, I didn't actually think you were going to raise dodos, but you were looking perplexed. You get my point? We should revisit in a year. That's a reasonable recommendation and that might solve the registrar's anxiety about this.

ALAN GREENBERG: As succulent as dodo meat is when broiled on a beach … Oh, this is getting silly. I don't think it is our job to make a recommendation because Volker has not been sufficiently successful on the IRT. I think it's a completely reasonable thing for the IRT to say this should be reevaluated in a year. I think it would've been reasonable for the PDP to say it should be reevaluated in a year. For us to make a recommendation while this whole thing is in flux in that area I don't think is completely reasonable at all. Thank you. Cathrin?

CATHRIN BAUER-BULST: I'm also wondering whether we're here to make recommendations on business models. Maybe people have to make their own choices. I

would just argue that what the accreditation fee is designed to serve is not just the one-off process of certifying that the privacy-proxy service provider is fit for service at the point in time when the accreditation is issued, but there's also a compliance element involved and there's two ways of financing that. One is to do that through the accreditation fee up front and then perhaps have this annual fee, then it would make sense to have it based on the number of registrations to the privacy-proxy service because the compliance verification needs will scale with the number of registrations.

The other way of financing this is by way of fines. So, you either do it through the accreditation fees or you do it through the fines that you apply if there is a violation. And as of now, I don't really see that there is a fine structure, so we would need to cover this somehow with the accreditation fees. If we do want to recommend anything on that, we should keep that in mind.

ALAN GREENBERG: Susan?

SUSAN KAWAGUCHI: Thanks. So, not to jump ahead too much, but I think issue four we sort of fleshed out a little bit. We've talked about maybe there could be incentives. Anyway, we'll go to issue three and this is something I put in here, that this implementation should not be delayed because we may need this more than ever once GDPR goes into effect. So, we need a proxy … Especially if in Stephanie's example that someone decides they don't trust the accreditation process that eventually will be developed

to go along with the GDPR and I know we're supposed to park the GDPR stuff, but it's hard. That they would also put a proxy on it. So, you get one. You'd see domains by proxy, then go, "Oh, all I get is the registrar." You're not going to get very much in that reveal. That just makes me sick to my stomach thinking about that process.

But, we do need … There should be absolutely no reason – and I have not heard anybody express that we should wait and not implement this, but I think we should make the suggestion if we see that still happening … If we see something being derailed down the way when we were writing the final report, that we should make a suggestion. I'm not saying it's a recommendation.

So, issue four – and you guys can correct me if I didn't find any … I did not find any relevant discussion of incentives and the recommendation suggests using a mix of incentives and sanctions to encourage and enforce this policy once implemented. There's been the compliance component I think has been well-discussed, but I did not find anything on incentives in the report of PPSAI PDP Working Group report. So, maybe – correct me if I'm wrong.

ALAN GREENBERG: The incentive is we won't take sanctions.

SUSAN KAWAGUCHI: In that discussion with the fee structure, maybe there could be incentives like you have no problems in the first three years, no compliance actions, and maybe you get a reduced fee or something. I

don't know. But, it wasn't addressed. We could recommend that they [inaudible] an incentive.

CATHRIN BAUER-BULST: I also don't remember mention of incentives. I certainly wasn't around when it was discussed, if ever. But, I think it's a really good idea and we could take, for example, the example of the car insurance industry which basically says you have a certain rate that you start out with and then it sort of bottoms out and if you have an incident, it goes back up. I think that's a really good idea.

ALAN GREENBERG: I have a recommendation. The WHOIS report was tabled in mid-2012, if I remember correctly, and was, according to Lisa, the board responded at the end of 2012. By the time we get our report out, it will be the end of 2018, roughly. That is six years.

If the fastest ICANN can move on a recommendation like this is six years plus, we need to fix our processes. That's not a recommendation on privacy-proxy. It's a recommendation on ICANN. If the best we can do as a review team is make a recommendation that will see the light of day seven years later on what was a relatively straightforward issue, though there are some complexities to it, we've got to get our act together. This is crazy. I think that's a recommendation we could make not in relation to privacy-proxy directly, but in general. Thank you.

SUSAN KAWAGUCHI: I wholeheartedly agree and I think that's one of the reasons this review, even though GDPR is going to impact everything, was critical. We have to make that statement and say, hey, we're living on the Internet, guys, but we're back in the 1800s on policy. I wouldn't put that in the report, but …

CATHRIN BAUER-BULST: In the 1800s I believe it was actually easier because there was a monarch to society. I think this is turning into a review of the multi-stakeholder model.

SUSAN KAWAGUCHI: No, no, no. We had a President and a Congress.

ALAN GREENBERG: is anyone here old enough to remember use groups and use net? Alright. A little anecdote. [inaudible] we have very nice, old, elegant building – the faculty club. In one of the rooms where we would often hold meetings, there was a bookcase at the back of the room of old volumes. I went to look at what they were one day. They were from the late 1800s, early 1900s and people would send letters into this service that would then publish it once a week of, "I have an idea." Someone else would, a week later, comment on it. It was use net in the 1800s and was almost as effective even though they were doing it on paper and mail. We think of ourselves as being magic, but we are living in the 1800s at some point. Lisa?

LISA PHIFER: The question I have is that Volker [inaudible] some issues here, several of which have to do with what might happen during the progression through the IRT and actual effective date. Are the recommendations here tied to thee issues, or is it too preliminary to actually formulate recommendations on something that's a moving target?

ALAN GREENBERG: I think I already stated that I think I have a real problem with that, unless it becomes really obvious that the PDP and the IRT are doing something which is very counter to the original recommendation. I don't see that at this point. Stephanie?

STEPHANIE PERRIN: There's something faintly contradictory in our approach here. We can't make an overall recommendation that we're not moving fast enough on some of the implementation of the recommendations, and at the same time say we can't comment on something because we don't know how it's going to turn out, e.g. GDPR, e.g. the IRT and the PPSAI. I apologize for the alphabet soup. Those two are pulling in different directions. I agree with should not give into speculation. As you can see by my dodo barbeque analogy I'm capable of infinite speculation. But, we can't duck some obvious recommendations. You don't like to revisit in a couple of years and check on the economics.

As an ex-government wonk I can tell you – and I feel very forcefully – that we have killed many policy options by pricing them out of the market and pretended that, oh, we were doing the right thing for the

lower levels of society, and we weren't because we priced it right out of their range.

So, if this is giving an added incentive to somebody like GoDaddy to be the only one that can offer privacy-proxy services or if we are creating a new line of business for somebody like domain tools who clearly are going to need some new lines of business, that is interfering with the market and I think we have to take that on board.

So, I think we have to take a measured middle path here between hands off and let's all fantasize about what might happen. That's my point.

ALAN GREENBERG: Lili?

LILI SUN: Regarding the proxy and privacy service, as an incentive on behalf of law enforcement agencies, I'm still deeply concerned about this PNP service will be exploited by criminals. Last month, I happen to run into a privacy provider's contact information when I conducted a WHOIS lookup. I did dig deep into this privacy provider's service. I noticed there are like 100,000 domains registered use this single point of contact information and I did a reverse search about this contact information, the e-mail address listed on this privacy service provider's e-mail address. I noticed there is over 500,000 domains hosted on a single IP address.

ALAN GREENBERG: Fast machine.

LILI SUN: Yeah. More than 400,000 domains were hosted on a single IP address. If you look into this domain, it all pointed to the single web page. So, I [inaudible] Chris and [inaudible] just now. Maybe, yeah, this kind of service is used by the web designers. They just registered this domain name, use privacy and proxy service. Maybe they can just [inaudible] it as a service for the criminals.

Last month, I checked most of the top 20 domains hosted on this single IP address. It's all pornography website and it's all [inaudible] pornography websites. For adult pornography, it's illegal in China. But, the criminals, they are smart. They are getting smart. They just register domains and get the website hosted abroad.

I'm still impressed by Stephanie's comment yesterday regarding the data accuracy topic. ICANN should conduct a risk assessment. I would suggest to conduct a risk assessment regarding the PNP service as well.

ALAN GREENBERG: I have myself and then Cathrin. I guess my reaction to that is that just reinforces in my mind the reason why we have to do privacy-proxy service because at that point if we can demonstrate that this is acting as a privacy service but has not been accredited, then we have the mechanism to bring down the 400,000 domain names instantly and the whole thing just disappears without having the process and the privacy-proxy rules associated with it, we don't have that ability other than by doing it one by one, so I think this is a plus.

Now, that does mean we need to have the rules to be able to demonstrate someone is acting as a privacy service without accreditation. Of course, they might say these are all my personal domains, all 400,000 of them. It's interesting.

UNIDENTIFIED FEMALE: But, we didn't really talk about issue number four, but that's it.

CATHRIN BAUER-BULST: I agree. Just to say that, from the GAC perspective, of course just picking up on these law enforcement concerns, there continue to be some concerns and the three that the GAC has raised most consistently has advised that it will reassess at the end of the IRT are the rules about law enforcement access from another jurisdiction, the timeliness of access and the availability of privacy and proxy services to commercial actors. So, they are engaged in facilitating transactions online where the GAC felt that that was inappropriate to offer privacy and proxy services also because it is not compliant with the rules in a number of countries, including Europe, where there is an obligation to identify who owns a site if you're engaged in a commercial activity targeting consumers.

So, those are three points that the GAC will reassess at the end of the IRT just to add to the issues that the IRT faces, and indeed I think the compliance bit of course, exactly as Stephanie was saying, it speaks to the compliance issues and how we deal with that. In fact, if the outcome would be that you can just take these 400,000 domains offline because of the failure to be an accredited privacy-proxy service provider, then that might be a useful outcome from a law enforcement perspective.

But, if we end up in a situation where compliance is as [inaudible] as it appears to be in some of the other areas that Susan was looking at, then obviously that cannot serve as the response and then we have to recommend something else on top of it.

ALAN GREENBERG: Certainly, the timing of our report in relation to this is less than optimal. Please go ahead, Susan.

SUSAN KAWAGUCHI: I just think that – because, as I mentioned earlier, I haven't been following the IRT closely enough, I don't know what the compliance repercussions are, but as we said in the EWG report, some of the answers to this is swift repercussions for illegal activity and the ability to shut them down. And I don't see why, if you're bringing in, say, half a million new dollars in the compliance branch for the accreditation fees minimum, because I think there's about 100 proxy service providers, are there not? Anyway, let's work with that number. They should be able to hire some people that respond rather quickly to a complaint from you that you have an actor who is not within your jurisdiction, but who is employing a proxy service. Mind you, they're going to quit using them because they know that you could get them under the proxy service, but you can't get them under cross-jurisdictional, but anyway that's a separate problem. But, you could at least kill off the proxy service very quickly and make them go dark. I think that would fit under my accountability for the costs thing.

My worry is that compliance isn't going to do any enforcement. They're just going to take the money and accredit and that's not going to help if they don't investigate.

ALAN GREENBERG: Not clear that compliance is the one doing the accrediting, but ignoring that, if indeed as we get closer to our report there's an indication that the IRT is not taking action to define what compliance can do and make sure that's identified in the agreements that the privacy-proxy services will sign. We're building a new picket fence, essentially, of what compliance can do with this new class of contracted party. I think it is quite reasonable if we do not seem to be going in a direction where compliance can take reasonable and fast action in the area of privacy-proxy providers that we make that recommendation. That I think is quite reasonable if there's not strong indication that the implementation team is working in that direction.

UNIDENTIFIED FEMALE: Philosophically, I agree with you, Cathrin, on the commercial distinction and argued for that for a long, long time until it just … It's not going to win. ICANN doesn't cover content, though I would hope someday we could figure that out.

Then, on Lili's example of the porn sites, and I have done more enforcement on porn sites than I ever imagined, unless there was a trademark infringement, I would have no way of – in the current status, if it was domains by proxy – requesting information on a porn site that was using their proxy service because it may be illegal there, but in the

country that the terms of service is in, it's not going to be illegal. So, I'm not sure this would address your issue, the proxy-privacy process.

I think the registrars or the proxy service would stand back and go, "No, no, no, no. You don't have a right to ask for this information." Sure, there's some way of overcoming that. Do you want to address that, Alan?

ALAN GREENBERG: Yeah. I thought she was talking about an organization that seems to be acting as a privacy-proxy service but is not going to be – would not [inaudible] not be accredited, and we would get them not on the content, but by the fact that they are an unaccredited privacy-proxy service. I think that was the gist.

UNIDENTIFIED FEMALE: Okay, so I missed that.

LILI SUN: It's not only the pornography. Also, it's similar to online gambling. Maybe ICANN asks other colleagues to enumerate more black industry business model. So, it's not only pornography. There are some other cases.

I'm also not quite sure about Alan's comments. Can really the PNP service providers being accredited, we can fix this issue? Even they are accredited, as long as they are not violating the rules, they can still keep on playing this black industry business model.

SUSAN KAWAGUCHI: Yeah, as long as they pick the right jurisdiction to register or establish themselves in. I just don't see that – and I did miss the point that they were pretending to be a proxy provider, but even in that, are they really … I mean, you do have 3.7.7.3 where if you're saying you're a proxy provider and you don't turnover the underlying contact information within a certain amount of days, you could be held liable, but no one has ever tested that. I would have loved to have tested that and there were a lot of reasons I couldn't with both of the companies I worked for.

Even though that's in and I've asserted that language from the RAA with a lot of … When people say, "No, no, no. It's not me. Somebody else is using the domain," they're not a real proxy. I've asserted that. But, the educated ones know, just blow me off.

The other point that you made, Lili, and it was back to Stephanie's point on a risk assessment – and maybe we did capture this yesterday. Maybe we should spend some time discussing: is that an overall, overarching recommendation that we want to make, that a risk assessment should be done and making sure it pertains just to WHOIS or registration data, and really flesh that one out.

CATHRIN BAUER-BULST: Just to add maybe we should also include the question of what happens if somebody does not self-identify as a privacy and proxy service? So, if we have the situation that Lili was describing and the service provider simply says, "Yes, these are my 400,000 domains," do we have any way of detecting that and dealing with that? Then, can we really get them on

the fact that they haven't been accredited of the privacy-proxy if we cannot even prove that they are a privacy-proxy? Maybe that part needs to be thought through, and I have to admit, I haven't thought of that before.

ALAN GREENBERG: Just out of curiosity, Lili, were the 400,000 domains or whatever sample you looked at registered through the same registrar or were they of wide variety?

LILI SUN: Yes. In this case, yes. It's the same registrar. It's based in Japan. It's a privacy service provider and the domains registered on various gTLDs. Yeah. I have the screenshot here, if you are interested. You can come and have a look.

UNIDENTIFIED FEMALE: What's the name of the provider?

LILI SUN: GMA Internet, Inc. Sorry. The registrant name is omamae.com.

ALAN GREENBERG: People have hypothesized what the physical impact would be on ICANN if we could stop all nasty things from going on on the Internet. 400,000 domains hit the dust. Can we afford that to have that happen? Stephanie?

STEPHANIE PERRIN: Oddly enough, that was part of my point, Alan. I was just going to say in terms of the risk-based assessment, if an organization is not doing a risk-based model for its investigations, then inevitably, no matter how hard you work on metrics, they're going to measure the successful ticks in the box on how many stupid things they shut down and they are not going to tackle the big, ugly cases or the ones that are bringing in – what's the math on that? That's a pile of money that ICANN is raking off from that little enterprise there in Japan.

So, I think we have to push for a risk-based approach to investigations and enforcement and that may help solve some of our problems. I don't care who's doing it, but they need to measured on whether they're doing the bad stuff.

ALAN GREENBERG: Back to you, Susan.

SUSAN KAWAGUCHI: Just a quick comment on Lili. I agree with you, by the way, Stephanie. GMO, yeah I've run into GMO a lot. They're just bad players. Again, we could almost put them in the same category as [inaudible] names and that's my personal opinion. I don't have anything else on this. Any other thinking on the proxy? [inaudible] names, which is owned by famous four, which is a registry, owns various registries. So, we have all kinds of contracted parties doing really nasty things.

ALAN GREENBERG: Lisa?

LISA PHIFER: So, I'm trying to think of next steps for this particular topic.

CATHRIN BAUER-BULST: Just to complete. The privacy-proxy services also came up in the CCT Review. Maybe we just want to … I made a note to crosscheck that, but I haven't done it yet, so maybe we just want to take a look at that before we dive into the recommendation more. Sorry.

ALAN GREENBERG: Carlton, provide any insight?

CARLTON SAMUELS: In terms of the CCT Review, the proxy-privacy service provider came up in the domain abuse section. If you read the domain abuse chapter, we have outlined a lot of ways that it is abused. Names is one that we took care of there. It was, I would say, skewed towards the IP international property and those kinds of uses.

Certainly, the recommendation, if I recall off my head, was that we would … This is where the pattern matching became important. We used that as a poster boys, girls for pattern matching requirements saying that we should look at the whole set of miscreants and then apply more specific sanctions to them and pay more attention to them. Stephanie, going back to the risk model, again, and the idea is that we

would have used a [risk] model to determine the ones that we should pay more attention to, and therefore spend more of our compliance and enforcement on those, that they are doing the most damage. That's where that came in.

UNIDENTIFIED FEMALE: There was an actual recommendation that came out of CCT on that?

CARLTON SAMUELS: Yes. We had about four recommendations and that first one was that we [inaudible] more data. I'm just paraphrasing now. We need more qualified data. We should work with outsiders, the [reputation] companies, to get more data. We should use the data to do more pattern matching, and from the results of the pattern matching, we should use graduated sanctions against those who are caught in the pattern matching. We had A, B, C, D, four parts, to the recommendation.

SUSAN KAWAGUCHI: Thank you. So, jumping back to the comment that I wanted to start making earlier, which is what is next steps for this particular recommendation.

We had a couple of issues on the list, which I believe essentially we have actions for Volker to clarify what he meant on those issues. Identified a couple of new issues, one of which was how long it took to develop and begin the implementation process on those policy and the other was related to exploitation of privacy-proxy services.

I guess I heard a sentiment that possibly there are no recommendations specific to this policy right now, but that further down the line closer to our report completion, which would be moving in parallel with the IRT that there might be recommendations to make if we see that things are not moving in the direction that you would hope. Is that a good summary?

ALAN GREENBERG: That specifically was on the compliance one and I think we could sort of pencil in a recommendation that we have to reconsider whether we do it and how it's worded a little bit closer to the end, but keep it as a specific targeted one.

There are certainly a number of concerns that Volker has raised and I think we need to be careful, and with his absence here, we can't have that discussion. But, I think we need to be careful to segregate concerns of the review team with concerns of someone who runs a privacy-proxy service and a registrar and make sure that we're not just acting as a surrogate, but are expressing concerns that we believe are widely held. That's not a fair thing to say about what he has written, but I think we need to be cognizant of it. Yes, Carlton?

CARLTON SAMUELS: One thing that came out of DNS abuse study. Recognizing, when going back to your statement, Alan, about losing money if you disallow the registrations. The first recommendation was that maybe we should put in the registration agreements incentives for the registries themselves to act against abuse, anti-abuse. Then, it includes monetary incentives.

The idea is that registration provides revenue and maybe it is the revenue situation that's top of mind that is causing the registration to be lax in enforcing anti-abuse.

So, maybe in the registration agreements, if you incentivize registries to put in anti-abuse measures, then they might act proactively to detain or reduce the amount of bad actors that we want to register domain names.

ALAN GREENBERG: I support that concept. I'm not sure it's our business as the WHOIS Review Team.

CARLTON SAMUELS: Can I tell you that there's a lot of argument around that because we feel that is – some people believe we have a lot of support for that one. Let's leave it that way.

ALAN GREENBERG: Noted. Further comments? Chris looks like he has a comment he wants to make. I think Carlton is saying a lot of people would applaud if we put such a recommendation in even if it's not our business. I'm not sure we could worry about people's applause at that stage. We'd need a pretty tight tie-in for WHOIS for us to make that recommendation and maintain our credibility. We have 25 minutes. If we finished this, do we want to break for a long lunch even if lunch isn't ready yet or do we want to go on to the next topic? The next topic is update on ongoing community initiatives. That sounds like one we could start talking about

if we wanted to. By community initiatives, I presume we are talking about things like ongoing PDPs that have been halted and other stuff like that. Was that the intent? Sorry, Lisa, go ahead.

LISA PHIFER: I was just catching up on my notes from the previous topic, if we could advance the slides.

To kick off this discussion, we developed a list of – actually, what we did is we went back to the terms of reference. You might recall that in the terms of reference there were a list of other activities going on within ICANN that might have some impact on this review. As part of the terms of reference, ICANN Organization was asked to provide periodic updates on these activities.

So, in going back to that list, what this table actually does is identify for you two things. One is the subgroup that actually received an update on the specific activity as part of your implementation report or briefings, so that's the middle column saying covered in the subgroup briefing. For example, there was material on the next generation RDS PDP in the material that was provided to the subgroup working on recommendation 1 as well as the subgroup working on anything new, which I guess we'll do this afternoon.

Then, in the right-most column, what you have is links to the place where you would find ongoing updates related to that activity. So, not just what was written in the implementation briefing that was provided, but also where to look if you want to see the latest on a particular topic.

For example, RDAP implementation. There was information on RDAP provided as part of briefing materials for your subgroup, Dmitry. But, also, if you want to see the latest on the RDAP pilot, which is ongoing now, the link is provided for you to do that.

You can see the list of activities that were identified in the terms of reference. Many of these we've actually touched on as part of our discussion already. Some that we haven't will fall into anything new, which we'll talk about later today, such as the procedure for handling conflicts with privacy laws. I guess we'll touch very briefly on thick WHOIS, but that's part of that same list of policies that were developed since the original WHOIS review that's completed.

Of course, the last item on the list and the one you probably want to have some discussion on is all the activities related to GDPR compliance.

ALAN GREENBERG: Does anyone want to ask any questions, make any comments? I'll wade into a dangerous area. Is Lisa in a position to give us any indication of what's likely to happen with the GNSO PDP? Or maybe Chris.

CHRIS DISSPAIN: Which one?

ALAN GREENBERG: The PDP on next generation RDS. Would you like to go off the record?

UNIDENTIFIED FEMALE: I can share a little bit there. Anyone who's been following that PDP a all knows that three or four weeks ago the working group calls were suspended indefinitely following the Puerto Rico meeting and that was done for a couple of reasons, one of which is that basically the community is very distracted by GDPR and the people that need to be focusing on GDPR right now cannot be focusing on next generation RDS.

But, also, it wasn't clear what role the PDP would have in the next steps for GDPR compliance. So, rather than continuing to deliberate on the long-term future RDS, we thought it would be we, the leadership team of that PDP, thought it would be appropriate to take a temporary break, let those working on GDPR do what they needed to do and try to sort out that question of what is the role that this PDP might play.

There was a communication to the GNSO Council last Friday, so just a few days ago, regarding ongoing interaction that the GNSO Council has had with the PDP leadership about what are the different ways that one might pursue policy development on a temporary policy that might emerge from the compliance activity.

The leadership of the PDP had put together basically a series of three options. One would be repurposing the existing PDP to look at something related to temporary policy. Another would be to temporarily suspend or terminate the existing PDP and start a new PDP focused specifically on the temporary policy. Then, a third would be to use the process that was developed for an expedited PDP. Again, that would be a new expedited PDP, but a new policy development effort related to temporary policy. Yes?

ALAN GREENBERG: You've used the expression temporary policy. The only temporary policy I'm aware of is the contractual ability … Of the board's ability under contracts with contracted parties to set an interim policy if the stability of the DNS is endangered on the three-month basis renewable three times. Conceivably, on day 367 or 6 they could reenact accidentally the same policy again and get a second year, although I don't know how that would be viewed.

That's described as policy the board can enact, and then in parallel, instruct the GNSO to do something permanent. Are you suggesting that it is conceivable the board might ask the GNSO to propose that temporary policy which they could then enact? Otherwise, I'm not sure what the phrase temporary policy means.

UNIDENTIFIED FEMALE: Actually, you laid out exactly the temporary policy that has been being discussed. The question was a hypothetical one. If the board should choose that contractual measure to put a proposed interim model in place, then that would become a temporary policy of three-month periods, renewable four times.

ALAN GREENBERG: Three times.

UNIDENTIFIED FEMALE: Thank you. Instituted once, renewed three times. So, the question that the PDP leadership looked at was if that happens and that contractual clause requires policy development process to be initiated immediately, what process would you initiate? Would you initiate a new PDP? Would you initiate an expedited PDP or would you try to reuse the vehicle that's already in place?

ALAN GREENBERG: So, that's not to build the temporary policy, but to replace the temporary policy.

CHRIS DISSPAIN: Would you like me to tell you what the board's position is? Would that be helpful? Good. So, the board had – a small group of board members, which was comprised of GNSO board folks Becky, Matthew, and then Avri and Sarah who are also obviously connected in some ways to the GNSO, and Cherine and myself, had a call with the GNSO leadership and the RDS PDP Working Group leadership. That call was recorded and has been published. It's available to listen to.

That call was basically, as a result of the board reaching out to the GNSO saying, "Look, we would like to talk to you about what next steps are necessary and how to deal with it."

We discussed at some length with them that one of the distinct possibilities of the board …. So, I should say this call took place before the letter from the DPA arrived, so that had made a little difference but I'll get back to that in a second.

On that call, we discussed the possibility of the board instituting a temporary policy before the 25th of May which would possibly be … Well, it would be a temporary policy that said in order to maintain compliance with GDPR and WHOIS [inaudible] follow the GAC's advice, here is the temporary policy.

We discussed with the GNSO the fact that the bylaw mandates … That, in effect, automatically after the institution of that temporary policy specification, the GNSO or the board must then ask the GNSO to launch a policy development process. We discussed whether we could find a way of making sure that that policy development process used the expedited policy development process mechanism because it's useful [inaudible] policy development process would never get done in twelve months.

We discussed that we couldn't say for sure that's what we were going to do, but that whether we were leaning towards doing that, and that whilst we weren't asking the GNSO to do anything, given that we were starting to think about, it might be a good idea if they started to think about it. That then led to Heather writing to the Council setting out the fact that they had done the call and it was time to start thinking about it.

We also talked about whether there are some concern that the way that the way that the bylaws are drafted implies that a temporary specification – sorry, that a PDP expedited or otherwise following a temporary specification or temporary policy specification from the board, it could only be a straight up and down, yes or no. Is this in fact … Can this become consensus policy or not? We all agree that we thought

that was a nonsensical reading of the bylaw, and even if that's used the way that it's read, it's ridiculous and needs to be immediately ignored because you can't possibly have a situation where the GNSO isn't capable of amending the temporary specification [inaudible] reach consensus. It just doesn't make any sense.

So, we did all of that and that's all public. We then got the letter from the Article 29 folks which means that … It doesn't change the fact that it may well be that we end up with a temporary specification and my understanding is that if we do end up with a temporary specification there is a reasonable likelihood that the GNSO will be prepared to consider an expedited PDP to deal with that.

Does that answer your question in enough detail? Okay. And I think Heather's letter is also public and everything has been published, so it should all be available for people to look at.

ALAN GREENBERG: Thank you.

CHRIS DISSPAIN: I'm sorry, and needless to say, although the board hasn't made a decision yet on whether it would use the temporary policy mechanism, the board is aware of the fact that there are certain things that it needs to believe to be the case in order to use that mechanism and I think it would be fair to say that we think that this circumstance probably does fit fairly and squarely inside the reasons why it would be okay for us to do it.

ALAN GREENBERG: Stephanie?

STEPHANIE PERRIN: Thanks for that explanation. I'm fascinated by a potential policy that would manage to square the GAC advice with the Article 29 letter. Any thoughts on that?

CHRIS DISSPAIN: Well, no, those two things are totally unconnected. Any move that involves the institution of a temporary policy specification will require … Sorry, unless that temporary policy specification actually accepts all of the GAC's advice or rather is drafted in a way that shows that all of the GAC's advice is accepted, then it's obvious that some of the GAC's advice will need to be rejected.

Now, there are mechanisms in place for dealing with that. There is no time limit – sorry, there is no timeframe in which those things can be done. That said, it is also my understanding that it may be that the GAC may in fact reconsider its advice. I don't know if that's correct or not, but they may reconsider their advice.

But, irrespective, if the GAC advice is still in existence, then it would be necessary for the board to reject that advice in order to … It might be necessary, I should say, for the board to reject that advice in order to issue a temporary specification. Or not. If the temporary specification doesn't do anything that is outside of the advice.

The only specific point – and this is way too down in the weeds to the discussion here, really. But, the only specific matter that is at odds between the two pieces of advice is actually the masking of the registrant e-mail address. Nothing else is immediately obviously at odds.

Sorry. And just to be clear, the GAC's advice on the registrant e-mail address is not that it should be open. The GAC's advice on the registrant e-mail address is reconsider masking the address. So, it does not prevent us from masking the address without rejecting their advice and the other pieces of their advice are in respect to matters that are at odds with our current model, not necessarily at odds with what the DPA folks have said.

So, for example, it's at odds with our parent model of applying these rules across all WHOIS records rather than just personal ones and it's at odds with the possible interpretation that you should only do it in respect to your [inaudible] records.

ALAN GREENBERG: I would've thought it is at odds with or at odds with future GAC advice not yet given because I didn't think it was necessary.

CHRIS DISSPAIN: If you can see into the future …

ALAN GREENBERG: I love seeing into the future. Related to the Article 29 letter advice that says ignore … Stick to your own business and ignore thigs like law

enforcement and cyber issues where I believe they simply don't understand what our business is.

CHRIS DISSPAIN: Again, we could bounce this ball around forever, but I agree with you. I think it's a different point. If you parse this down to try and deal with the issues at hand, there's a deadline. There's a model. There's comment on that model and there's GAC advice. The comment on the model and the GAC advice are, in some respects, at odds with each other. Those two things need to be sorted out. One way of sorting that out is to reject the GAC's advice where it is at odds. I don't actually think it will be necessary based on the fact that the advice is to reconsider, not to actually do.

But, the question then becomes is the temporary specification the right way forward? If it is the right way forward, and I think it's probably the only way forward actually, then we need to do that.

But, I don't think that the GAC advice … Sorry, let me just finish by saying in order for us to accept the GAC's advice, we need to change our model. It's got nothing to do with the DPA's input. Our model is not currently at [inaudible] with the GAC's advice because our model is universal worldwide rather than the GAC's advice being stuck to the jurisdiction, that is a problem.

So, that's where we're headed.

STEPHANIE PERRIN: Chris, just one more question. The GNSO has a meeting imminently and it's about to get moving again on the wretched WHOIS conflicts with law procedure. Yes.

CHRIS DISSPAIN: Sorry. Which one is that? I don't know that.

STEPHANIE PERRIN: Yeah, the [IAG]. Has the board considered the possibility that registrars will invoke the procedure in order to get waivers because they don't believe that the interim position sufficiently protects them from prosecution under the data protection laws?

CHRIS DISSPAIN: No because it, as an interim policy, there's a policy and there are no waivers. The whole point about having an interim policy is that it is compliable. It needs to be complied with, and so therefore, once that policy is in place, it becomes a compliance issue and there would be no waivers.

STEPHANIE PERRIN: So, that, in fact, gets rid of the former waiver policy.

CHRIS DISSPAIN: There is no waiver policy. There isn't an agreement, or is a statement rather from compliance that in certain circumstances certain things will happen. Well, that's not a policy. It's [inaudible].

STEPHANIE PERRIN: Well, we have pointed to that in our correspondence with the Article 29 group for many, many years.

CHRIS DISSPAIN: Not as a policy. It's not an ICANN policy. It hasn't gone through a policy development process through the GNSO, so it's not a policy.

STEPHANIE PERRIN: That's an interesting approach to take. I will dig out my dissertation and get you chapter and verse on when we said it was.

ALAN GREENBERG: It may be an ICANN policy with regard to their practices, but not [inaudible].

CHRIS DISSPAIN: Maybe I'm being [inaudible], but it's not a policy with a capital P. It was something that we put in place in respect to contractual obligations, but nothing whatsoever to do with GNSO policy.

ALAN GREENBERG: It is way outside of the picket things among other things, depending on what the waiver is for. It may be inside the picket fence if it's WHOIS, outside if it's something else.

STEPHANIE PERRIN: But it was, nevertheless, the output of the 2006 WHOIS task forces. There was agreement that ICANN would have a procedure and it went through the GNSO. It did not go through what I would call a policy development process. That's for sure. And staff developed the procedure.

But, it has been what we have pointed to and Fadi wrote to the Article 29 guys and pointed to it as our WHOIS policy saying, "Here's what we've got." Was it working is another matter, but …

ALAN GREENBERG: We're quibbling over whether it is a capital P probably in the sense of gTLD policy.

CHRIS DISSPAIN: I'm not clear what the point is. I don't know why that matters. I don't understand why that matters.

STEPHANIE PERRIN: Well, I think it matters if you are saying that the interim policy that the board is talking about imposing then wipes out any earlier materials, then why is the GNSO resurrecting the IAG for a procedure that is now irrelevant? Before I sign up and spend more quality time on that wretched procedure, I'd like to know.

CHRIS DISSPAIN: Well, two things. One, I haven't said that that's the case. I've said we haven't thought about it and I don't know. And secondly, what the GNSO does is a matter for the GNSO. If the GNSO wants to look at the IAG procedure, then that's a matter for them.

What I'm saying to you is my understanding – and I stress I'm talking about my understanding right now – is the intention would be that there would be, if we do it, that there would be an interim policy and that policy is binding.

Now, can registrars take us to court and say we don't believe that this makes us compliant with GDPR, therefore we're not going to abide by the policy? Of course they can. There's nothing to stop them from doing that right now.

ALAN GREENBERG: Miraculously, it's only two minutes until lunch. Any more comments? We will reconvene in one hour. Can we stop the recording please?

Unless there's any objection, we're going to start the afternoon session with consumer trust, when we start.

ERIKA MANN: Don't ask in German when to start, I will say now.

ALAN GREENBERG: I said when we start, we will start with consumer trust, but we haven't started. At the time when we start, we will initiate the discussion with consumer trust. It's not on the record yet.

Welcome to the afternoon session on the second day of the face-to-face meeting of the RDS WHOIS Review Team in Brussels. It is the 17th of April. We are rearranging the schedule slightly and we'll take the item on consumer trust first on the agenda and then we'll spend the rest of the afternoon talking about WHOIS.

Erika, please.

ERIKA MANN: Thank you, Alan. So, this group, the subgroup members are Carlton, Dmitry, Stephanie, Susan, and myself. Let me guide you quickly through the slides and then I hope we can have a discussion about it.

The objective of this particular subgroup was consistent with ICANN's mission and bylaws section 4.6e, blah, blah, blah. The Review Team will assess the extent to which the implementation of [inaudible] WHOIS promotes consumer trust in gTLD domain names by a) agreeing upon a working definition of consumer and consumer trust used in this review b) identifying the approach used to determine the extent to which consumer trust needs are met and c) identifying high-priority gaps, if any, in meeting those needs and d) recommending specific measure steps if any the team believes are important to fill the gaps.

Before I start with the guiding you through the questions, it's really a hard issue to identify the topic about consumer trust and consumer –

anything related to consumer in the WHOIS environment. We will show you a little bit later one review which we – and this was actually the original review which we found where the topic is really explicitly mentioned and it's targeted in the [inaudible], but otherwise it's very, very hard to find the items and the topics covered.

So, the questions we were looking into are the following. Is the term trustworthiness the best and only option in determining consumer trust in the gTLD environment as mentioned in the relevant WHOIS report? That's practically what the original review team came to – they took out the word trustworthiness. That's a key indicator to identify if consumer needs and consumer trust is actually in existence.

Second is to increase an alternative identity. For example, Facebook [inaudible] indication that the current use of gTLD is not sufficiently advocating consumer trust. Now, this is already a high assumption question because it's not something which relates automatically to WHOIS, but we wanted to see it captured because it might be actually an indication that other firms or, let's say, other services may be closer to what consumers at least expect.

Three, a key high priority gap in understanding the consumer trust environment is apparently the lack of sufficient data as mentioned in the various WHOIS reports. Are there new developments that need to be considered for as the decline in awareness for some of the legacy gTLDs – for example, dot-info or dot-org – an indication for changing patterns in consumer trust?

Five, security and transparency play a major role in defining a trustful Internet environment. Did the current gTLD and WHOIS system achieve this?

Six, are regulations like we should say for example the European GDPR increasing consumer trust as major information is missing in the publicly available WHOIS?

So, you see here on the next page, if you can move to it – yeah, please, anytime.

CATHRIN BAUER-BULST: I just had one question on the second question to clarify what exactly you mean. Are people using Facebook as a platform to access information or vendors that otherwise they could access through the domain name system itself? What exactly do you mean by that?

ERIKA MANN: It's just a hypothetical question which we came up with. The question is: is the indication that we have a decrease in domains in principle, in particular even gTLD was not meeting the expectation at least what was expected originally. The question is: is this an indication that consumer trust, as a pattern, is shifting? So, it's a little bit related also. That's why I said it's a little bit relating outside of the WHOIS environment, but it's still a relevant one because if it is shifting, then at least you have to be careful in the end in judging. If you want to answer the last question six, if it relates to … Because you will not be able in the future to see WHOIS data anymore maybe. Maybe there's another pattern behind at the

same time, which is that consumers in general are shifting away from the domain environment.

So, it's just an awareness-raising question, not really one maybe we want to keep at the very end if we can't find a good answer to it, to be frank, in the review.

SUSAN KAWAGUCHI: I'm becoming Carlton today. Well, they don't register a domain and launch a site. They start a Facebook page. And sometimes that evolves, but it's not necessarily an actual step. A lot of times, they just do all of their business on a Facebook page or I'm sure there's other platforms they could do the same thing on.

Are they doing that because it's less cost or are they doing that because they think it's more trustworthy and can be found easier than just an individual website?

One more point. I didn't do any of this work. Erika did this work.

ERIKA MANN: But, I think that's true for all of us, for all of groups I mean. How much can we … But, I mean we still use each other as a bumping. We bump back and forth what questions. Insofar, yes, I think we still do all participate.

So, here you see on the next page, which is page three, the main background material. There's a lot of more background material. I

[screened] practically all documents available which relate somewhat to WHOIS, and even indirectly to WHOIS.

So, these are only the main ones I wanted to draw your attention to. One is the review team, the first report, which actually is quite good in relation to consumer and the appending stuff which relates to a consumer study. That's the core which we have available. There's little done afterwards. Practically, let's be frank, nothing. The word pops up sometimes in different environments, but it's never verified. There's no understanding at all what consumer trust actually means or what public interest in relation to consumer trust means or whatever. Whenever the topic comes up, it's a [vague shell] and it is not defined, with the exception of the first WHOIS Review Team, which did when you look back when it was done in 2012 actually a pretty good job.

I do have included the competition consumer trust consumer choice review team draft report, because again, it relates and it gives some flavor about the understanding of consumer choice and consumer trust, not related to WHOIS. So, keep this in mind.

ALAN GREENBERG: It strikes me as we're talking and trying to define consumer trust that it's again one of these negative things. If someone approaches the Internet as a novice, unless they have bad experiences, their inclination is to trust things. The mistrust has to be built. If you start using e-mail and start getting a huge amount of spam, you lose trust in the e-mail system. If you mistype a domain name and you get a pornographic site, you start mistrusting it. In the absence of those negative things

happening, you almost implicitly have trust until something happens to cause it to go away.

One of the things I think we're going to have to be looking at as we do this is are there aspects of WHOIS which cause trust not to disappear, even though the user is not conscious of the mechanism through which it works?

ERIKA MANN: Alan, that's actually a very, very good point. We will take this up and review the work, taking your point into consideration. I think it's right.

Now, in the regulatory environment, of course consumer trust relates typically or it has a quite solid understanding. So, in the regulatory environment for consumer regulations. But, it always relates, then, typically to a product definition or whatever companies must do to ensure that companies, as you say, either are not losing trust or how far the company is liable or responsible if damage is [inaudible]. So, you have a quite narrow understanding. It's a good point. Yeah.

ALAN GREENBERG: To put it in another world, and going back a few decades, when people started driving cars, they didn't inherently say, "I wonder if the gas tank is going to explode if someone hits me." But, when gas tanks started exploding when people hit them, it becomes a relevant factor. I think that's the same sort of thing we're talking about here.

ERIKA MANN: Then we included the global registrant survey, again, because it's relevant for the topic and the topic sometimes shows up but it's not automatically a strong connection to WHOIS. We included the ICANN bylaws, although again, consumer trust is not mentioned in the bylaw. But, Lisa, maybe you're so kind and you check the strongest connection we found in the bylaw. Do you remember? We found when we [inaudible]. Maybe we can at the end just read it just to give an indication what we are thinking, why we believe it should be included.

What we like to do is, because that's maybe the only real task which we have for the global domain division is to provide us with answers and indicate about how consumer trust is reflected in their approach to WHOIS policy implementation and enforcement. That's a very general question, but we want to keep it so general because we want [inaudible] to reflect upon the question themselves and come up with different answers, because I don't think they have done this so far.

So, then, describe your methodology to answers questions and analyze the materials. We agreed to a working definition of consumer to include any Internet user of which was registrants were a small subset.

We agreed to examine the term trustworthiness by determining the extent to which consumer trust needs are met.

The last one is maybe the most relevant one. We plan to do a gap analysis by examining the finding and analysis of other subgroup assessing implementation of the WHOIS recommendations.

So, what we wanted to do, because there's so little we can find in our own environment, we thought we would see what you have identified

and then we want to do a gap analysis and we want to see how does this relate either if there's something missing in connection to consumer trust or if there's something you identified, not in relation to consumer trust, but in relation to the topic you are covering. We then believe there's a connection to consumer trust.

Let's assume accuracy of data, for example. We discussed this already. There is a clear indication or there can be a clear indication if data is really seriously not accurate and there can be a connection to consumer trust. But, we want to do this based on your findings. Yes, please?

CATHRIN BAUER-BULST: I just had a question on the definition of consumer because just from the legal context that I have been working in, a consumer is normally an individual acting outside of their professional capacity. I was just wondering whether that is something you had also considered or whether it's just any Internet user.

ERIKA MANN: [inaudible] any Internet user. Any Internet user who is using because we are talking about also domain name.

CATHRIN BAUER-BULST: So, including any professional, a lawyer, company, anyone using the Internet.

ERIKA MANN: Not if it's a company. Go ahead, Alan.

ALAN GREENBERG: In this context, I treat consumers of Internet services and that covers everyone. It covers the corporate user and the other ones, although clearly our focus in terms of consumer of trust … At a corporate level, you put your trust in things in a different way, so I think we're looking mainly at from an individual perspective. An individual probably non-technical perspective is our main focus, but I think I would include everyone as potential consumers because they're consumers of the Internet resources, not of buying things over the Internet. That's how I take it, anyway.

ERIKA MANN: [inaudible].

CATHRIN BAUER-BULST: Thank you. I think that actually might make the work of it more difficult because then Susan would be a consumer for the purposes of the WHOIS and [inaudible] has a completely different understanding and sophistication in terms of the uses she can make of it. Then, your average Joe Smith on the streets who is not aware. I thought the main issue with this is also that the consumers might not even be very aware of the WHOIS and the question is, of course, how much of a role this plays in consumer confidence.

ERIKA MANN: I mean, that's a philosophical question. I think it's a good one, but I would agree with Alan. We should really call an individual user – it doesn't matter if it's a company, as long as a person behind. If it's just a company, info.fb.com, it's not an individual user. Now, there might be in the tech office somebody sitting and looking at it, but there's no indication that it's an individual user. But, if it is susank@fb.com, yes, it's an individual user. I would say so.

SUSAN KAWAGUCHI: [inaudible] using e-mail address [inaudible] how would you characterize a domain at fb.com.

ERIKA MANN: Exactly. I would say it probably falls outside of the definition of an individual user.

SUSAN KAWAGUCHI: It was me sitting there using domain at fb responding for managing the domain names and then …

ERIKA MANN: How about we distinguished it to [inaudible]? Alan, please.

ALAN GREENBERG: Look, we have four billion roughly Internet users of which maybe some hundred million of them are technically savvy enough to be able to do a WHOIS query, whether it's someone who's doing it professionally or

someone like me who's done it not professionally, but for enough years of my life in various forms that I know what I'm talking about.

So, there's a small percentage of us who are technically savvy and knowledgeable of what WHOIS. The vast majority of the consumers of Internet services have no clue. And I think we're looking at the whole spectrum from one to the other. Clearly, there's a lot more of one than the other. The question I think that we need to look at here is: is there an issue of consumer trust? Does WHOIS factor in at all? Clearly, it factors in for the people who know how to do a WHOIS query. To what extent is it relevant for the rest of them?

DMITRY BELYAVSKY: It seems to me that of course we potentially have an Internet user as a consumer, but according to consumer study, common users [inaudible] use WHOIS for their purposes. But, there are some groups more or less professional users who can be [inaudible] according to their request and their [competition]. Thank you.

ERIKA MANN: Yeah. I think what I will recommend and maybe discuss it in the group, what we can do, maybe we can identify and clarify the consumer trust environment a bit closer, so we can talk about individual users. We can talk about the professional. We can talk about cases like Susan is highlighting, which I think it's an important one, because even behind each company name, there's still persons behind. [inaudible] can be much more clearer and we might even be able to capture Cathrin's concern that there are still many users or Internet users, if I understood

you right, which are not part of actually the WHOIS or ICANN ecosystem. So, they're potential users. Right now, they're not users of domain names. We can do this because they still might be affected by it.

CATHRIN BAUER-BULST: Just to clarify, my concern is not to get all of those who never used the WHOIS because clearly the relevance to them will be limited, but just that there's a legal meaning that's been given to the term, at least in the EU context and I'm just interested if the bylaws were thinking of the consumer in sort of the legal sense, and it would be interesting to see also how the CCT Review Team defines this, so that we're sort of aligned. If they had any … If they gave any thought to what consumer trust means.

SUSAN KAWAGUCHI: Carlton could answer this, too, but I did go through and read the … Look for consumer and trust, those two terms, in the CCT report looking for definition and just did not come up with one.

The other point I wanted to make, too, was the WHOIS is used from a technical point of view to establish those reputations and therefore protect consumers on a website. Facebook is a massive user of WHOIS information for that. So, by extension, that's promoting consumer trust in the Facebook platform, for example, or any domain or website could do that.

ALAN GREENBERG: Excuse me, Susan. Alice, did you have something?

ALICE JANSEN: Yes. Actually, the CCT defined consumer trust in its terms of reference.

SUSAN KAWAGUCHI: Oh, I missed that.

ALICE JANSEN: Yeah. Do you want me to send that to you or should I read it now?

ERIKA MANN: Would you send it to me as well?

ALICE JANSEN: Yes, of course.

ALAN GREENBERG: If you could just read it right now.

ALICE JANSEN: Of course, yes. The confidence consumers have in the function, reliability, safety, security, and necessity of the domain name system. This includes trust in the consistency of name resolution, confidence by Internet users that they can safely navigate to a domain name to find and safely use the site they intend to reach. Confidence that a TLD registry operator is fulfilling the registry stated purpose and confidence by a registrant in a domain's registration process and lifecycle.

ALAN GREENBERG: Now, that defined confidence. It didn't define consumer.

CARLTON SAMUELS: Yes, you're right. It's about confidence, but we tend to talk about trustworthiness more than trust.

ALAN GREENBERG: For the reasons that Susan started going into, I think our conclusions are inevitably going to indicate that WHOIS has a significant impact on all classes of consumers, both the unknowledgeable individuals and the knowledgeable ones. So, I really don't think we can afford to use anything other than a very wide definition and that may well be different from how consumers are trusted, where the terms are – consumers are normally consumers of something, and in this case, it's consumers of Internet bits. So, by definition, anyone who touches a keyboard or a smartphone or whatever is implicitly a consumer of those resources. Just like a consumer of telephone resources is someone who has a telephone. I think the analogy is consistent there.

ERIKA MANN: Okay. The rest is pretty much on page four what we debated, but I will run through it quickly. What we recommend based on the analysis and where we found actually the main relevant document, I just mention them quickly again.

So, after reviewing available documents to [inaudible] finds that the only document which specifically explores the relationship between WHOIS and consumer trust is the WHOIS1 final report. The topic of consumer trust is mentioned in various documents. Sometimes its only referenced and like what we heard just a few minutes ago, not even in the center of attention [inaudible] have been provided for subgroup analysis and other documented identified as significant in judging the relevance of consumer trust and the board [or context] of ICANN's consumer and public interest value system.

Phase two is the global consumer research survey and ICANN bylaws. We have to separate it a little bit from the … Because the topic of consumer trust comes up only indirectly and it's not explicitly mentioned.

So, based on the findings, the subgroup identified the following problems and issues. Gap analysis to identify areas of WHOIS which may need to be further enhanced to promote consumer trust and gap analysis to be repeated after WHOIS [inaudible] to comply with GDPR. Now, that's a placeholder because that's of course time-sensitive and time-critical. If there is no real implication from GDPR to WHOIS or it is only impacting a certain group of consumers, only European consumers, then the gap analysis of course will look different than in case let's say WHOIS goes dark totally. So, we would come to different conclusions depending on the outcome of the implementation of the GDPR into the WHOIS environment. And so far we haven't identified any recommendations yet. Back to you. I don't see anybody raising their hand.

ALAN GREENBERG: Let's talk a little bit about what are we trying to do here. Let me go back to the original question.

ERIKA MANN: Shall I read it again?

ALAN GREENBERG: No, no. Okay. The crux of the matter is the review team will assess the extent to which the implementation of today's WHOIS promotes consumer trust in gTLD names. I think the answer is based on the use of WHOIS by the knowledgeable expert and the use of WHOIS by those who create reputation lists and spam filters and things like that is such that we can say without much doubt that WHOIS does, is a component of generating trust in the domain name system.

To some extent, although we clarified it with an A, B, C, D of what we're going to be doing, that answers the basic question. So, the rest of it now is we have to flesh it out with what we committed to do or decide we don't really need to do that because it's not relevant now that we've done more analysis.

Clearly, your statement at the end, GDPR may impact this. Until we know what it means and then actually watch the fall out, we can predict that the whole world will fall apart because reputation services and spam filters will all stop working and we'll be flooded with bad websites and spam and we'll all just give up and go back to a piece of stone and a chisel. Or, it may not be bad at all.

I think our overall task is a relatively simple one and I don't know if we want to overcomplicate it just to make it look more important.

ERIKA MANN: No, of course not. We want to keep it simple and straightforward, but we might find something excessing the reports coming from others. We might identify something which is relevant for this topic outside of the points you just mentioned. That's all what we want to do and we don't want to complicate anything.

ALAN GREENBERG: I wasn't trying to stop conversation. I'm just saying we have to go back and keep a focus on what was the original item in the AOC and in the bylaws that we're trying to focus on.

ERIKA MANN: Key issues, yes. Correct. Totally agree. Lisa, have you found a bylaw point, the one which we had in mind when we, why we added the bylaws? Dmitry, please?

DMITRY BELYAVSKY: I'm speaking about the definition sent by [inaudible] from CCT. Well, that definition is formally absolutely correct, but the point [inaudible] from various branches, and for some cases, people almost never or very rare use WHOIS to ensure they receive what they want. Their trust in the [inaudible] name resolution seems to be very slightly related to WHOIS. [inaudible] that domain name is [inaudible]. Well, people

usually go to [inaudible] to the site and never verify the owner of site via WHOIS. [inaudible] they are common people, not professional users.

The subpoint is, well, that the registry operator is fulfilling the registry stated purpose. I hardly can understand this point at all. Sorry.

We have the fourth point, which is mostly directly related to our group, confidence by registrant in the domain registration process and lifecycle. It seems there's only one point of [inaudible] which have [inaudible] of significance for our study. Thank you.

CARLTON SAMUELS: The review team, in looking at the definition for consumer trust, we figured we were talking really about trustworthiness and the reason that came up is because, as you look at – we talk about the average user, registrant going to a website and not even looking who owns it or anything else. That's true. But, there's a secondary requirement for reputation companies that sometimes you yourself does not make the determination about the trustworthiness but it's the secondary. Somebody makes a determination and then sells that to you.

The people who do that, they use the WHOIS as a baseline to create a profile of the website. So, that's the domain name. That's how that comes into play. It is the sense we recognize that trustworthiness is a manufactured kind of attribute and it comes from the reputation companies actually creating the profile of the property, the web property, and then transferring that to the ordinary user. That's the context in which we use trustworthiness.

DMITRY BELYAVSKY: Carlton, sorry, I have an objection, because in the scenario described, we have two patterns, which is [inaudible] you were speaking about [inaudible] professionals create reputations maybe based on WHOIS among other sources, of course. The other people don't trust the WHOIS, but trust the reputation of the market professionals. Well, trust [inaudible] professionals seems to be out of scope, no? Okay.

ALAN GREENBERG: I disagree completely. If WHOIS is a component that is used by, as an example, reputation services or spam filters, then WHOIS contributes to the confidence that users have in the Internet and in the domain name system. If you type in a misspelling of Facebook and whoever today is in charge of Facebook things catches it, they will try to take action to take it down. But, if they don't catch it, there's a good chance that if that site is doing the phishing or something like that, there's a good chance that if it's not taken down, the reputation services will tell your browser to say, "Warning, this is a potentially dangerous site."

The fact that you don't get to a bad site but you get a warning about, and if the services doing that work use WHOIS as one of their tools, then WHOIS contributes to consumer confidence. It's indirectly. The user doesn't know anything about WHOIS. Go ahead.

DMITRY BELYAVSKY: I understand your position. Okay. If the [inaudible] providing input, but as it is being invisible to end user – in effect, invisible to end users, should we treat it as a consumer experience regarding WHOIS?

ALAN GREENBERG: it's not part of the consumer experience, but it contributes to the consumer confidence in the domain name system without them understanding it at all. Just like if you fly on an airplane and you have confidence the plane won't fall out of the sky, there's an awful lot of people in professions that are contributing to making sure that plane doesn't fall out of the sky. You're completely oblivious to all of them, but the fact that they're doing their job properly means the plane doesn't fall out of the sky. Some of us have some idea of why planes do fall out of the sky and we worry a little bit. It happens to be one of my interests.

ERIKA MANN: [inaudible].

ALAN GREENBERG: Understanding why planes fall out of the sky. It's a really interesting issue. Susan, pixie dust. But, if they run out of pixie dust, you're in trouble.

LISA PHIFER: Erika, you asked me to look at the bylaws. On the phone, you and I had sort of scoured the bylaws and the bylaws of course injected this

particular objective that you're trying to address, and although we couldn't find a specific call out to consumer trust, we found quite a number of references to the public interest and to – for example, individuals being part of the community.

For example, in the bylaws core values section, there is a point that talks about while remining rooted in the private sector including businesses, stakeholders, civil society, the technical community, academia, and end users, and then recognizing that governments and public authorities responsible for policy take into account public policy [inaudible] of governments and public authorities that there's a point five that operating efficiency and excellency in a [inaudible] responsible manner where practical and not inconsistent with ICANN's other obligations, but [inaudible] that is responsive to the needs of the global Internet community.

So, you can see just by those two examples that the Internet community or end users is not the central point of those core values, but they are referenced as part of the core values.

ERIKA MANN: I have taken note of most of the points mentioned today and I will add them into the review of the document which we have done on this topic, consumer trust, and then we will see if this will in the future capture the points you have raised today. Go ahead.

CHRIS DISSPAIN: Me?

ERIKA MANN: Yes, you.

CHRIS DISSPAIN: Thank you very much. So, the last point there, number six – thank you for numbering, by the way, Erika. Are regulations like the GDPR European [inaudible] increasing consumer trust if major information is missing in the publicly available WHOIS? I can't remember what the timings are for this review and I can't remember whether there will be much of an opportunity post after a reasonable time post GDPR assuming that GDPR leads to a significant reduction in the amount of data that's published to deal sensibly with that question.

But, I just wanted to suggest that one thing this review team could do is make recommendations of things that should be done in a post-GDPR world to assess the affect.

So, this review team could, for example, recommend that in a year's time or 18 months' time or whatever is appropriate a full review should be done – I'm just making this up as I go – along with consumer trust, given the reduction in the available data and so on. I'm just suggesting that that's something to think about. Thank you.

ERIKA MANN: Thank you, Chris. It's actually a very good point. I wouldn't have thought about this. You can make … In case the timing is not working and making precise recommendations, you can make recommendation when it needs exactly to be reviewed. Yeah. Thank you so much. Any

other points? No? Okay, Alan, back to you. You can start another session earlier.

ALAN GREENBERG: Or I can cancel the meeting for the rest of the afternoon. It seems like a delightful day outside. We won't cancel quite yet. The next part of the agenda for the rest of the afternoon, actually, is described as WHOIS1 implementation assessment, establish findings, determine need for recommendations if any, discuss nature of the resulting recommendations if any.

Essentially, this is what we started off in the morning where we were supposed to have a very brief summary of what we've done and instead started on the substantive discussion. So, what I would suggest is we go back to that at this point and start looking at the recommendations – not at the recommendations, at the subgroups that we have looked at so far and see if we can come to a little bit more closure on what work needs to be done and what is our outcomes are to date.

This partly goes along with an item that is elsewhere somewhere on the agenda – I'm guessing tomorrow – of what I described as a critical assessment of each of the subgroups and the work … It's now? Oh. We changed the name of it. This is what it is. Alright. Essentially, we need to take stock of where we are so we understand within each subgroup what we have to do going forward, identify whether there are any problem areas either because we still need input or we don't think we have the right resources to follow through on it or rethink our overall

direction was misguided or whatever. So, essentially, coming out, do we feel comfortable going forward and know how we're going to do it?

With that, I don't know, perhaps it's easiest to go back over the original slides for the recommendations we looked at. I'm not sure. I don't think we have anything here.

ALICE JANSEN: We've actually abstracted the recommendations from the presentations yesterday and we have them here, so that's helpful.

ALAN GREENBERG: Then, thank you for being prepared where I wasn't. Let's do them section by section, then. Alright. Recommendation 2, WHOIS policy. We accept that WHOIS is fully implemented, accept the adoption of the EWG's report and development of the framework to do its work and essentially we are making no further recommendations out of that. So, in at least one case, we are saying, "Thank you, ICANN, you did a good job," subject to the difficulty of not providing a single source, but just having pointers. I personally think that is not a really great implementation, but I'm not sure what other one I would propose in its place. Susan would like to say something.

SUSAN KAWAGUCHI: As always. But, on this recommendation, I think we could include some sort of statement like we were talking about for the privacy-proxy that, okay, it's been six years and we still don't have implementation. Even though … Do I have the right one?

CARLTON SAMUELS: Did we not say that this was going to be a kind of general [inaudible]?

ALAN GREENBERG: I think this is another example like privacy-proxy of despite our best efforts – and I put that in quotes – we seem unable to deal with either relatively easy subjects or difficult subjects in a timely manner. And on a relative scale, privacy-proxy is trivial compared to this one.

SUSAN KAWAGUCHI: No, I absolutely agree with that.

ALAN GREENBERG: So, I think is [inaudible] example.

SUSAN KAWAGUCHI: In the single WHOIS policy … I just was making sure my brain was working here. I think that we should make that as an overall statement, like this is taking a long time and someone should look at this, but then also make that statement in our review of each of the policies that applies to, so we're really reinforcing it.

UNIDENTIFIED FEMALE: I guess I'd like to clarify. Are we talking about identifying the problem or making a recommendation? If the problem is that the process to reach

that point took too long, you still need that to lead to a recommendation which is in some ways specific and actionable.

ALAN GREENBERG: And I believe we will do that. Stephanie?

STEPHANIE PERRIN: So, we're accepting that WHOIS RT recommendation 2 is fully implemented. Can you please remind me what WHOIS recommendation 2 was?

ALAN GREENBERG: There should be a single WHOIS policy.

STEPHANIE PERRIN: A single WHOIS policy.

ALAN GREENBERG: Identified in a single place.

STEPHANIE PERRIN: And we are accepting that the board initiated EWG and the board initiated PDP is …

CARLTON SAMUELS: Is [inaudible] to the single policy.

STEPHANIE PERRIN: Right.

ALAN GREENBERG: What we are saying … Sorry.

STEPHANIE PERRIN: Well, then, recommendation number 1 was that WHOIS be a strategic priority. And what are we saying about the strategic priority?

ALAN GREENBERG: I believe when we get to discuss it, we'll say we don't think they did a really good job.

STEPHANIE PERRIN: Well, I guess this is where my question is coming. So, we're kind of doing two before we're doing one. Two might've worked a whole lot better if we had addressed one, in my view. When I came in onto the EWG, I didn't quite realize what I was walking into, the intense hostility, the lengthy battles.

UNIDENTIFIED FEMALE: [inaudible].

STEPHANIE PERRIN: No, no, no, but certain parties were plenty hostile to me and very suspicious of what I was doing there, along with plenty of the other members of the EWG. So, I don't really think that effort was launched in a way that would assure the strategic priority and I think the seeds of its … I mean, I'm not saying we didn't do great work, but the seeds of failure were already sown by the failure to address one.

In other words, I'm saying I'd sure put a lot of caveats around this statement. Yes, kind of, but it depends on what you say about one. Same thing with the RDS PDP. Unless you explicitly recognize the blessed battle with new combatants that arrive for the RDS PDP, you're not going to figure out how to make any progress.

CHRIS DISSPAIN: Can I ask some questions? Because I'm confused again. I'm not clear. I guess you could argue about whether … Let's be clear. These recommendations are made to the board, so you can argue that the board didn't arrange for or didn't treat WHOIS as a strategic priority in the way that you think it should've been treated as a strategic priority. Given that there's no definition of what that meant, I could argue [inaudible]. I'm not going to, but I'm just saying …

ALAN GREENBERG: If we're going to talk about strategic priority, can we at least get the slide …

CHRIS DISSPAIN: No, I'm not, I'm just saying I wanted to [inaudible] this one. So, I get all that and I'm very happy to have that discussion when the time comes, but I am at a loss to understand what that has to do with this particular one because what was recommended has been implemented. The board can't make the policy. The board did two things. It put in place an Expert Working Group and now there's a GNSO PDP. That is it.

ALAN GREENBERG: You're agreeing with what it says there.

CHRIS DISSPAIN: Absolutely. I don't understand how you can caveat it. Stephanie, what …

ALAN GREENBERG: So, you're not arguing with us. You're arguing with Stephanie. Just to be clear.

CHRIS DISSPAIN: Correct. It seems to be outcomes and the recommendations can't legislate for the outcomes, neither can the recommendations have any effect on the outcomes. So, I don't see how you can say that … I just don't understand the connection.

ALAN GREENBERG: If you'd like to respond, you may respond.

STEPHANIE PERRIN: I sense I may be the only one that feels this way and maybe I'm out of scope for what a review team actually does, but they're all rather linked. If it takes six years to get a privacy-proxy policy through, then maybe we're going about it the wrong way and that might be because we're not putting enough work into recommendations 1 and 2 to actually figure out strategically how to do something.

In a very difficult [inaudible] environment, it's a bit like when you pop a law into parliament. You have to figure out how it's going to get passed. I realize in the US Congress there's an awful lot of laws where nobody ever thought they would pass and they just throw them in, but that shouldn't be the way a volunteer organization works. We should be reasonably certain that we're going to get a result if we initiate a PDP process, for instance. I realize the board maybe can't predict, has to be hands off. But, that doesn't mean you don't do the policy work and figure out what might have a chance of succeeding.

ALAN GREENBERG: I have a queue of Susan and Lisa and Carlton after that. I put myself in the queue first. I didn't jump the queue. I put myself in before they put their hands up.

I think we have decided, although we haven't fleshed out the words, that we are going to make a strong recommendation that ICANN needs to rethink how it develops policy if it takes this long to do some of these things. Okay. Let's take that off the table in this discussion. I think the world is different from what it was when these recommendations were written. I have spent a fair amount of time talking to people about what

I believe are the problems with the PDP and related things, and up until recently, when I said those kinds of things I was told, "No, you're wrong."

I attended a meeting at ICANN 61 where the same people who repeatedly told me there is no problem were standing up and talking about why the current PDP, such as the new gTLD subsequent procedures and the RDS1, are having such a hard time working. I had a hard time standing afterwards because I didn't believe these words were coming out of the people and the GNSO Council is debating this seriously. So, there is an acceptance … I think we have a community that is going to be more receptive to us saying this than we might have ever before. Instead of being completely ignored, people are acknowledging there are problems. That's a positive sign. It doesn't fix them, but it's a positive sign. But, that's not what we are talking about here.

Now, are we unhappy that the world didn't work better and we didn't end up in this period of time with a new WHOIS policy that is all-encompassing? Yes. We're all unhappy. But, I think within the constructs of what the board and staff could have done, they have fulfilled the mandate. Not the way I would have liked to see it done, but I'm acknowledging that since I cannot tell in my wisdom how you should've done it differently, I have to accept what was done.

So, I'm happy to accept what is there. It may be the only recommendation that we say was implemented. And I'll get off my soap box. Susan?

SUSAN KAWAGUCHI: So, I don't know if you have what's in the slide deck, the single WHOIS policy. I agree that if this was … You're looking at me. I thought I wasn't doing something right with the microphone.

I agree that this should have gone … These recommendations, worded differently, may have resulted in a different status than what we have right now, but we can't go back and rewrite these recommendations.

So, there's two components. Oversee the creation of a single WHOIS policy – I think they did that in the EWG, which led to the PDP. So, the board has done that part because they can't do anything more than those things. And then documenting all the WHOIS policies and the contracts and everything. So, those are two elements of this.

I mean, I guess we could continue debating whether or not those were done, but I think what you have in mind – and correct me if I'm wrong – is we really need to write another recommendation now and say maybe combining these two and saying, okay, it didn't work, so let's start over and this is our new recommendation from this review team.

STEPHANIE PERRIN: Let me respond to that, if you don't mind. I am not trying to rewrite the questions that were set back in 2011 by any means. I think that there was enough friction on the first WHOIS Review Team that one could have predicted that it was going to be difficult and there is a perception out there that a shortcut was taken with the EWG, that that was going to sort of do an end run around the PDP process which might be construed as not particularly working well.

So, I think that a slight, as they say in cooking – I won't bother with my cooking analogies. A slight nuance that perhaps a little more thought going in … The board did its best. It did this, it did that. But, we still don't have the policies. I'm sorry Chris isn't here, but I don't think the board can just wipe its hands and say, "Well, we did our bit. The rest of you guys don't know how to run a PDP process, so it's all your fault." I don't think that's good enough.

I think, for instance, even on the RDS PDP, it was pretty obvious a year ago we were getting [inaudible] nowhere and nothing happened, which is why I was so deeply suspicious when I quit the PDP and upon hearing about the interim policy, it sounded like another … I'm on the record here, I know, but I'm up to my neck right now anyway … It sounded like another runaround. [inaudible] board will just impose a policy. I'm sorry, but PDP was on the pathway to hell, as my father would've said, a long time ago. We weren't getting anywhere and nothing was happening to stop the people who refused to even do their [homework] let alone contribute constructively to the discussion, and bringing in the ombudsman is no cure for that. So, I'm not comfortable saying, "Oh, yeah, tick-tick, the job was done."

ALAN GREENBERG: We are not going to fix the PDP here.

STEPHANIE PERRIN: I know, but you have to answer the question. Was it properly done? No. We wasted a lot of very valuable volunteer time doing this.

ALAN GREENBERG: I think we've already established the fact that the PDP process seems to have some problems with some classes of tasks. Do remember when we're looking at the overall timeline, we took a break of two to three years for the IANA transition. The Expert Working Group finished a long time ago and we didn't start the PDP because of exhaustion of the community until we were well into the IANA transition and accountability things. So, the timeline has been expanded significantly because of that.

In any case, we have a speaker queue at this point. I've lost track of where I'm going. I think we have Susan, Lisa, and Carlton in that order.

SUSAN KAWAGUCHI: I talked.

ALAN GREENBERG: You talked, then Lisa. Unless I'm looking at a list for some other subject, I've lost track now.

LISA PHFIFER: I put myself in the queue maybe to step back a bit. We have identified some general overarching recommendations through the course of our conversation today and I think even yesterday, one of which was the need to have a more effective policy development and implementation process that would produce more timely results, but we also, stepping back to what you said first thing in the morning is what is our objective

in trying to formulate recommendations here? I'm wondering if we're not essentially doing the last bits first. Should we not step back and say, okay, what is it that we're trying to accomplish with this walkthrough of overall WHOIS1 recommendation implementation, and if what we're trying to accomplish is to put on paper some of the recommendations and to look at the ones that some subgroups, but not all, produced yet, what are we trying to accomplish with those objectives? Because you can't tell whether the recommendation is good unless you know what it is you're trying to accomplish with it.

ALAN GREENBERG: Carlton?

CARLTON SAMUELS: Okay. So, we already agree that there were two parts to this recommendation. One is documentation, and I propose that if you think the single webpage with links to all things WHOIS is a good enough facsimile for a document, then you could accept that that part of it is implemented and it's done.

The other part of it goes to whether or not the board could set up a single WHOIS policy and they put a framework in place. They did two things. They chartered the EWG to come up with new thinking about what overarching WHOIS policy should be. The reporters made, the board had a resolution saying there's a next step, and in the next step there were very specific things. It said pre-work groups and this framework was developed with a bunch of GNSO councilors and the board. That's the framework. And it says pre-work group steps, issues,

report, and input development phase one policy requirement, phase two policy functional design, phase three implementation and coexistence guidance, and then four post-work group steps approval IRT formation implementation. That is supposed to be the framework that is going to be followed to get a single overarching WHOIS policy in place.

I am going to make the case that if you had followed the framework as was agreed by this group, you would have timely results. What we've see, though, so far is a lot of [inaudible], people reinventing the wheel. That's why it's going to be slow, because if you just stuck to the framework agreement, things would move much faster. That's how I see it.

So, that is why I recommend that a) the documentation part of the recommendation is implemented, so long as you accept that in the digital world a webpage with links to all the various documents could substitute for a single document and b) the board did as much as it could in terms of trying to get a single WHOIS policy that would bring all the bits and pieces together by laying out a framework of action that was agreed with GNSO Council as a subset of them that agreed that this was going to be the way it was going to go. That is why I'm recommending that the policy – that specific recommendation is fully implemented.

ALAN GREENBERG: Cathrin?

CATHRIN BAUER-BULST: Coming back to what Lisa was saying also about the objectives, we could of course go back and look at what the board could've done differently and whether there were any other tools in their framework that they could've used to set up the PDP in a different way or to instruct it as it was not moving at all, and maybe the one thing … If we agree that this has been implemented, maybe the one thing we could look at in the framework of the [inaudible] recommendation we might want to make on how the policy process functions is to take a look at the toolkit that the board has to influence these processes and see whether that's fit for purpose or whether that would need to be reconsidered in the face of PDPs that are clearly not moving along and how this could be addressed.

CHRIS DISSPAIN: May I respond to that please? I'd just caution about … Some people in this room will attest I'm renowned from my ability to step on the toes of especially the GNSO folk, but I caution about doing anything in this review team that [inaudible] of suggesting changes to the way that the policy development process operates all the way to the GNSO operates. I may have misunderstood, but if you were talking about was saying the board's only tool is to [inaudible] PDP and we should therefore look as to see whether or not that could change, that would involve … It struck me when I was listening to you that I could interpret that as saying consider moving the responsibility for making that policy outside, but maybe I misunderstood. No? Okay, then I did misunderstand, so I apologize.

ALAN GREENBERG: Cathrin, then me, and then Lisa.

CATHRIN BAUER-BULST: Sorry. It must be the non-native speakers. I'm doing a lot of clarifying of my random ramblings here. It's just I'm wondering whether, as the board, in the way that you can call on PDPs to be launched by the GNSO, whether there is additional guidance that you can provide as the board in how the PDP, whether there's specific deadlines that will need to be respected and what would need to be part of the terms of reference of the PDP, and if that's not already in the policy for what the board can do, then maybe consideration should be given to this and other elements to be added to what the board can do in order to contribute to the smooth functioning of multi-stakeholder policy development process.

ALAN GREENBERG: We have a speaker order is what I'm saying. If you'd like to get in, we'll add your name to the list. If I may recall for those who are, again, old enough, we had a PDP a while ago because of some GAC advice on Red Cross and Olympic committee names, and the GNSO was advised through whatever process, not an official process, that it really needed to get this done quickly. And it did.

I would not want to go anywhere near suggesting that we should add things to the board's toolkit to be able to do that. Now, there are subtle pressures one could add, but that's not … I think what I heard is we are interested in making a recommendation that ICANN needs to rethink how this is done. Based on what I'm hearing today, this would be

received very well and perhaps will already have been done by the time we get around to issuing a report.

So, it's a very different thing about being very specific and targeted in saying how to do it and simply saying it needs to get done, but it's not our job to do it. I think that goes along with what you were saying.

CHRIS DISSPAIN: Cathrin, I acknowledge that distinction between what I said you said and what you said, but my concern stands that what governs the way that the policy development process works is the structure of the GNSO, not the board. So, the board can say … Basically, the board is [inaudible] the GNSO to call a PDP and it has done so. In fact, the current WHOIS PDP is in essence a board [inaudible] PDP.

But, what the board can't do is to say, "And please do it within six months and please use the Expert Working Group," basically copy everything the Expert Working Group agreed to do. They can't do it. It would be wonderful, from some people's points of view, if they could – but they can't.

In essence, what I'm saying is it sounded like what you were saying to me meant recommendations about things that would effectively restructure – not restructure, but change the way the GNSO operates, which would be wonderful, but isn't actually in the scope of this working group.

ALAN GREENBERG: You should make that recommendation right after you tell the GAC how to operate their business.

CHRIS DISSPAIN: No comment.

ALAN GREENBERG: We have Lisa and Carlton.

LISA PHIFER: So, I thought it might be useful to just briefly walk through the steps that led to this. Upon reviewing the first WHOIS Review Team's recommendations, the board decided to … Well, with input from public comment, then advice from the SSAC, decided to initiate a two-prong process, one where the organization would fully enforce policies that were in place and the other that would envision a more comprehensive WHOIS policy for next generation.

In doing that, the board asked for an issue report. The board directed that a PDP open and asked for an issue report to be developed. One of the things that the board did as part of that is actually set the scope of the PDP. I want to point that out. The scope was set at that time by the board. In order to set the PDP up for greater success than the previous 15 years' worth of task forces that had not succeeded in policy overhaul, the board initiated the Expert Working Group, put a tremendous amount of resource behind the Expert Working Group in terms of if we ask for analysis, if we asked for a face-to-face meeting, whatever we asked for we got in order to try to produce output.

The board's role in that process, they did monitor. They did send Chris and Steve Crocker to all the face-to-face meetings. So, they did provide an active role in the Expert Working Group, not necessarily in suggesting what the group should find, but in providing guidance and being available to ask questions and provide answers anytime that was asked.

When the report was published and delivered to the CEO, the board met and considered what had been produced and then reaffirmed its request for the PDP, taking into consideration as applicable the Expert Working Group.

So, it was not a directive to use the Expert Working Group as the policy, but rather to use it to inform the policy-making process.

Because it was clear that the issue at that point was so incredibly broad and complex and full of inter-dependent pieces, the Process Working Group was formed to produce the framework that Carlton described. In that process framework, there are requirements for the manager of the PDP, which is the GNSO, to establish deadlines, to provide oversight to see that deadlines are in fact being – progress is being made towards the deadlines I think is what the process framework says.

So, the role in coming up with the process framework was actually collaborative for board members and members of the GNSO Council to talk about the challenges this group will face, and how can we put a management framework around that, if you will, to help them actually succeed.

Once the PDP was initiated, however, I think that was kind of the end of the road from the point of board involvement. I know that Board

Working Group has sort of an ongoing touchpoint role, speaking to the leadership of the PDP, but in terms of actually trying to steer things, that was the point at which it became the GNSO's baby to continue to raise.

CATHRIN BAUER-BULST: Thank you, Lisa. I'm speaking out of turn just to say that's been extraordinarily helpful.

ALAN GREENBERG: Carlton was next.

CARLTON SAMUELS: No. Lisa actually said everything I wanted to say and I wanted to put up the framework to show you how the thing was structured. They even went as far as deciding which pieces of the pie go in each step and this was with the GNSO Council. The only thing that was different is that once that started, once that was agreed, it was hands off because they were very mindful that they don't want to step into the GNSO's bailiwick for developing policy, but if there's an issue, it is the fact that the board is acting as the board should which is to provide from steering up to a point, the point where they can rationally do so and get out of the way. What has happened is that we didn't follow the process [inaudible].

ALAN GREENBERG: A lot of things happen, including the fact that there are many people who were participating in the PDP, certainly at the beginning, who were very mistrustful of the EWG report and certainly did not want to accept the concept that we might just accept parts of it. There were people on multiple sides who took that position and felt that the work had to be done from scratch.

Look, we could do a critique of the GNSO, of the history of the two years of the RDS PDP. I really don't think that's a productive use of our time right now.

Stephanie, please go ahead.

STEPHANIE PERRIN: I take it that's a prefatory remark prior to me opening my mouth. I do think that from a management perspective, and the board has a management role, in order to get work done there's really three things you have to look at. Have you set up a proper framework form a policy perspective that permits people to work – not sets the policy but set up a framework in which they can work – set up proper procedures so that they can get the work done, and set up proper HR conditions?

Now I have to say that the mediation help that we had on the EWG was not inclined to inspire confidence in me at any rate nor in my constituency, pointing out that I wasn't in my constituency when I was on the EWG. But that mediation wasn't enough to have everybody immediately yell, "Get us mediators." But it might have helped.

But that's an HR issue and in my view the PDP if you stopped and looked at where we weren't going after a year, those three factors are very important. The policy framework wasn't adequately set. It allowed people to just reject any of the work that had been done in the EWG. It allowed people to come in and just basically rag the puck as we say in hockey and nothing could be done to stop them.

Now I think that's a management responsibility, and I think that something should have been done. This is why I'm not comfortable with saying, "Well, the board did everything, tick, tick." What's our goal in writing this report? I think whatever our goal is, we certainly don't want people to read the report and say, "Well, they don't know what they're talking about. They're just going tick the box." Just like we have looked at some of the other things and said, "Oh, they're just ticking the box." We don't want to do the same thing. We need critical analysis.

ALAN GREENBERG: I don't think we're writing the text of the report here. I think we're trying to agree on overall concepts.

Chris, please.

CHRIS DISSPAIN: Stephanie, with respect, you are wrong. It is precisely not a management issue. It is a GNSO issue. The GNSO decides how it makes its policy and it's governed by their bylaw. And there is nothing that the board could have done to prevent the GNSO from deciding – in fact to prevent the GNSO from completely ignoring the Expert Working Group

report should it have chosen to do so. It is not a management issue. It is not a board issue. It's a GNSO issue.

The Expert Working Group was put together. It was embraced by a number of people who moved into it from various aspects of the community. But it always suffered from being something that Fadi basically plucked out of thin air as a thing that should happen that was always going to struggle to get acceptance with some parties in the GNSO. And there is, frankly, nothing anyone could do about that apart from the GNSO.

So I'm sorry. With great respect, you are wrong. It is not a management issue.

ALAN GREENBERG: Is there any further discussion on Recommendation 2? Susan?

SUSAN KAWAGUCHI: So not necessarily Recommendation 2, but we could address the fact that Fadi plucked that whole EWG idea out of thin air and we wouldn't recommend that again. Because it did create some trust issues there and was not – I don't know. Could the GNSO Council at that point have said, "Hey, stop. This is not policy"? I don't think they could have done that because they might have done it. And he also lied because he said 90 days.

ALAN GREENBERG: Well, up until now we have been using the party line that the EWG was a board idea. I'm not quite sure we want to switch even if there was some reality to what [you're saying].

CHRIS DISSPAIN: Yeah, I'm sorry. It would be unfair of me to blame it on Fadi in the sense of I'm not entirely sure whether it came directly from him or not, but it became a board endorsed thing. It's quite clear that the board [bought into that].

ALAN GREENBERG: Certainly the chair of the board took it as one of his babies.

CHRIS DISSPAIN: You are indeed correct.

ALAN GREENBERG: Stephanie?

CHRIS DISSPAIN: But again, the recommendation doesn't say how the review team wanted us to treat it like a strategic priority.

ALAN GREENBERG: If we're going to start poking holes in how ICANN has done things over the last eight years, there's a long list. Stephanie?

SUSAN KAWAGUCHI: [We're] just trying to limit the focus to this particular recommendation, and I think in this respect obviously Chris knows better than I whose responsibility the management is. If this is totally a GNSO management responsibility, the problem, of course, is that initial lack of trust that carries through. So when you know that the terms have been set up by a joint board and GNSO group and an excellent scoping document was released and there were proper comments on it and yada, yada, yada, but nevertheless the board still has a working group that communes with the GNSO RDS group and we don't necessarily find out what the output of that was. Things are a lot more transparent now. But I still regard it as having set in place a process, however remote the manipulation is, we were set up for failure and now we're reaping the harvest.

ALAN GREENBERG: I'd like to exercise chair's prerogative of calling this to an end. Our rules are that we will make decisions by consensus and we have a rule of thumb. Is there anyone in the room other than Stephanie who believes that we need to adjust what Carlton as subgroup leader has suggested? Then I say for the moment that is accepted and we'll move on to another recommendation.

I thought you had some new slides, so we're just summarizing them.

CARLTON SAMUELS: [inaudible]

ALAN GREENBERG: Okay. All right, the next one that came up in the lottery is [Jay's] outreach. The recommendation of the subgroup was that we are recommending that the entire compliment of WHOIS and registration information be reviewed and reformulated as necessary. Again, we're not trying to word the recommendation right here. And to be consistent and be focused on a user orientation that is understandable by people at the various different levels. And in terms of timing, it should not be undertaken until we have some level of stability with regard to GDPR and privacy issues.

CHRIS DISSPAIN: Alan, may I ask a question? All we're doing right now is just looking at it and saying this is yes we think but do not discuss? Do you want us discussing? I'm interested, for example, in hearing what the rationale would be for making this recommendation. I presume we're going to produce a rationale at some point. Because of this, this, and this, we think you should do that. That's fine, but I just wanted to check that that will be discussed at a later date?

ALAN GREENBERG: Well, it was discussed yesterday at a significant level of detail. I'm not sure if you were out of the room at the time.

CHRIS DISSPAIN: No, no. That's fine. I'm very comfortable with that. As long as it's….

ALAN GREENBERG: The analysis was there are lots of documents.

CHRIS DISSPAIN: Yes, and we want to bring them all together.

ALAN GREENBERG: They were written at different times. They're not consistent with each other. They don't point to each other. And all of that.

CHRIS DISSPAIN: That's fine. I'm comfortable with that. So we're going to use that discussion of yesterday's as the basis for crafting our rationale?

ALAN GREENBERG: That's correct.

CHRIS DISSPAIN: Cool. Thanks. That's exactly what I wanted to hear. Thank you.

ALAN GREENBERG: And that is in the draft report that was circulated for that session. Erika, you look like you want to say something.

ERIKA MANN: Alan, I think it is already covered what I wanted to say, [the up-to-date]. I was just trying to understand the sentence, the WHOIS, the second part [inaudible] the education tools ICANN Learn and video and tutorials [ensuring] up-to-date and consistent messaging. My key complaint was that many key information there was no update. The last information one could find was in some [key] areas early 2017. I think it's covered.

ALAN GREENBERG: Early 2007 or 2017?

ERIKA MANN: 2017.

ALAN GREENBERG: That's late in my mind.

ERIKA MANN: No, no, no, not on this topic. Some of the topics I checked are really changed since 2017, and they have to be covered.

ALAN GREENBERG: The references there, I haven't looked at ICANN Learn documents, but many of them have been out of date. Some of them have been rewritten recently. The video tutorials tell you to go to InterNIC to do a WHOIS search. Those are just examples.

ERIKA MANN: Yeah, I agree with you. That's why I was reading the sentence and you understood me that I was trying to say something. I was just trying to understand if the last part, "ensuring up-to-date," relates only to the ICANN Learn video and tutorials or relates back to the WHOIS portal. And it relates back to the WHOIS portal, so I'm fine.

ALAN GREENBERG: It relates back to the whole sentence.

ERIKA MANN: Exactly, the whole sentence. Yeah.

ALAN GREENBERG: Lisa?

LISA PHIFER: Yeah, I had actually the same question. So I think the recommendation is actually interrupted, if you will, by the list of examples. So I think the recommendation is that the public-facing information related to gTLD registration needs to be reviewed and reformulated to ensure up-to-date and consistent messaging. And that includes…. Correct? But that was your goal.

ALAN GREENBERG: Yeah. I included the parenthetical because I suspected a lot of people weren't aware of any ICANN educational materials.

LISA PHIFER: I agree.

ALAN GREENBERG: Further discussion? Spin the wheel and we'll see what recommendation – oh, sorry, Lisa.

LISA PHIFER: Sorry. Yesterday we talked a little bit about what the target was for this registration information, and I think you questioned whether consumers were one of the targets or not. Can we get some clarity on that.

ALAN GREENBERG: Oh, okay, I'm sorry. On the second part. I think our analysis will be – and I need to look at the response we got in detail – but the response I think basically says GDD people talked to people and of course we would have talked to them about WHOIS if it was relevant. Not a particularly detailed response about what kind of outreach they did. But I think in light of things like GDPR, the world will be very different going forward. So any outreach that was done three years ago on last year's WHOIS is not particularly relevant.

I think that program of outreach, including to both ICANN communities and non-ICANN communities, is going to have to be rethought. So we can slap them on the wrist slightly saying you might not have done what we asked for, but I'm not sure it's relevant going forward. I think the recommendation for outreach will be reiterated in the context of

whatever the new WHOIS is at that time. At least that's what I envisioned yesterday when I was talking about it.

Further comments? Lisa, go ahead.

LISA PHIFER: Sorry, I just want to make sure I really understand the objective here. In redoing the documentation, we're doing outreach such as GDD does. Would that still include the individual user as part of who you're performing outreach to? Or was it only those who were inside the stakeholder fence?

ALAN GREENBERG: I'll answer, and then I'll go to Erika and we may go to Cathrin because Cathrin has pointed out that within Germany there has been outreach to users saying WHOIS may be a valuable tool for you to establish who it is you're dealing with. Based on the outcomes of GDPR and associated things, those users may have zero access, at which point we're not going to go telling them to do it. So I think the outcomes will depend on how the world unfolds.

But if users can make reasonable use of WHOIS, I think then we probably want some level of outreach, although I'm not quite sure how you do it or who you go to. Consumer organizations in many countries seem completely disinterested in this kind of thing. Other countries may be more interesting. [There's probably interesting paths] if we have anything to advertise.

Erika?

ERIKA MANN: I agree with both of you, Lisa and Alan. I think we want to do this, but it has to be done in such a way to allow individual users to understand the context. I don't think we need another educational, something educational to be done. But when they review the portal, I think they have to search for places and locations where it makes sense to approach the individual user directly, choosing a language which they will be able to understand.

The pages I reviewed, sometimes you find a location and you see that's a paragraph which needs to be edited saying to understand the WHOIS environment you have to look into the following. Just the tiny introductions which are sometimes missing for individual users who are not familiar with our environment to understand what the specific chapter is actually talking about. It's not super complicated. I think any good communication person can do this sitting in a communication department.

ALAN GREENBERG: Just to follow on, then I'll go to Cathrin if she wishes. I think I said yesterday that this should be done using focus groups or things like that. For instance, if indeed WHOIS has some meaning to individual users and whatever they can get out of it, we probably don't want to provide to them the raw output that we get from WHOIS today in our standardized format. That produces three screens of information, much of which is not relevant to them. If it indeed has a real use to individual users, we probably want to formulate it and format it somewhat

differently. I think these things have to be taken into account, depending on who the target is.

Cathrin? If you wish.

CATHRIN BAUER-BULST: I'm always happy to talk. I'm not sure I have anything to say, but I think this was the example. I mean, the outreach to consumers specifically, if here we define consumers as your noncommercial user of the Internet, that outreach if we make any recommendation on it would only be useful if there is something that your normal user can still access. And as of now, it doesn't really look like that will be the case unless we go for volume limits rather than for upfront user group limits. So there I would really say that we can determine whether or not the recommendations of the [RT1] have been implemented, but at this point I don't really see an avenue to talk about promoting this to the consumer if the consumer has no access. So I would just drop that one.

ALAN GREENBERG: Remember, consumers in Europe may have no access to information, but registrants in Europe may have access to registrants – ugly Americans and ugly Canadians – who may still have their information public.

CATHRIN BAUER-BULST: Or even pretty Americans and pretty Canadians. But nonetheless, I don't believe in this regional implementation business. I just don't see it happening, and we can condition the whole thing. But I think we should

think about the general sense of it. We can certainly say it might be useful to reach out to consumer protection agencies and just point out to them that this is something to consider in general consumer awareness raising strategies that this tool is available. But to put ICANN in charge of just reaching out to the world I don't think is a reasonable approach, and in particular, if there is not going to be any information that's useful.

And I would posit that if a large part, a major region is out anyway, the question is whether it really is reliable or whether then it will have downsides for European businesses because no information is accessible which might make them look less trustworthy or whatever. Then I don't see it as a useful tool anymore for the direct consumer protection.

But I think what we have discovered in Erika's point is that there are two elements to consumer confidence. There is the direct outreach to the consumers, but there's also the indirect mechanism for fostering trust which is the use of the WHOIS by antispam, anti-phishing, antimalware tools. That can still work just fine, but that's not the outreach part.

ALAN GREENBERG: I don't think there's any disagreement. All we're saying is there should be outreach as appropriate based on the various applicable uses and what's available, and we're just not defining what they are right now. Remember, the outreach is not just on how to use it. It's outreach on why we collect it. There's all sorts of rationales that go along with it.

Erika?

ERIKA MANN: I would argue that even let's assume the worst case scenario, there will be no WHOIS data visible, you still would have to explain to everybody – to the individual user and to everybody else – you have to explain what's going on and you have to explain why information is not visible any longer. I think I believe this information becomes even on the WHOIS portal you have to explain it.

Because first of all there's a history, so you have to explain the history what is suddenly happening, why information is not seeable any longer. And then you have to explain it because I'm pretty certain even for consumers there will be many who will argue, at least on a global scale, but we would love to see this information. So you have to give background information an explain what is actually going on. And this has to be done, this was my only argument, it has to be done in simple words, not always so complicated that only ICANN insiders can understand it. Wouldn't you agree?

CATHRIN BAUER-BULST: Yes. I think we're again vehemently agreeing. But my concern is going back to what we discussed a couple of times about being specific in our recommendations. I think if we are just saying you need to in general review your approach and then make sure that outreach works. I'm totally [caricaturing] the whole thing here, but I think that's the kind of thing we should avoid.

If we are asking the board to look at how you can better educate everybody on what's happening to the WHOIS now, I think that's a bit different from the outreach that was meant under WHOIS1 Recommendation 3. And then that's a new issue we might want to cover separately, so I would take those two apart. I would still say maybe we can park this one and come back to this specific wording in a couple months when we know a bit more at least about where things are headed. I'm being extremely optimistic here, but that's me, and then see whether we can be a bit more specific in the wording because that I think would be very helpful to everyone, also to our [credibility].

UNIDENTIFIED FEMALE: So listening to this, it occurs to me that trying to identify the target for the outreach is maybe sort of a proxy – sorry, bad context – for my real question which is, what are we trying to accomplish with the outreach? If in formulating the actual recommendation, we can identify some of the goals of the outreach, then that would provide the organization more guidance so that when it does the review and update and make sure that it's actually aiming at those goals instead of simply producing documentation that is at the level that a consumer can read or a domain name manager can read. But what is it you want to say to them? That will be helpful.

ALAN GREENBERG: I think if you look at the portal right now, there was a philosophy saying WHOIS is important to us therefore it's important to everyone and therefore we have to educate them. I'm not quite sure that was

rationale for the original recommendation though. Susan, can you come up with any rationale as you recall it?

SUSAN KAWAGUCHI: Well, we were definitely concerned that it was a tool that you could verify. In some cases, you might be able to verify whether or not it is somebody trustworthy or at least you recognized and that no one outside of those in the know are using. So we felt like with education and outreach that there is a possibility to improve how many people are using it.

Now I'm not sure the outreach has done that, but there is some anecdotal evidence that more Internet users use the WHOIS. The FTC has referenced 10 million uses of WHOIS from U.S. citizens, but there has not been an analysis or study of that. And then we did the brief study of trying to get individuals to walk through and look up WHOIS, which was pretty painful. I don't know how legitimate that study really was, but it is still today people don't know how to read WHOIS records, which is frightening, including some people within Internet companies, which is even more frightening.

ALAN GREENBERG: Any further discussion? Last call. Let's go on to the next recommendation. Oh, good. An easy one: compliance.

SUSAN KAWAGUCHI: Oh, God. Can't we just…?

ALAN GREENBERG: Can't we just ignore it? Let's skip compliance for the moment. Data accuracy is the same as compliance. We have to skip that one too.

SUSAN KAWAGUCHI: Oh, come on. Mine again?

ALAN GREENBERG: Common interface. That is the portal part of the portal. Our summary was we need to define metrics [SLAs] to be tracked and evaluated to determine the consistency of results of the queries and use of the tool. And I thought we also added that information related to compliance should implicitly be passed on to compliance for endorsement.

UNIDENTIFIED FEMALE: Yeah, we did talk about that. There just wasn't a recommendation formulated yet.

ALAN GREENBERG: Ah. Could you say that again for the record with the microphone?

UNIDENTIFIED FEMALE: I'm sorry. I said this one has not been drafted in English because I've left out several words. I was just looking for my notes. I think if this is truly a recommendation, it needs to be drafted better, and Lisa has some ideas.

LISA PHIFER: Well, I guess I still feel like we've skipped a few steps here and that we're looking at a few individual recommendations that were put forward when maybe we need to step back and look at the implementation of recommendations overall and whether that was effective. And then the recommendation should support that as opposed to looking at just pieces of recommendations when we haven't really – well, we certainly haven't applied yesterday's discussion yet, right? So to your point, you had an additional recommendation from yesterday that you haven't had a chance to draft.

UNIDENTIFIED FEMALE: Right.

LISA PHIFER: But also the recommendations then stand alone. They don't link the findings and problems that were identified, which they should.

UNIDENTIFIED FEMALE: Where does that put us?

ALAN GREENBERG: I guess I see that last part as part of the drafting exercise to make sure it is cohesive when we draft it. I feel comfortable right now identifying, doing our analysis and perhaps – forgive the expression – but at a gut feel what is he direction of our recommendations. And as we refine

them, I think we have an obligation to provide rationales and link them to the findings. But I'm not feeling uncomfortable. I don't think any of the recommendations we're talking about at this point are not linked to the findings and are just drawn completely out of whole cloth.

So I'm feeling comfortable with it, albeit there are still a lot of words to be written. If anyone else feels otherwise, then please speak up. I guess I'm not a fan of trying to draft things on the fly in a room with a lot of people, but I think we need a level of confidence coming out of the process that for each of the recommendations we will be able to join all those dots together.

Cathrin?

CATHRIN BAUER-BULST: I still think for me this is going a bit fast. I understand that we need to have a first go at the recommendations, but I just feel like we're so – and we've not yet finished going through the problem and we are I think still assessing bits and pieces. And I think it's helpful to just take off a few recommendations now that we're sure we want to make but with a view to coming back to these.

And I still do think that we should talk about what the overall objective is with all of this and then that will tell us something about each of the recommendations as well, how those should be designed and whether they're still useful in view of this overall objective. I guess it's just a different way of the top-five methodology. You want to make sure that it's relevant and that it's important, and you can only assess that once you have decided what the objective is.

And obviously the objective for the first review team was to make sure that we had a better WHOIS. I think that's the overall objective that very clearly shines through all of the recommendations. And we don't even have that luxury at this point to say we're striving for a better WHOIS. So we need to make sure that we know what it is that we are striving for.

So I can say something about what's up there on the screen, but I'm not really sure that I will feel the same way four weeks down the line if we've had a bit more reflection on what the objective of the team is in this sense and once we finalize what I think should be our problem definition.

CARLTON SAMUELS: I'm trying to see how we could go about this probably a little bit more efficiently. So the [inaudible] now is that we look at the recommendations as they stand and we have a caucus determination if they're acceptable or need more work, right? That's what it is. Is there a better way to do it then?

ALAN GREENBERG: I think that's the case for the simple ones we're looking at. We skipped two of the more complex ones, and I don't think we're anywhere near the point of recommendations on those.

CARLTON SAMUELS: I was going to that because I thought that the easy ones where there was very little controversy, we were trying to tick those off. And then

we were retaining the others that might require extra work, we were going to leave. So we continue on that, or are we trying to change it?

ALAN GREENBERG: Well, Lisa is next, but I've heard from both Cathrin and Lisa that we need to determine what our overall objective is, overall endpoint is. I'm not sure there is a single overall endpoint. I think in terms of the existing recommendations, we're looking at what was recommended. We have no choice. We can't change that. We're evaluating whether they did a good job. That's our mandate. And then we're saying, are there any follow on recommendations which we think are going to pass the test of being worth the effort to do because of some real benefit.

Lisa?

LISA PHIFER: I agree with that. From this morning, I also heard some questions about who the recommendations are targeted to. Are they only targeted to the board, or does this group want to have the ability to make recommendations that are cross-community? Also, speaking to what the goals are in formulating any recommendation, you identified this morning that there are some recommendations that may apply to WHOIS/RDS in any form, no matter what it takes.

For example, compliance was the example from this morning. But focusing on objectives that apply to any system regardless of the contours of that system, if you will. And then other recommendations that go to how the first review team's recommendations were

implemented. Maybe process improvements. So those would be two examples of goals.

And are there any other goals that if you look at any particular recommendation looking at that as criteria or a litmus test or something, who is this recommendation aimed at? If it's aimed at the board, are you asking them to do something they can do? Does it go to process improvement? Does it go to a system? Is it applicable to any system, not just the one that we have today? So a series of questions that might then help guide us in looking at any recommendation and saying, is this a good recommendation?

CATHRIN BAUER-BULST: Yes, I completely agree with this. I didn't mean to suggest that there had to be one objective. I think if we keep the objective we want to help design a better WHOIS, then the recommendations that are independent of any changes brought about by GDPR like the ones on compliance can still serve that purpose. That can be our objective.

Then we can have an objective based on the problem that we identified around the processes to improve the overall process. And then we can decide how reviews are conducted or how review implementation is monitored or do we want to go as far as to say how the policy development processes work. That's really where we need to see how far we want to reach as the review team and what's realistic also in terms of what we can achieve in that objective. I think that's one that will need a bit more discussion.

Then there's a third subset which are those parts that will change significantly with the new WHOIS, whatever form it will take after GDPR and [I would count] a common interface as one that might be very strongly affected. Where as of now, I'm not really sure what our objective is. If it is to create a better WHOIS, then I'm not sure whether the common interface will be relevant to that objective anymore in the future. That's the category that I'm struggling with right now.

ERIKA MANN: Cathrin, it's a good point, but if you [read the] WHOIS, the current [portal] and all the details and you move around from topic to topic and subtopic to subtopic, it is a super good document. It's one of the best documents that we have. But there are certain bits and pieces which either are so sophisticated that it's only understandable by ICANN insiders, so independently how GDPR is evolving, you need a short introduction for other people too because this isn't relevant and key information. It doesn't matter if GDPR impacts or not. It's not relevant.

And then there are certain topics which relate to this point here where you need a little bit more coherence. This is natural because all portals evolve over time because they're updated depending on who is writing it and on the topic of the day. There is sometimes no complete consistency. And this is all actually what I understand is recommended should be done.

So I wouldn't worry so much about the future or how it may evolve. I think this needs to be done independently how it will evolve.

CATHRIN BAUER-BULST: Maybe I'm misunderstanding this one, but I thought this was the one where we used a single lookup tool. To my understanding, that's what ICANN has announced it will deactivate shortly because of the compliance issues. At least the WHOIS.ICANN.org will no longer exist. If there is to be no single interface, then there's no use in us making recommendations about what it should look like. That's just my concern.

ALAN GREENBERG: We've got a queue. I think in a GDPR world, we are looking at something that's far more relevant. Now it's not a single entry box that you type a domain name in and hit enter anymore because if you just do that, you're going to get some very thin WHOIS data. On the other hand, that will likely be a portal or perhaps the portal where you would type in your authentication information, identify who you are, and you may get a completely different set of information from it.

There's going to have to be some sites like that, and surely ICANN will have a responsibility for providing it. So it may look very different and it may look very different to different people, but I think there's still going to be a need. Now are we going to describe that right now? No. We'd be looney to try to do it because we don't know the details, but there's still likely to be a need for a place to go to get WHOIS information and perhaps in very different measures. I can't imagine a scenario where that isn't going to be the case.

Cathrin, please.

CATHRIN BAUER-BULST: Yes, just to respond very quickly, I agree with all of you. What I'm saying is just if we look at the specifics of what the portal looks like now and say we would like it to be slightly different in this sense, then if it's going to be a completely functionality by the end of the year, it's just not going to be useful for us to say this. At least we need to come back and reevaluate.

That's why I now feel not in a position to say anything about what this recommendation should say because ICANN so far, at least when I've talked to them, have said that they're not really looking to provide this. That they would see the responsibility elsewhere to provide this central lookup facility and don't necessarily want to accept that themselves. I do remember, and maybe I'm mixing things up here, that there was a blog post where ICANN mentioned that they would discontinue the single portal, at least the WHOIS.ICANN.org.

So I just think this should be something to park and come back to. That was the only point. Now I don't think – and I'm wasting a lot of our time just by kicking up this whole discussion expressing myself in very convoluted ways – but my main point is I don't think this is an easy one. I think this is one we should come back to once we know what exactly the shape of any common portal, if there is one, will be.

ALAN GREENBERG: Clearly, if we do not run a portal and ICANN decides not to run it, I can surely see we're not going to run the authentication service. But if we choose not to run a portal, then obviously we don't collect statistics. On the other hand, if we are still running a portal of some sort, then I think

we should look at maintaining records of what we're doing and if there are points of failure, identifying them so Compliance or whatever can take action on it. So I don't see how anything we're doing here is in conflict other than if indeed there has been a decision made that I'm not aware of that ICANN will not run any form of portal going forward, then clearly we don't have to collect statistics on it.

Susan?

SUSAN KAWAGUCHI: Two different things. First, if we took this requirement to define metrics and [SLAs] to be tracked and evaluated and took it up a level and not just a common interface but to any implementation, then that could be used for any sort of thing implemented. Even if I wasn't on the WHOIS team, if the WHOIS team had made that recommendation concerning WHOIS, then I think I would draw from that too and say WHOIS review team or RDS review team made this point.

I think it applies across almost any function ICANN is providing. Because if you're going to implement something, you have to know if it works and they don't know if it works. It may work just fine. There may not be a problem, but they can't answer that. And then also if it doesn't work, there are some contractual issues there. So if we tick it up a level and not just point it at this, then I think we have a recommendation there. But to get into the weeds a little bit and guessing what's going to happen is I don't see for the same reasons this common interface was recommended, I don't see that reason going away unless we truly go to

a thick WHOIS for .com and .net. Because .com is always going to be the largest gTLD, at least when I'm caring about domain names.

I think it's a real if that all the registrars are going to transfer that data to the registry. So therefore you still have that same problem of how do you identify which registrars [we're with]. And the thin WHOIS data is how you do that now, and it looks like we will still have the registrar record in a GDPR compliant record. So I think for the same reasons that the common interface was recommended, I'm 90% sure we'll still have those reasons. So I think it's important, though I have no problem with stepping back for a little bit on this once we've memorialized everything and say let's rethink this when we know a little more.

UNIDENTIFIED FEMALE: Susan, I think what you're saying probably applies more generally to other subgroups, but that maybe being more explicit about the intent of the recommendation, not the specifics of it but the intent, what are you trying to accomplish through this recommend would help. And then the recommendation can be formulated around today's system trying to achieve that intent but then still leaves the breadcrumbs for if we don't have today's system but a different system, how do you still meet that same intent. So I think I'm hearing you say that one-stop shopping part of the intent would still apply no matter the mechanism that's underneath.

CATHRIN BAUER-BULST: Yeah, and just to support that, indeed depending on if we want to be future proof, it might be worth just saying again that we think the same

rationale [inaudible] and for this reason there should continue to be a single interface even if it would only serve to point to a smaller subset of the information or whatever. But just to make sure that we don't just have a recommendation that can get tossed out if some minor details change in the whole thing.

ALAN GREENBERG: Clearly, if nothing else, at some point we're going to do a final proofread of a report and hopefully we'll be looking at that in the context of what we know at that point. So I'd like to think that we'll have a sanity check at the worst case. Even if we wrote it in detail today, there's still going to be a lot of iterations before we get to the final point.

Any further discussion on this one? So we have tentative suggestion that if we are going to have a WHOIS interface under whatever name, we should instrument it properly and we should use any information related to compliance that it generates.

Next one, if we have any more simple ones. Or we'll go back to compliance.

UNIDENTIFIED FEMALE: When is our break.

UNIDENTIFIED MALE: Should we take our break.

ALAN GREENBERG: Time for a break. Time for a break. Break. Stop the recording please.

And welcome back to the RDS WHOIS2 Review Team, second part of the afternoon session on 17 April 2018. We will resume our discussion on various recommendations, and this one will be Recommendation 15-16, plan an annual reports.

What we have so far at this point is plan and annual reports are essential to guarantee the effective implementation of any recommendations. More specific methodologies on planning and annual reports should be taken in the future.

Comments and discussion. I will. I'm not quite sure what it means. What does specific methodologies on planning and annual reports should be taken in the future? Maybe it was explained yesterday, but in that case I've forgotten.

LILI SUN: Yesterday when I presented about the implementation of the Recommendation 15 and 16, it was mentioned that there is only a general action plan. There is no detailed work plan for every recommendation. The milestones, deliverables, and deadline are missing. So it's difficult for the subgroup to check the implementation progress for each recommendation. Also, the reporting structure for the annual report is based on activities being implemented, but the impact, the [inaudible] reduction for example for the inaccurate WHOIS data and also the outcome of the implementation are missing in the annual report. So we need an organized reporting structure. So that's where the text is coming from.

ALAN GREENBERG: Okay, that was captured in what we had on the screen this morning, but I guess it's not as well reflected here. If that's just a transcription problem, that's not nearly as significant as I was implying.

Lisa?

LISA PHIFER: Yeah, I think just in general what we've been presenting here on screen were the recommendations coming into yesterday. They're not recommendations that result from discussion that occurred yesterday.

ALAN GREENBERG: Further comments? Now I don't think – we're commenting on to what extent did they document the plan for the last set of recommendations and report on the results. So that's at this point a done deal because they're not going to continue to do that forever. Presumably eight years after the recommendations are in, it's probably time to stop reporting one way or another.

We, of course, could make a similar recommendation coming out of our report saying, oh by the way, we expect you to carefully document whether you're following our recommendations or not. And we may word ours slightly differently to take this into account. But I don't think we're going to do a follow up recommendation on the last implementation plan. I don't think we want anyone wasting time on that at this point.

So I think this will get transferred into a general recommendation coming out of our review echoing what 15 and16 said perhaps in words taking into account what we've learned. Does that sound reasonable.

LILI SUN: Yes, agree. Agree, Alan.

ALAN GREENBERG: [Lisa]?

LISA PHIFER: The reports encompass two different kinds of reports. One was reports on implementation of recommendations of the first review team. So I think what I heard you say was a recommendation could be formulated on reporting the implementation of this review team's recommendations that would have perhaps some characteristics or criteria about how to make those reports more effective.

There also were annual reports on WHOIS that were part of this recommendation. And that series of annual reports on WHOIS or the RDS might continue. But again, the recommendation could address how to make those annual reports more effective going forward.

ALAN GREENBERG: Sorry, these are things I should have memorized and know completely. The annual reports we're talking about, are those largely focused on compliance though or other things?

LISA PHIFER: The annual reports were on all things WHOIS. So basically an activity report: what did we do last year related to WHOIS? Not specific to either recommendations or to compliance. Compliance is a factor, but not everything that's done about WHOIS.

ALAN GREENBERG: I guess it makes sense if there is value in these reports – and I'll be honest, I've never looked at them, so to me they clearly have little value if only because of lack of knowledge about them – then yes we can certainly incorporate it into a comparable recommendation going forward.

Lili?

LILI SUN: Yes, just want to chime in for the annual report. Actually, there is no specific annual report on the implementation of the WHOIS1 recommendations. So there is only an annual WHOIS improvement report which has some reflections about the WHOIS1 recommendation implementation. So my understanding is it's [to the] discretion of this review team whether we can request for a specific dedicated annual report on this review team's recommendation implementation. So it's up to us whether we need a dedicated annual report on the implementation of the recommendations we are going to propose.

ALAN GREENBERG: Correct me if I'm wrong, but at this point it is standard practice for all of the specific reviews to regularly – and I don't know if the word annual or semiannual is appropriate – to regularly report on their implementations.

UNIDENTIFIED MALE: [inaudible]

ALAN GREENBERG: Pardon me?

CHRIS DISSPAIN: Yes, and it's ongoing. In other words, it's a moving report. So it would certainly be more often than annually.

ALAN GREENBERG: I'm not sure we need to have a specific report asking for a specific report out of that cycle unless people feel there's some real merit. If the information that we need is available there and I've already made a number of pointed comments on the fact that I think that those reports were more interested in ticking off, creating green ticks than really confirming that the work is done, so we may well want some interesting words to reflect the fact that the challenge is not to tick it off but to actually do the work. I don't know how you say that more kindly, but I don't think we need a specific annual report. But I would like to see the reporting get a little bit more realistic.

Further comments? Then we're done. Let's see what magic comes up next.

JEAN-BAPTISTE DEROULEZ: The only other two we have are compliance and data accuracy.

ALAN GREENBERG: And I think we need to bite the bullet and talk about them. Did someone whimper?

We had two recommendations that came out of the subgroups initial work. The first one was all new policies implemented should be required to be measured, audited, tracked by the Compliance team. Consistent labeling and display policy requires a registrar abuse contact. Sorry, I'm confused. Consistent labeling and display requires a registrar abuse contact, e-mail address, and contact phone. This would be displayed in the WHOIS record, possibly to include – I'm having trouble parsing that. Would you like to take over?

SUSAN KAWAGUCHI: Yeah, I know. [inaudible] left out a few words and [inaudible]. The consistent labeling and display policy requires a registrar to provide their abuse contact e-mail address and contact phone number in the WHOIS to be displayed in the WHOIS record for each of the registrations they manage.

But when I asked about this from the Compliance team, they said they do not track this to see if there's any sort of compliance with this, which

seems like this is a critical need. I don't know if it's a problem or not. It could be that because it is also in the RAA, so this could be a recommendation. Well, first of all, I think we could do a higher level of recommendation that was not just the consistent labeling and display policy is just an example, but a higher recommendation. All new policies implemented should be required to be measured, audited, and tracked. And maybe it's not by the Compliance team. Maybe we do a full stop after tracked. And I don't even know if measured, audited, and tracked are the correct words to define this.

So does the Compliance team measure things? I don't know. But someone should at ICANN. So if we take this up as a higher, not just point it at that policy, then anything that's a new policy we should have some metrics around. But then that also came up in the common interface, that anything implemented should probably have. Because not everything implemented is a policy.

UNIDENTIFIED FEMALE: I wanted to press a little on that. I think you're in part saying that every new policy should include, I don't know maybe as part of policy implementation, a definition of metrics that then should be measured. Auditing is actually different than measuring metrics, right? I'm not sure whether you're saying that both should apply to every policy, periodic auditing versus ongoing measurement.

And it strikes me that the piece that's missing is probably the reporting piece. So is that your – I realize that was not well formulated – but is that the essence of what you're suggesting?

SUSAN KAWAGUCHI: Yes.

ALAN GREENBERG: We have Lili and then me.

LILI SUN: Actually, I strongly support this recommendation and I would suggest we can remove the word new. So in the WHOIS environment, I have the impression that there are enough policies. The issue is not all the policies are in full effective. Like [inaudible] also like to add the WHOIS data [reminder] policy into this recommendation. So it's already a consensus policy for more than ten years. And I learned from yesterday's discussion it's still in practice for some of the registrars. But according to the implementation report of 2004, there are only 70% of the registrars that send out the reminder.

ALAN GREENBERG: I believe that was the case in 2004. My understanding is it is something which is currently audited on a regular basis and presumably if they have any evidence that it is not being followed, they take action. I don't have any evidence counter to that.

LILI SUN: Okay, my understanding is that regarding to WHOIS in this specific occasion I believe more is less and less is more. We already have the

policies in effect to ensure the WHOIS data accuracy, but the outcome turns out it's not. And besides the Compliance team, I don't think within the ICANN community there is anyone else who can take the responsibility to check the policy effectiveness. That's all.

ALAN GREENBERG: On the WHOIS reminder, I believe we had a note to ask Compliance what the current status is and where are they verifying it.

My question I guess is we're obviously implying all new WHOIS related policies because that's the only thing within our scope. But are we talking about only things that ICANN can measure and report? For instance, we are obliging registrars at least on some category of registrations to validate, verify, check the format of the contact information. I do not believe we asked them to report how many of them when you check are good and how many are bad and you have to get fixed. They're obliged to by the time the name is registered that it be good, but I don't believe they are obliged to do any reporting.

Based on past experiences, there has been very significant pushback from registrars if we ask them to take on new responsibilities, including reporting. So I'm just asking for clarification. Are we saying that ICANN to the extent that it has access to information should report on things, or are we imposing a new set of rules that says if we implement any new policy, we must build into that policy reporting at all levels? I guess I'm asking the question of what did we really mean by this. If we put a requirement on registrars, are we asking them to not only do the work

but report on the various aspects that might be reportable? Susan if you want to answer, or we'll go to Carlton.

SUSAN KAWAGUCHI: You can go to Carlton.

ALAN GREENBERG: Carlton?

CARLTON SAMUELS: Well, my way of looking at it is that we put an obligation on them and it is for ICANN Compliance if they put it in as a regulation, as a requirement is for them to validate that they're staying with the rules. So it is ICANN that the obligation is imposed on ICANN to check to see if they are actually doing the accuracy checks.

ALAN GREENBERG: I guess I don't want to focus just on the accuracy. That may have been a bad example. Are we saying we will build into any policy the requirement to track it and report on it, including things that are done outside of ICANN organization?

CARLTON SAMUELS: Okay, well, in my estimation if we have a requirement, this is a [inaudible] regulatory position that I take, if you think it's important enough to impose it as a duty, then it is important enough for you to check that it is being executed. Rule of thumb.

ALAN GREENBERG: [That's different from this.]

CARLTON SAMUELS: Yeah, but outside or inside ICANN the rule of thumb is if you impose a duty on somebody else and it means something to you, then you have a duty of care to check that it is being executed.

ALAN GREENBERG: Checking is different from them reporting it as opposed to us going out and proactively checking.

CARLTON SAMUELS: Well, it can do two things. I can ask them to report it and based on the trust level that I have, I will accept the report as good or I can do the checks myself. There are two ways to approach it. I personally would prefer that you check it yourself, randomly of course.

UNIDENTIFIED FEMALE: So it would be a little different depending which policy or implementation. But I agree with what Carlton was saying. If it's something that the community decides to impose, then there should be some sort of measurement and enforcement to make sure it's done, especially with the history we have with registrars, some registrars, not following the rules.

What I don't know, which I think we need to figure out before we actually work on this recommendation, are most policies. Well anything that is a requirement of the registrar, is that part of the registrar audit. I've seen documents for the registrar audit, but either I didn't understand them or it's not as detailed as I thought they should be. But I do have access to that. I just haven't gone through it as in detail.

ALAN GREENBERG: Any further comments on Number 1?

UNIDENTIFIED FEMALE: Yes, Erika.

ERIKA MANN: Just a question about the word auditing or audited. It has different meaning. So we mean internal audit of this particular department, the Compliance department, and the corresponding department in the registrar. If they don't have a compliance department, then we do mean there needs to be a person assigned who is dealing with such kind of auditing procedures, yeah?

UNIDENTIFIED FEMALE: Audit may not be the term.

ERIKA MANN: Audited, it's okay. It's used in companies, an internal audit. Do we mean internal audit but sector specific internal audit for compliance?

ALAN GREENBERG: Audit however I think is used in very specific ways in the RAA.

ERIKA MANN: Do you have a reference. [inaudible] check it.

ALAN GREENBERG: So I think we just need to be careful that these words are the right words and don't have a connotation other than what we mean.

UNIDENTIFIED FEMALE: We talked about maybe creating a recommendation for the Compliance team to be proactive and not reactive. In that way, we would ask the Compliance team to not just look at reports of in this example the contact e-mail address is not listed for this registrar. I could only find the phone number or vice versa and ICANN Compliance please do something, some sort of report on that matter. This is where I need or we need to verify on the registrar audit, do they go out and double check that the registrar is doing what they say they do?

I do know on the registrar audit that some of the questions they do ask they want proof. For example, this isn't WHOIS, can you show that your customer has agreed to the domain registration agreement and your terms of service? You need to keep records like that, and ICANN wants to see.

And then on the inaccuracy reports, they have to come back within a certain timeframe to ICANN Compliance, but that seems to be fudged sometimes, and respond yes we've spoken to the registrant or no the registrant has not responded and taken any action so therefore we suspended or canceled the domain name.

But then again, they're not proactively going out there and going, okay, Mr. Registrar, 75% of your registrations are inaccurate. I'm not saying they should do that, but there has to be in a recommendation the way we word it – and I could not possibly word it competently today – is it makes it sensible to implement.

ALAN GREENBERG: Thank you, Susan. I spent a lot of time with Compliance a bunch of years ago. It probably goes back about at least four years, five years, for the couple of years after Maguy got there, whatever that was. As they were building their various systems, because they started off with almost no automation and records that were really usable, they were very proud of the fact that they kept records and could display the compliant reports summarized by registrar and registry. They could recognized registrars that were problematic in various ways.

I presumed at that point, naively perhaps, that they were then using that information when they recognize a registrar who is a real bad actor, that they would proactively either audit them more or check more of their things or stuff like that. I'm assuming their records, their ability to track that is even more sophisticated today than it was then. But your indication from what they're saying is they don't use that in that way. I

think we need to explicitly ask that question. Because I remember sitting in Maguy's office and looking at these charts.

UNIDENTIFIED FEMALE: I've not seen those charts or if I have, I don't remember them. This go round I have not seen them. But Maguy is very clear that they act upon all reports, which we discussed yesterday. They're reactive. If they see something troubling, they're waiting for a member of the community to come forward and say this is a problem and this is the evidence. But that evidence, then they go and do collaborative enforcement and say this party is complaining that you did this, this, and this. If the registrar addresses the issue and then makes that small point compliant, they're done. Close the ticket.

So if you really want to address a systemic issue with a registrar, then you – you being the complainant – need to bring not just one issue at a time and say we're seeing this systemically in this registrar, please go investigate. They will work with the registrar each and every time on each data element you bring them. If you brought them 1,500 inaccurate WHOIS records for one registrar, they would take them one-by-one and say oh, yeah, we contacted them. We did that. Maybe we didn't do it last time, but now we're working with you. Then they're done and they're off the hook. They don't look at it and go we have 30,000 reports for the same registrar for inaccuracy, but each and every time they cured that. That's my understanding.

ALAN GREENBERG: May I suggest that between the two of us we follow up on them explicitly because I don't think I'm imagining seeing these reports. I'm sure the reports I saw were from a previous system that doesn't exist anymore. But I may even have some slides somewhere maybe because they talked about them at ICANN meetings. They did display them. Without the names perhaps.

UNIDENTIFIED FEMALE: In the Compliance reports it will also show you, yes, they took certain registrars they issued breach notices and some of those they unaccredited. But if my recollection is correct, a lot of those were not paying fees because that's very clear. If the registrar is not paying its fees, it's not a simple act to pay them. They could just simply pay them, but maybe they're so far in deep with owing they're not – if they owed $100,000 in fees, they'd rather just walk away and not pay them.

So I personally filed a complaint which took me six months, and this was back in 2011 or 2012, against EuroDNS, a major registrar, that allowed a transfer of a domain name after a UDRP decision had been made. We were in the ten-day waiting period, and so the registrant had the right to assert a claim or appeal in court. We were in that ten-day period. They allowed the transfer. And when I reported it to them, that new registrant immediately went in and filed against Facebook and it eventually cost me $100,000 in Luxembourg courts.

They said that this was the same registrant, just a different party. I'm like, no, no, no. That doesn't work that way. The registrant does not change. Control of the domain name does not change. It took me six

months of arguing with them. Now I think if that was today, [AI] would be smarter. I think they're quicker. But the way they do collaborative enforcement is they do everything they can initially to get that registrar to comply with the policies. They don't say, Mr. Registrar, you screwed up here and you've got five days to change. Now if we want to implement new policies [inaudible], that's a different thing.

So for six months, this new registrant which was really the old registrant I'm sure was getting 250,000 hits a month off Facebok.com. That was worth traffic. We probably paid our lawyers more than he paid his in Luxembourg. They finally issued a notice of breach because I threatened to sue ICANN. And it was like somebody's ass is on the line. I don't care who at this point. I want my domain name. I want the UDRP to be followed. It was so clear cut.

So I don't think we have as many issues in Compliance as we've had in the past, but I still don't think we have – because I brought up the online NIC issue with the inaccurate WHOIS, and they have a policy, a view of the policy, interpretation of the policy that I think we don't agree with and so they go down a different path.

ALAN GREENBERG: Yeah, I'm sure there are more ills that we're going to fix here. But I think we are warranted in considering a recommendation that they must recognize persistent problems and recurrent problems. I think privately, we have to investigate a little bit about why are they not using the tools that they were so proud of having that will allow them to do that if, indeed, they're not.

UNIDENTIFIED FEMALE: Right.

ALAN GREENBERG: I think we can cover that between the two of us.

UNIDENTIFIED FEMALE: Yeah, and Cathrin brought up yesterday using DAAR. So that's just another tool that they've gained in the last two years or so.

CATHRIN BAUER-BULST: Just on this, it has been made very clear that this is not a Compliance tool and that there is complete separation between the work of DAAR and the OCTO team and the work of the Compliance team. I think one thing that we could consider is to encourage them to make that link and to look at what could enable Compliance to take a more active role if indeed they're also just hamstrung by their own regulations which is not helpful. So I think we can probably formulate a couple recommendations from the helping the Compliance team perspective.

UNIDENTIFIED FEMALE: I'm sorry. Carlton, did you want to go first and then I can go.

CARLTON SAMUELS: Yes, just for the record, the CCT actually [inaudible] recommendations pertaining to anti-abuse did make the recommendation that

Compliance take more interest in DAAR and use it as part of the process to eliminate the serial aggressors.

ALAN GREENBERG: In fact, I was told at one point that that was something that was being actively discussed. So it may have been actively rejected, Susan.

CATHRIN BAUER-BULST: I believe this is subject to an ongoing debate and in particular the contracted parties are somewhat concerned about this development. I just remember David Conrad stating this at the update with the GAC which the GAC has actively supported the work of the CCT Review Team and the recommendation on DAAR and it's possible use for Compliance. It's just still under discussion and subject to further evaluation because there's now these two independent experts that are looking at DAAR and the data sourcing to affirm its reliability. Then on that basis, that recommendation could be considered from the CCT Review Team at which point it could become a tool for Compliance. So it hasn't been refused. It's just subject to ongoing validation of the methodology and [resistance] from the contracted parties.

ALAN GREENBERG: Your information is much more up-to-date than mine. Mine goes back to when it was still called DART.

SUSAN KAWAGUCHI: It's more, again, anecdotal in some ways but in a discussion in Puerto Rico with the Compliance team with a matter not associated with this but definitely a Compliance issue and it surrounded [Alpnames], they admitted, yes, we know [Alpnames] is bad but you have to help us by providing evidence. So I was asking what evidence. It's just like anything you have: screenshots, this, that.

I'm like what it means is they have that evidence, and the question in that meeting was asked is the Internet works on using all these vendors out there, the Anti-phishing Working Group for example, and relying on their data and taking action against abuse. But why won't ICANN Compliance then rely on that same data? Why are you asking for more information? What it does is one company or entity might have a scenario, but we don't know what other entities.

It takes banding together and creating Compliance working groups outside of ICANN to say, okay, eBay, Microsoft, Facebook, 15 other companies, let's all get together, provide all this, bring all this evidence together. And then they're going to go, oh, yeah, we see that. Yeah, we knew that. Okay, but now we have the evidence and we can react to a Compliance request.

ALAN GREENBERG: Susan, isn't the right answer to can you provide us with evidence, are you prepared to pay my hourly rate?

SUSAN KAWAGUCHI: If ICANN paid my hourly rate, I'd be raking in the dough.

ALAN GREENBERG: Cathrin.

CATHRIN BAUER-BULST: Thank you, Alan. Susan's anecdotal evidence brings back fond memories of ICANN 60 where I co-chaired a cross-community or I think it was a high interest topic session on DNS abuse mitigation, which has been one of the two pet topics of the Public Safety Working Group, and where we had a discussion about what else would need to happen to the [inaudible] registries and registrars to take action who were saying we're just going to be sued by our [clients] because we don't have the contractual basis to take any action on the basis of this.

Then I said it's clearly in your terms and conditions that you can do whatever. They pretty much leave all their options open [vis-à-vis their clients]. In particular, Tucows was on the panel, and then the Tucows legal advisor spoke up and said, yes, but that's just there to protect us, not to work on DNS abuse mitigation. I thought that was a really telling comment, and I didn't shoot her down right then because I'm a nice person. But I'm just waiting for the right moment because I think this is just screaming.

I mean, it's clear. The contracts that the registries and registrars have perfectly well allow them on the basis of the evidence provided by DAAR to take down the sites. They just don't want to do it. So I think whatever we can do to promote this concept of using the DAAR data and taking action on that basis and supporting Jamie and his team in doing that – I think the OCTO team is already completely sold on this,

but it's the other side that's struggling and I understand that's because of the rules they're under and because of the serious pushback they're getting from the contracted parties.

I understand that it's maybe going to make their lives more difficult, but they either need to take a proactive approach on their own accord using the DAAR data, or if not, then Jamie and his team will just have to come after them using that same set of data and there's no reason why that shouldn't be possible.

ALAN GREENBERG: I like you on that soapbox. Lisa?

LISA PHIFER: Thanks. Several different things. One is I think that the whole discussion of proactive monitoring that leads to enforcement, leveraging data that may come from the DAAR project, needs to turn into a recommendation around that. That's probably not Number 1 up here. And a possible action item within that would be to look at what the CCT already recommended and try to either build from the structure of that recommendation or any obstacles that have been encountered and actually getting buy-in for that recommendation. So that would be one thing to wrap that discussion up in an action item to produce a recommendation and to look into what's going on with CCT as well.

Separate from that, the recommendation that is up there, the Recommendation 1 regarding every new policy, or if we're going to change that to every WHOIS policy, needs to have metrics [that are]

monitored, tracked, reported, and enforced upon. I'm wondering if it's worth looking at some of the policies that are part of this review's purview to see whether in fact that has happened. For example, privacy/proxy. Are there metrics? Are there requirements in the implementation phase to actually track and report on them?

So maybe doing that due diligence for all of the policies that we touch on, IDNs being another one, might be a useful way of testing out if you formulated a recommendation and then you tried to apply it to some policies, would it have an impact or would you want to refine your recommendation so that it could have more of an impact?

ALAN GREENBERG: On the first one, I think a lot of the data accuracy work that Lili did will feed into the requirement to use tools that recognize patterns and clusters of things. Because with the kinds of errors we're seeing on data accuracy, and accuracy is not the only issue, but on accuracy there's no way to fix it based on one-by-one. If there were some fraction of a percent of errors, then you fix them anecdotally. But when we're talking about in the tens of percentages, then we're looking at a problem that's systemic and another method has to be used.

Of course, we have the tools. With those kinds of samplings, we can also recognize are there patterns of registrars that tend to have more inaccuracies than others? There's not a lot of registrars. If you take out the registrars that are fake registrars that are used just for catching names that are dropped that are in the process of being deleted, there are only about 1,000 registrars. The curve of where the registrations are

is very, very sharp. A huge majority of them are in a small number of registrars, and those are probably not the ones that are problematic. If any of the big ones are problematic, then we have a problem but we should be able to address it. Therefore, you're looking at clusters of the smaller registrars. And we all know about bad actors anyway, so some of them we know where they're coming from.

So I think we can link these two together and make a strong case for why you simply cannot respond one-by-one but must be proactive and use all of the data that comes in from various sources to try to address it. So I think those could well work very well together.

Back to Susan.

SUSAN KAWAGUCHI: One other thing – I'm just looking at my notes – that we talked about was actually Compliance team again on the proactive enforcement because with GDPR we're going to lose the ability for reactive. I won't be able to report things anymore. I'm sure they'll be disappointed. What if we write some sort of recommendation if they accept a feed on phishing, whether that be APWG or whatever phishing database that can be relied upon. We could make it a generic with some standards recommendation, and that they check the records for accuracy.

Not that that's going to prevent more phishing necessarily. It might. But it also would give you the information on which registrars and if there's a pattern on registrant data that is used for bad acts. If it's in a phishing feed that the rest of the Internet is relying on to block, then you know that it's a bad action going on and this is a grand assumption but it

makes sense that after the GDPR, ICANN will have that data and could take steps to be proactively enforcing because the community can no longer provide reports because they won't have access to the data. Maybe we could extend this and broaden this to other types of feeds, reputational feeds.

STEPHANIE PERRIN: Not to sound like I'm trying to get free data from APWG or any other third parties that are getting access to data, but if they were properly accredited under a standards based accreditation system, would it be out of ICANN's remit, i.e., over the content line, to ask them to as part of that accreditation provide threat data? I honestly don't know the answer to that. Some of the threat data is content related.

ALAN GREENBERG: I don't know if we could demand it, but it would certainly be interesting if we would volunteer to take it. We may want to restrict it based on the content issue [and things like that].

Erika?

ERIKA MANN: Susan, you know this as well as I do that all Internet companies, and we discussed this before, they publish at least once a year so-called transparency reports. These transparency reports have actually included such kind of data. So it's not complicated, but they do publish it. So it's not upon request, but they do publish it. And they are more and more detailed. At the beginning because of different legal reasons, not so

easy to publish them because you have to look into the jurisdiction [where] you are headquartered. So there are certain limitations on what you are allowed to publish in detail.

For example, [if] they are from the FBI or INTERPOL, there are certain limitations which you do have. But you still can publish the numbers and you can still publish how many you accepted from them, how many you refused. So there are many things you can publish, and they're actually very good I find. When you read them, they're excellent. I never understood why we never did this because the indicators what actually is requested is actually quite interesting.

UNIDENTIFIED FEMALE: If I could respond to that, the problem from a cybercrime perspective is once a year is – I mean, I realize some of these sites go on forever, but if we had some sort of positive requirement that if they know they're after someone and it's an imminent threat to the Internet, that it would be part of their responsibility as part of having access that they share that data.

ERIKA MANN: [inaudible] a different case. All these companies have law enforcement portals, their portal which is a law enforcement portal inside the company. And law enforcement can send to them requests, and they have to be responded immediately. Yeah, absolutely right. This other one is more for the broader public. It's interesting for law enforcement as well, but you need such kind of immediate portal. And all of these

law enforcement which are sending these requests, they're authorized law enforcement agencies.

So it's like the police units in Germany. They identify three of the agencies which are the right portal because they're worried otherwise there might be hijackers which are hijacking the system and claim they are police and they are not in reality police. It goes so if an office in Germany, they have a request [inaudible] it goes to let's say the law enforcement portal is in Hamburg. It goes to Hamburg. Internally, they look at it and say it's a legitimate claim because they might have crazy cases too, law enforcement. Then it goes to the Facebook portal. Then you have people on the other side who understand what they are actually asking for, and they accept it or they don't accept it and say we need more information. This is not in accordance with the law, your request. We need more.

ALAN GREENBERG: I've got a queue. I think Susan was first. You wanted to speak.

SUSAN KAWAGUCHI: One thing Facebook did, and this isn't just a Facebook, that Facebook has set up also beyond that is Threat Exchange, and ICANN is a member of Threat Exchange. It's companies that have all agreed to share information. So ICANN is already getting that information if they want it on we're seeing this. These are the domain names used in this type of scam, or watch out for this criteria because this is what we're seeing. Then other companies fill in, this is how they tweaked it so this is where we think we're going. So a lot of strategy could be involved in that.

I don't know that – I think there would be pushback I think if we recommended taking these reputation lists that were beyond spam and phishing for ICANN Compliance to do something about from a WHOIS perspective. Because it's pretty well accepted that if you send in a spam claim or a phishing claim to a registrar, most of them, the good guys act on them. I don't know how far afield you could go into this.

Well, child porn or something, they're all going to act on that stuff too. But right there, why aren't they looking at every reported domain name with child porn for inaccuracy? I just think there's a lot of avenues that they could do it. It's going to cost a little money and it's going to cost some time, but you could also do that automatically.

ALAN GREENBERG: A couple of things. On the Threat Exchange, I suspect that goes to OCTO and not Compliance.

SUSAN KAWAGUCHI: Right.

ALAN GREENBERG: So we're talking about different part of the organization. It strikes me if we're going to make a recommendation like this, we are not going to go down into the weeds and say you should take phishing feeds. But I think we're going to have to phrase it in some moderately generalized ways, perhaps with examples but not necessarily mandated.

One of the things that struck me as we've been talking is – and I've mentioned that registrars have pushed back significantly if we tried to put reporting requirements on them – but registrars as you point out regularly take down sites for various reasons. Is it reasonable to suggest – because we can neither negotiate the RAA on our behalf nor can we require the GNSO to set policy – but is it reasonable to suggest that we should look at getting feeds, putting reporting requirements on registrars to report the kinds of actions that they're seeing? So at least we know what's going on in those worlds even if we can't control it.

UNIDENTIFIED FEMALE: If you're already getting Threat Exchange data from the threat guys, then wouldn't this just be burdening registrars with another reporting requirement when there's going to be a pretty heavy interlocking Venn diagram there of what this stuff comes from?

CATHRIN BAUER-BULST: Sorry. We just had legislation adopted, and there was an urgency. At least it's adopted. Just on all the information that's provided to ICANN, I think it's clear that there's ample information out there. The question is what happens with it inside the organization and whether we need to look at what Compliance can do with it and how Compliance can deal with it.

And maybe one constructive way forward would be to suggest that Compliance can take actions other than just to identify issues. It could have a service branch that says for those who are interested, we're providing a customized version of the DAAR feed with a readout on

whatever you registry or responsible for or you registrar. And then they could take a proactive approach on that basis if they wanted to. So it doesn't necessarily always have to come with a stick. We could try to also increase the carrot side of things.

But I don't think, at least from what I understood from our – and I'm totally not an expert on all of this – but from our discussions with the OCTO team, the question is not the lack of data. There's the cooperation with all the companies who are willingly sharing. There's the feed from all the reputable companies providing these feeds to commercial actors. All of that is available to ICANN. The question is just what happens to it once it hits that organization. So that's I think what we might want to focus on also with our recommendation.

UNIDENTIFIED FEMALE: So are you indicating that they could provide a health report? This registrar had very few complaints or acted upon any of the bad actors, and this one had percentage wise 25% of bad registrations go through there.

CATHRIN BAUER-BULST: I'm not asking and understand this domain name health indicator was not one of the most popular projects of recent times. I think just beyond what DAAR provides which could at some point be a public naming and shaming, there could be just a private channel of communication that doesn't necessarily rank one registrar publicly against another but that says for your information this is the information we've received or these warnings we've received in relation to your customers.

Then it could include information such as this places you in the X percentile of all registrars, and you're doing really well or you're not doing so well in comparison. But not to share this with anyone else necessarily. Just to have it as a service to the contracted parties in the spirit of increasing the overall health of the domain system.

UNIDENTIFIED MALE: I'm going to preface what I'm about to say by saying I come from an environment where we would bend over backwards to work through finding out the bad actors and deal with them [inaudible] as a ccTLD, so I'm not averse to it. But I can feel issues arising. What I'd like to ask is, what are we trying to achieve? What's the goal? Is this compliance with WHOIS accuracy or compliance with WHOIS – what is the goal to do with WHOIS? WHOIS is giving us information. What are we trying to achieve with what you've just talked about to do with WHOIS? Because a bad acting registrar has got nothing to do necessarily with WHOIS, has it? Or are we suggesting we're talking about inaccurate WHOIS data? Is that what we're talking about? Specifically?

ALAN GREENBERG: It does seem to be linked.

UNIDENTIFIED MALE: Right. So what we're saying is – and again I stress I'm fine with this – what we're saying is we could run algorithms, tests, whatever you want to say that say this particular registrar or these particular registrars are much higher in inaccurate WHOIS data than others, yes? Okay, cool.

Then what was the suggestion that we should do with that data? That we would use that to be more careful with them?

ALAN GREENBERG: If I send them 1,500 reports, they will act on those 1,500 reports. I see no reason why the 1,500 reports cannot be generated internally.

UNIDENTIFIED MALE: So the goal of what we're talking about using all of the threat stuff and all of that is to beef up our Compliance's ability to recognize patterns of bad acting – I always find that quite hard to deal with – patterns of bad acting and then to act on those. Is that right?

ALAN GREENBERG: Effectively. A registrar's business is not a very profitable business. If someone has to take half an hour to address each claim and we're feeding them quicker than they can handle, that's an incentive to either clean up the act or get out of the business or something.

UNIDENTIFIED MALE: And I'm fine with that too. That's great. And the premise for this is based on the rationale being that we don't think that there is enough work being done to identify bad actors. Is that right?

SUSAN KAWAGUCHI: We've been told by Compliance they're reactive and reactive only. So we want them to become proactive. We can talk to APWG and find this

out and I was at eBay and Facebook both, in my own reports I received for domain name enforcement I often was able to identify phishing domain names that were not identified by our phishing vendor.

So when I would send those over to the phishing vendor I did not assume that they would also check the WHOIS record for accuracy, and I would file each one by one. It just seems like we have a feed that the whole Internet really relies on for reputation that ICANN Compliance could take that and so in those cases where the registrar will not respond to a phishing because there are sometimes they don't agree that it's phishing when it's pretty blatant but if you had an inaccuracy report it would take 15 days or 30 to get it down but at least it would be in the system and come down.

Then you would have metrics for knowing that ICANN itself has validated and would have a hard time walking away from and saying we found a strong correlation of phishing because these were reported and inaccurate records.

UNIDENTIFIED MALE: Thank you. I understand that and I'm fine with that. The only thing I would say is just to bear in mind, and again I speak from experience, moving from a complaints based compliance environment to – it depends on how proactive you want to get and that's why clear recommendations are helpful – to a proactive is expensive and people wise quite heavily burdened. Not that I'm saying that's a reason not to do it. I'm just saying bear that in mind that there is significant cost

involved in doing that and there are budgetary constraints that need to be met. The principle that you've set out sounds fine to me.

ALAN GREENBERG: Yeah, they're already in that world. The accuracy checking work that was being done that Lili reported already shows they are taking 1,500 or 2,500 reports from the accuracy checking and filing one-by-one complaints or acting on them as if they're one-by-one complaints. They're already in that world. They're accepting them from one internal department.

UNIDENTIFIED MALE: What's the change then?

ALAN GREENBERG: The change is we're asking them to take the incentive to do the research instead of having another part of ICANN doing the research and handing it to them.

UNIDENTIFIED FEMALE: But in a GDPR new world, they cannot be reactive if an individual cannot report them because they don't have access to that information. If ICANN has access and does not display that information, they should be able to use the information for security I would think.

UNIDENTIFIED MALE: Right, so what you're saying….

ALAN GREENBERG: We're on a ten-minute notice before our closing parts of the session.

UNIDENTIFIED MALE: Okay, I'm sorry. I'll [inaudible] take this offline, but I'm fine with it. Thanks.

ALAN GREENBERG: Unless I'm reading my watch wrong. You're apparently having a private consultation there. Okay. We'll wait.

UNIDENTIFIED MALE: We'll walk out. That's okay.

ALAN GREENBERG: I wasn't trying to interrupt. I was just saying we have ten more minutes.

UNIDENTIFIED MALE: I was trying to use those [inaudible].

UNIDENTIFIED FEMALE: You want ten minutes [inaudible]?

ALAN GREENBERG: Have we beat it to death then and I've accidentally ended it?

UNIDENTIFIED FEMALE: Yep, you did.

ALAN GREENBERG: Any further comments? Last call. Clearly, this is an….

UNIDENTIFIED FEMALE: What's the last call on?

ALAN GREENBERG: Last call on comments before we end the session.

UNIDENTIFIED FEMALE: So we never got to Recommendation 2, did we?

ALAN GREENBERG: Require all domain name registrations adhere to WHOIS requirements in the – oh, okay. That one says by hell or high water, make the 2013 agreement apply even for registrations that are not being changed otherwise but are only being renewed. That again is not something that I think we can recommend because I believe neither the board can do it nor can we require the GNSO to do it. We could strongly suggest the board twist arms to get it negotiated in the next update. We can certainly make a recommendation that we strongly believe that has to be done and let the board try to figure out how to do it.

SUSAN KAWAGUCHI: Yeah. So what I can do with this is go back to some of the details on the negotiations of the 2013. Because I was told the intent at that time was that all registration would adhere to the 2013, and somehow it was negotiated to not be. So let me do a little digging. I'm sure there's something there that I can – maybe not. Negotiations are usually not public. But let's see where the change for the 2013 originated.

ALAN GREENBERG: There is another path. It has been suggested recently that the GNSO in general has great fear of initiating PDPs because they use huge amounts of resources. It has been suggested however that if one were to initiate a PDP on a very small subject, it may still take a lot of elapsed time to do because of the requirement for public comments, but it doesn't have to take a lot of resources and that maybe we should stop being afraid of initiating a PDP on a small subject. This is within the picket fence, and it is subject to PDP.

SUSAN KAWAGUCHI: Yes, I agree.

ALAN GREENBERG: So there are multiple paths. And the board could initiate a PDP on that specific subject. So I think it's fair game for a recommendation, and if it's happening anyway for other reasons, so be it. It's done. [Great].

SUSAN KAWAGUCHI: I'll do some research though to see if we can [inaudible].

ALAN GREENBERG: Thank you for bringing us back to that one. I think that's a nice short one that would attract strong support from everyone with the exception perhaps of the registrars involved but would put us on a much stronger position to say if accuracy matters especially in a GDPR world, then let's get everyone on the same ground.

Back to you, Lisa.

LISA PHIFER: I think it was related to this, although it's a long day. I believe that there was a suggestion yesterday that information that ARS may already have could tell you of the grandfathered records. How many were missing the registrant contact information, and that could give you the ample evidence to base the PDP on. What would be the impact of launching the PDP? That you'd fill this hole that grandfathered records are leaving.

ALAN GREENBERG: Okay, I'm sorry. You said who could tell us?

LISA PHIFER: The question yesterday was whether the Accuracy Reporting System might actually already have information to tell you how often those grandfathered records are missing the contact fields. That would tell you the severity of the problem.

UNIDENTIFIED FEMALE: I got a stat earlier today on just how many of those grandfathered records there are. There aren't that many. Can we not just do a scan and figure out how many are missing fields? It can't be that hard.

UNIDENTIFIED FEMALE: [inaudible]

UNIDENTIFIED FEMALE: Tons?

UNIDENTIFIED FEMALE: 40% of legacy.

UNIDENTIFIED FEMALE: 40% of legacy?

ALAN GREENBERG: And there's roughly 100 million .coms, 40% is a big number.

UNIDENTIFIED FEMALE: What we don't know is are they missing that data?

ALAN GREENBERG: Yeah. Lots of people have the zone file. Lots of people have access to this WHOIS information. It could be done.

UNIDENTIFIED MALE: Not everybody has the whole WHOIS database, but there are people around.

UNIDENTIFIED FEMALE: Yeah, with pretty much the full. But the other issue is like you just said, all the registration data should be on the same ground or a level playing field. What we don't want to have happen is this 40% get to play the system with the GDPR and not even list the name of a registrant.

ALAN GREENBERG: Let's investigate privately or publicly how we can get a metric on that.

UNIDENTIFIED FEMALE: One other point. On the Recommendation 1, it says measured – and I wrote this – measured, audited, tracked, but it doesn't say enforced. So we just want the Compliance to just go just look at this stuff.

ALAN GREENBERG: Why would we want to enforce?

UNIDENTIFIED MALE: [inaudible] this is great. [inaudible] lovely [inaudible].

ALAN GREENBERG: Last call on discussion on compliance for this session. Lots of cocktails. Then I turn it over to Alice. I never get it right. If I call Alice, it will be Jean-Baptiste.

UNIDENTIFIED MALE: [Poker game], Alan.

ALAN GREENBERG: Okay, Alice.

ALICE JANSEN: We're going to run through the Day 3 agenda real quick. Thank you. Similar to this morning, we'll have a debrief of Day 2. We will prepare the highlights of the discussions that happened today for the review team to [confirm].

Then we'll go to Cathrin for the law enforcement needs update. We'll have Stephanie deliver an update on the anything new progress and Alan with safeguarding registrant data.

Then we have one of our famous parking lot for items to be discussed. This will be the leadership will need to identify which topic will be given the parking lot during Day 2 debrief and Day 3 objectives.

Then tomorrow afternoon will be dedicated to discussing Subgroups 2 and 5 findings and potential recommendations, similar to what you've just done and another parking lot.

Then we'll close with a work plan review as well as a wrap up that will include a number of items, such as ICANN 62, next steps, action items, decisions reached, and so on.

So this is the program for tomorrow. Are there any edits you'd like to make at this stage?

ALAN GREENBERG: The only statement I make is we have a fair amount of time that is currently unallocated, and I certainly would like to hear from anyone who would like to use that time for specific topics, subjects, whatever or to go back on things that we've done that we think need more thrashing out.

Lisa?

LISA PHIFER: If someone else prefers to use the time for something else, I would cede. But if we do have time, I would like us to spend at least a brief amount of time on that framework for assessing effectiveness since all of the Subgroup 1 subgroups should at least be thinking about the framework and whether it applies to the recommendations that they looked at to determine the effectiveness of the implementation.

ALAN GREENBERG: Thank you. Weren't we going to have a small session on the overall report structure? Yes, that's part of the wrap people.

Alan, I do realize that we are going to regroup some of the data accuracy compliance subgroups areas of work, but we also had one of the meeting objectives that you identified as establish [the need] for

any [strategic] changes in the subgroup structure. So we may want to discuss that again as well tomorrow.

ALAN GREENBERG: We should pick that up in one of the parking lots, so to speak. Once we've done all of the individual recommendations, so once we're basically up until noon, we can have some flexibility there. Other than the clear overlaps we have with data accuracy and compliance and we've noted some minor ones other places, I don't see anything major. The anything new, if our direction changes from what the subgroup had recommended on our last meeting, that might cause something to be rearranged if in fact we have any major new projects that were unanticipated at this point. That may well require some adjustment.

I think we also have to look at specifically law enforcement and try to make sure that we cover it. It's not one of our trivial areas, and it's not one that we ever considered not doing. So I think we have to figure out how we're going to do it.

That's all I have. I think we're done. If we can stop the recording, I thank you all.

[END OF TRANSCRIPTION]