LONDON – Expert WG on gTLD Directory Services Final Report Discussion Session 2
Wednesday, June 25, 2014 – 08:00 to 10:00
ICANN – London, England

FADI CHEHADE: Is this better? Yeah, so this one is dead. All right, how much did this group pay you to wake up this early and be here? If you didn't get paid, you should find out why, but I know half of you there.

JEAN-FRANCOIS BARIL: You might want to check they know why they're here, Fadi.

FADI CHEHADE: Good morning to all of you. Honestly, I wasn't planning to be here. I have a meeting waiting for me elsewhere, but I had the real privilege to chat for a few minutes with Jean-Francois with coffee earlier this morning and I came to, first and foremost, and again and again, because I'll be doing this many times, but at least I will do it this morning again, to thank each member sitting at this table for the incredible, not just work you produced, but spirit with which you produced your work.

It's really amazing. The more I think about how you came together from very different schools of thoughts, different backgrounds and you produced something on the one issue I was told when I came at ICANN is intractable. “Don't even bother,” I was told by some people in the community because, “We'll never get there. We've been at it for ten years. Why do you think this group will advance us even an inch?”

Well, frankly, for someone who has not read in detail, but skimmed – I did skim the report – it is amazing. You didn't move us an inch. You moved us a mile. And thank you for that.

The spirit with which you did this, I just asked Denise, should be recorded. In other words, not just the report and the substance, but also how you did it is also a guide for us how to attack very complex things in the future.

I think, with humility, the rest of the community should take your work and understand the spirit that got it here, and hopefully –hopefully – with leadership, but also with conviction, we will take this work and turn it into something that the DNS will advance because of. Because this is a huge advancement of the DNS system on which everything else we're doing is builds. But yet, some of its foundations need to be fixed and you have made that step forward.

So I don't know how else to thank you, but I'll keep thanking you for the next few months. And as I just told one of you, unfortunately – so this is the bad news – when you create something this good, this important, you cannot just leave it and go away.

We need you to work within the community to ensure that this work is watered. You just put seeds in the ground. They need to be watered. They need to be maintained so that they can grow into something we can all benefit from.

So please do not – I know you're exhausted. I heard you met almost daily for months. Daily for months. Mind-boggling. I don't know of any other volunteer group that met daily for months. This is really

incredible. But please, with all of this, take a day off, but then come back. Okay, two days.

JEAN-FRANCOIS BARIL: Only one day, Fadi?

FADI CHEHADE: Okay, two days off. And then please come back. And believe that this is your opus and it needs work. It needs attention. But you need to give it up to the community. That is part of the game, as well. It is not yours.

The genius of this would be that you brought it to us and now you need to let us own it. But to do so, it takes effort, as well. And we will call on you. We will call on you as we move forward.

But you have my commitment and I know Chris's commitment and Steve's commitment on the Board to not let this thing not bear fruit. It has to bear fruit.

So thanks again, really, sincerely, to all of you. I think everyone in the community, as they get to know you and know what you did, and know the substance of what you did, will be equally thankful. Have a great day.

JEAN-FRANCOIS BARIL: Thank you very much, Fadi, for these nice words. It means a lot for us, for the recognition. It doesn't mean that what we've said is right, but at

least we've done our best to digest this very, very complex elements to make the proposal that we have today.

So, I think it's a very much stick in the ground for the community to look at what these difficult issues could be. And as we said on Monday during the public session, we spent already one hour, and then two hours of Q&A. I'm very, very pleased to see that, even today, for another two hours, we get still a lot of people attending and willing to help us to digest further on how we can make it appropriate.

Also, on behalf of EWG, I can say that we are very, very committed to let it go this way. We are not going to direct anything, but we are going to be at the disposal of anyone who wants to do something [inaudible] with this report to help, definitely, for the benefit of the overall community.

So that's our commitment. We cannot escape and we'll never escape. We have a big commitment on this one. This is a group of volunteer. We have done that on top of the work. And as you said, it's a daily type of task. So we are very, very – and our heart is very, very warm for us to make sure that this is useful for the community.

With that, I pass to our fantastic moderator, Chris, for turning the Q&A session into a success.

CHRIS DISSPAIN: Thanks, Jean-Francois. Okay, who was here on Monday, please? So, new people, which is kind of encouraging. You were here and you weren't here? Okay.

We're just kind of continuing on a discussion about the report, and I guess, it's up to you guys what you want to talk about. So does anybody have anything they want to say?

Does somebody want to look at a particular aspect of the report? Does somebody want to volunteer something for us to talk about? Do we still have questions and comments? This is supposed to be an open discussion session and we weren't planning on doing any presentations because we did those on Monday.

No one? Because we can all go and have coffee if you don't want to talk. If you all turned up just to see what we would say, we're not saying anything. J. Scott, thank you.

J.SCOTT EVANS: [inaudible] Adobe systems. And I'm also president-elect of the International Trademark Association.

My question is what are we getting that's better for us than we are now? I know that for privacy concerns, registrants are getting less public information that is available to anonymous requesters.

But what's the tradeoff would have a company like Adobe which is seeking to stop the unauthorized distribution of our software, trying to find the illegal participants. What's in it for me that would better for me that would be better for me than what I have today?

CHRIS DISSPAIN: Leaving beside the obvious questions, which is why there should be anything in it for you, but [inaudible] Susan, Michele? Michele, you go.

MICHELE NEYLON: For everybody in the room, if I vanish shortly, it's not because you've all offended me. It's because I've ended up triple booked.

CHRIS DISSPAIN: Thank you for that. Did you get that Scott? That's the answer to your question. Michele is triple booked.

MICHELE NEYLON: There's a couple of things we've come up with that we think might be a help to you. One of the issues that intellectual property owners, business owners, and law enforcement in the broad context have raised in the past is the scenario where somebody will go off and register domain names that use a famous mark.

So, for example, in the case of Adobe, if I was to go off and register Adobe CreativesSomethingSomething.whatever, at present, I could easily put in all of your corporate details with the exception of, say, the e-mail dress. In terms of passing ICANN's policies with respect to WHOIS, syntax, validation, verification, etc., etc., etc., you can verify and validate it until whatever. Under normal circumstances, that will pass right through because, obviously, it would be syntactically correct.

But you would be scratching your head going, “We didn't register that domain name. What the hell?”

We're a much smaller company than Adobe and we've had this happen to us. We've had scenarios where we get – how do I word them? Nasty-grams from lawyers demanding that we take down websites, and we're scratching our heads going, "We don't have that website." It turns out that somebody's actually used our contact details. So that aspect is one part of it.

Again, some of the stuff that we've put forward is purely optional, so that in the case of a large company like yourselves that probably has quite a large portfolio of domain names, plus you're dealing with issues around domain names being registered that are going to cause you problems at one level or another, you could, optionally – and please note this is optional – set it up in such a way that nobody else could use your physical address and things like that.

I think that is something that you don't currently have under the current system. I don't think there's any way to have that under the current system. I think that, for even quite a small business, that's actually quite a nice idea.

I'll hand it over to the others since that's more their area than mine.

FABRICO VARYA: You asked from an infringement enforcement perspective, so no need to cover a lot of stuff, because I think we've enumerated a lot of benefits for people.

I think the big-ticket item is access to accurate data. One of our slides that I had the pleasure of presenting was our little garbage can that said

they're full of garbage. Hopefully we don't have to say that going forward if this gets implemented. We won't have, in five or ten years, another slide that says, “I'm full of garbage.” And to get that accuracy, we've operated on the premise twofold.

One, that gating people's data raises the level or incentive to put in accurate data, and that building an accountability structure that has a first step of credentialing or authenticating users who access that data for certain purpose also drives higher incentives for accurate data. People don't need to hide or falsify their data because they don't need to worry about the drive-by, anyone can pick up your PPI.

So for you, as a brand owner and corporation, I think the two things to think about or to focus on – and I think it's a legitimate question because, as we've all worked on this group, we've worked on principles, right? A lot of what we've said are principles, recommendations. They don't then, for the majority of the 180 principles we've put out, we haven't then gone through and flushed out every single detail of what is an authentication system.

So I would focus on is the authentication a proper bargain for exchange for the accuracy we think we're going to get? Is the gating a proper bargain for exchange for that?

And I think that that's all going to come down to the implementation details, because if in authentication, everyone is going to be asked for a blood sample for possibly more accurate data, I'd argue maybe that's not a proper bargain for exchange.

So look at the principles, and then I think when the community digests this and goes through a policy development process, those are the things you should think about.

CHRIS DISSPAIN: Does anybody else want to say something?

SUSAN KAWAGUCHI: One thing I think will be really helpful to the community in general is identifying the proxy services. In the minimum public data set, there will be that proxy ID. You will have their number. And once you've found out their processes, then you will know what to do each time. We're relying on the PPSI Working Group to define all of that.

But simply knowing, yes, this is a proxy. This isn't some strange registrant registration that is not a proxy. So you don't have to do that judgment call.

And then, having clearly identified processes – and you would know where you have a right to ask for the reveal of the registrant information and where you would not – that would be at the proxy vendor services site. But still, not having to go through that analysis each time, and hopefully, the Proxy Working Group will also ensure that the proxy vendor responds, because in today's state, most of them do not, in my experience. So, I think that proxy ID is crucial going forward.

CHRIS DISSPAIN: Rod?

ROD RASMUSSEN: Just one other bit that's in there I think makes the job easier, or potentially easier, for both trademark purposes and abuse investigations and the like is the concept of – two concepts. One of Who Was and also of, to some extent, a reverse WHOIS search.

So you can, once you have been authenticated, etc., etc., to get into the information for the purpose of determining if there are additional domain names re also in that potential for infringing or what have you, or part of a botnet or whatever, then you've got that capability built into the system.

CHRIS DISSPAIN: Okay, next, Alex?

ALEX DEACON: Alex Deacon with the MPAA. I just want to continue this discussion about identify verification. I understand it's optional. I know how difficult it is to do true identity validation in the global context. But I also know that optional features often are not implemented, being someone who has written specs and both implemented specs.

I'm curious to get more understanding about the discussions you had and the thought process you had with regard to optional identify validation. For example, what's the incentive for a validator to actually verify and validate and authenticate the true identity of the user?

CHRIS DISSPAIN: Validation is not an option.

ALEX DEACON: I may be using the terms incorrectly. I apologize.

CHRIS DISSPAIN: Rod, [inaudible].

ROD RASMUSSEN: There are a lot of incentives. You have to take and put the whole thread through here, too. What is the incentive for the validator? I would assume that they're going to get some sort of compensation for providing a level of validation, as one way of doing it. Fabrico?

FABRICO VARYA: If I'm not incorrect, I think what he's going at is. We have three levels of validation – syntactic, operational and then identity, actual identify validation.

ROB RASMUSSEN: Yeah, I'm talking about identity validation. I thought that's what you were asking about.

FABRICO VARYA: What's the incentive to actually have people do that final one, that third one?

ALEX DEACON: Why would someone pay a validator to do that if it's optional?

ROD RASMUSSEN: For identity validation, the optional?

SUSAN KAWAGUCHI: I can answer.

ROD RASMUSSEN: Well, you want to go ahead instead, that's fine.

SUSAN KAWAGUCHI: No. No, I'm good.

ROD RASMUSSEN: And if you want to add more, feel free.

You have to take a look at the type of registrant that's involved here. So for a business or somebody who is doing commerce on the Internet, there's two strong incentives. One is that you would have an identity-validated contact. That information, the level of validation and the last time it was checked are published.

That is something a consumer could go take a look at or somebody who is doing reputation or etc. could go look at and say, "This e-commerce site has been identity validated in the WHOIS," or in the RDS system.

There's also this concept around protecting my personal or my business credentials from being misused, which was already brought up. So if I have identity validated, I can then say nobody else can use this address and phone number in their contact details. This is mine. I've been identity validated to that level, so that guy down the street who steals your credit card or wants to impersonate a business is blocked from being able to do that.

Those are two, actually quite different, but very strong incentives to do that.

ALEX DEACON: But if that individual who stole that identity goes to another validator that doesn't validate their identity, is there a way to prevent that? Is there something already there.

ALEX DEACON: Is there something already there?

ROD RASMUSSEN: Yes. The idea is there would be a mechanism in the system for you to be able to say this particular set of contact details has been identity validated and cannot be used without the authorization of that contact holder, whatever they're tied to.

Did you want to add something, Susan?

SUSAN KAWAGUCHI: No. Great job.

CHRIS DISSPAIN: Excellent. Does anybody else want to say anything? No? Okay.

Wendy, are you walking to the microphone or just standing in the corner?

WENDY SELTZER: I would love it if there were a printed copy of this that I could page through more quickly than scrolling through my documents on screen. But that aside.

CHRIS DISSPAIN: You provide your own trees.

WENDY SELTZER: So, among other things, I'm trying to understand all of the language and implications here. I find principle eight nearly impossible to read.

CHRIS DISSPAIN: Would somebody like to talk to principle eight? We'll go through it slowly, otherwise we'll all get lost. I don't have a copy in front of me, so…

WENDY SELTZER: "At least one purpose-based contact must be provided for every registered domain name which makes public the union of all mandatory data elements for all mandatory PBCs. This PBC must be syntactically accurate and operationally reachable to meet the needs of every codified permissible purpose."

CHRIS DISSPAIN: Yep, makes sense to me. We'll happily talk about that, and just to say that all of us acknowledge that, in order to put this together, there had to be acronyms created and strings of words created and so on, and the report does sit as a whole and does need to be read as a whole.

And, we acknowledge that that's incredibly hard work to do. And we acknowledge, just so that we're all clear because I said this on Monday, nothing is going to happen following this meeting to suddenly see all this stuff implemented. There's a huge amount of work to be done before we get any further. But Carlton, would you like to answer the question?

CARLTON SAMUELS: Okay. If you notice, the principle is that for every data element that is collected, there must be a purpose, and every purpose must be permissible. So you start at that level.

CHRIS DISSPAIN: Does that not make sense, Wendy? There has to be a purpose.

CARLTON SAMUELS: Every element that's collected. You don't collect an element without establishing a reason to collect it. Every data element must have a reasonable purpose in order to be collected. First principle. Second—

WENDY SELTZER: Permissible defined by the set of reasons that you've allocated—

CHRIS DISSPAIN: Permissible defined by whatever the policy ends up being.

WENDY SELTZER: But not as defined by an outside review or court determining that, for some users, those purposes are not permissible?

CHRIS DISSPAIN: If a court decides that a purpose is not permissible, then it's not permissible, but only in that country. Not anywhere else.

CARLTON SAMUELS: Presumably there's a policy perspective, or policy framework, that will decide what is permissible or not. This is going into the policy development process, but the standard floor level principle is you may not collect a data element unless it is purposeful.

CHRIS DISSPAIN: Wendy, can I ask you, perhaps, to come at if from the other way? What's wrong with saying that every piece of data that's collected has to have a purpose that's an approved purpose or a principle purpose? What's wrong with that?

In other words, what we're saying is you can't just decide to collect somebody's inside leg measurement because you feel like it. You've actually got to have a justified, acceptable purpose for collecting it. And that falls into a series of buckets. One of those buckets, for example, it would be legal contact.

WENDY SELTZER: If you'd actually let me respond, when reading this text, I could easily get the impression that if I were able to come up with a new use for some purpose, it would be permissible to have that.

For example, I have the height measurement for the criminal who was viewed leaving the scene of the disrupted ATM, and knowing his inseam measurement would help me determine if this registrant was the person who was stopped on the scene, it would be permissible to have that information. Therefore, should I be able to throw it in here?

CHRIS DISSPAIN: But it would only be permissible if the policy allowed that information to be collected in the first place. So there's a policy in place that says this is the information that needs to be collected. There's a bucket full of information.

CARLTON SAMUELS: Let's go to the second part.

CHRIS DISSPAIN: Hang on. It's really important that we go through it slowly so that everybody understands. So Susan, just deal with the first part.

WENDY SELTZER: My problem here is that the text of this principle makes it appear that if I can develop a new purpose for which I need information and for which everyone will agree that in some cases it is legitimate to have that information, and I can codify it, then it can be made mandatory to collect.

Now, if that is not the intent, the language could be clarified to make that apparent.

FABRICO VARYA: Wendy, it's not the intent that you can create anything because you are not the community. This is just a representation of what we, as representatives or a reflection of the community, thought as a sample our best effort of what purposes could be.

But I think what Chris is trying to tell you is that what ultimately becomes the purposes, permissible purposes, is going to be defined by the community. So I, or you, can't ever come up with the inseam or the

height because it won't pass muster with the community. It wouldn't pass a vote in this room.

And so the reality is, if it won't pass muster in this room, it won't pass muster in the ICANN community, and it sure as hell is not going to pass muster with governments in the countries, which is also going to be...

So it's going to be a complete feeding-in process that will determine ultimately what those purposes are, so you don't have to think or feel as though any one of us is going to come up with a purpose like the inseam or height because, no matter how hard I tried, it's not going to happen.

So I guess if you start from the premise that "I" can come up with a purpose, your starting point is wrong because you or I can't do it.

WENDY SELTZER: I am simply trying to say that don't think I'm being unreasonable in saying that's not apparent from the language of your report. And so I am asking, as a member of the community, for clarification of the language that you have printed and distributed to help others who are reading through this material to understand that the mandatory union of every codified, permissible purpose is rooted in purposes accepted by the community.

FABRICO VARYA: That's why, during our Monday session, I believe when Susan presented this section and had the slide on permissible purposes, she actually made the point at the beginning and the end of her five slides that this

was our best attempt at, but that we probably didn't get a holistic view and we probably didn't get it 100% right. We could only do what we could, and we're going to have to rely on the community to finish it off. So that was clarifying then and we're just going to reiterate that clarification now.

CHRIS DISSPAIN: So did you have the clarification?

WENDY SELTZER: I hear clarifications that are, could usefully be added to this text.

CHRIS DISSPAIN: First of all, let's be really clear. We're not adding anything to the text. The report is the report. But I thought we had established, had we not, that this is a report that is going to then end up, at some point, after a whole series of processes in a GNSO policy development process, and that's where you need to be doing the work on what the principles would be and all of that sort of stuff.

I acknowledge completely that you might not find a particular paragraph or a particular series of paragraphs clear. I get that. But that's the drafting style. As a lawyer, I know that I can read some lawyer stuff better than others, for example. But the key is to understand that all of this is going to go in to a discussion that you guys are going to be leading as the GNSO.

I've got Stephanie and then I've got Rod, and then come back to you, Wendy.

STEPHANIE PERRIN: I think Wendy's clarified. I just want to bring us back to her original point, which was that the wording of that particular principle is quite confusing, an opinion I share. I must say, I don't know why we can't fix it because I bet we're going to hear it often.

CHRIS DISSPAIN: It doesn't matter how many times we hear it. We have produced a report and we're happy to clarify, but we're not going to go back and rewrite the report. I've got Rod and then I've got Michele.

ROD RAMUSSEN: And to that last point is what I wanted to speak to. And everybody's concerned here that when we have a fundamental thing like this that a lot of people are saying is confusing, we've already started. I don't know if the FAQ has been put up yet. I think it has been online. We want to address exactly these issues and get clarification language. And if you still find it confusing, help us.

You're listening. I think we are agreeing on what we actually want to see happen here. I know we did on the working group. So if you can suggest some language that would clarify in your mind, submit that. We are still cogitating on this feedback so that we can make it clear going forward in this process what the intent of these various principles is.

SUSAN KAWAGUCHI: Thank you. It's very difficult to read one principle and pull it out. So read all of the principles. It's a lot.

But principle four also speaks to that. There's a process. We definitely saw that technology innovates constantly. There are new things that may come up that, believe it or not, we didn't think of. Even if I had, we'd all be in new businesses.

We tried to accommodate letting the community have some sort of process to define a new purpose and decide if it was permissible and add it to the data set. We don't want static. We don't want to be working in 1980 data elements. So read all of these principles together and then you will have a more comprehensive view.

CHRIS DISSPAIN: Do you want to come back and say something, carry on? Because I'm happy for this to go as long as you guys want. It's just that I'm not clear what – Michele, sorry.

MICHELE NEYLON: Thanks, Chris. It's cruel and usual punishment to forcing anybody to deal with this at 8:00 in the morning. Especially me. I don't do mornings particularly well, and yes, they all know that.

With respect to the levels of confusion around terminology and everything else, I tend to agree that we need to be able to clarify these things. I don't want a situation, Wendy, where we're arguing over the

definition of something that's because the way it's worded is awkward or unclear. I'm more than happy to end up debating things where it's substantive, but if it's just because we haven't explained it very well, then we need to be able to clarify it. If that means we need to add some kind of FAQ or something like that, so be it.

I think what could be a potential – the kind of issue that I think has come up here a couple of times, and maybe the way we're responding isn't helpful, and it's honestly not intentional. From my side, it's because it's early in the morning. I'm using that excuse and I'm sticking to it.

The report itself is done. We cannot change that because will have grabbed the reported, downloaded it and consider it to be definitive, and if you change it, how are they going to know that there's a new version of it out there? But adding extra materials to clarify all of this, if that's what needs to happen, then let's do it.

WENDY SELTZER: And further in the drafting clarity question, I haven't found definitions of lots of these terms in a way that would allow me to say, for example, permissible purpose is clearly limited by the risk analysis that has to be done against whether – even if the community has identified a permissible purpose, it might nonetheless be impermissible to collect a piece of data, for example, because the risk analysis layered on top of that has determined that the data should not be collected. The risk of its collection outweighs the value it might have for those permissible purposes.

It's, I guess, left to those of us who subsequently read and parse the report to pull together those diagrams to come to the ultimate limitation of what appears from the text to be a very categorical statement that anything permissible will be collected.

Please, go on to others and I'll come back later with further questions, I'm sure.

CHRIS DISSPAIN: Kathy, you're next.

KATHY KLEIMAN: I'm going to run the queue for a second on this side, Chris. And, Mike, are you still here? I have a question for Michele before he leaves, so [inaudible]

MICHELE NEYLON: Is this beat up Michele time? just as follow-up to...

CHRIS DISSPAIN: Who's going first? Mike?

MICHELE NEYLON: I'm staying for a few minutes, but then I've got to go.

CHRISS DISSPAIN: Mike, you go.

MIKE REED: I'll make this really quick, thank you. One of the things we heard yesterday in the GAC was about certain classes of TLDs that will require additional verification elements. I myself am working with a number of financial services, clients, also working with the sports community where you might have memberships.

Is any of those elements that might be collected by a registry somehow [encompassed], or are you only looking at the minimum baseline data?

CHRIS DISSPAIN: You mean like .bank and...

MIKE REED: .creditunion.

CHRIS DISSPAIN: The requirement of the TLD is that you must be a whatever in order to use the TLD.

MICHELE NEYLON: Yes, Chris, I can speak to that a bit. The way we looked at a lot of this is, if you needed to add extra contact data, extra data elements specifically for that kind of thing – I can imagine, financial institution collecting something. If it's a sports club kind thing, maybe it's some kind of membership number.

We also looked at concepts like, let's say, if somebody wanted to add their Twitter handle as a way of contacting them. Technically speaking, there should be no limitation. So, to answer you, it's a non-issue. Yeah, it can be done. Scott can probably speak to the more technical elements of that, but we did think about this.

CHRIS DISSPAIN: We could make it, if one agreed that one should have these...

MICHELE NEYLON: Well, obviously.

CHRIS DISSPAIN: Restricted use TLDs, it would make it easier because you could bolt things on to this particular system that you can't really do right now. Scott, do you want to...?

MIKE REED: Again, context to .name where there are additional elements that were added in DNS.

SCOTT HOLLENBECK: Indeed, it would be a very difficult task for us to enumerate all of the possible data elements that might possibly appear in all TLDs yet to be identified. So rather than trying to come up with an endless set of elements, we focused instead on what we thought the minimal set would look like with the recognition that both the provisioning protocol

(EPP) and the resolution protocol (RDAT) are extensible and elements can be added with community consensus.

UNIDENTIFIED MALE: Thank you.

KATHY KLEIMAN: And one of the things I wish is that we had a semi-circle here, too, to continue the discussion. Just on that, let me just issue the warning. It has nothing to do with the question. The warning of the slippery slope that fields we heard were optional in Singapore are now mandatory – legal contact, abuse contacts. Once some people start asking for it, you start requiring it of everybody, whether or not it's a fit. It's a slippery slope.

CHRIS DISSPAIN: I think it's really important that we try and dialogue on all of these points. I want to get through everything if we can point by point. I know it's annoying, but I think it's actually important. Have we made some stuff that was an optional contact purpose in Singapore now mandatory?

KATHY KLEIMAN: Yes.

CHRIS DISSPAIN: Hang on. After the feedback we got in Singapore, we went away and we worked on what we thought the mandatory ones should be?

UNIDENTIFIED MALE: Yes.

CHRIS DISSPAIN: Right. Okay, cool. Susan?

SUSAN KAWAGUCHI: I think it's how you view it, too. And obviously, Kathy...

KATHY KLEIMAN: I'm a lawyer. I know how few people have legal contacts.

SUSAN KAWAGUCHI: Right. And this is personal, but the way I view it is I find it helpful that I can say this is the legal contact, or this is the abuse contact, for Facebook. I understand that is not for every registrant. But I think it does provide you some flexibility.

But at the end of the day, if you don't want to do that, the registrant ID, which is how it is now, could be put in all of those fields. So is that a major shift? It could be viewed that way, but it could not be viewed that way.

CHRIS DISSPAIN: I agree with that, and I also acknowledge that – because we talked about this on Monday, I think. I also acknowledge that what you think is

an acceptable minimum number of points and ideas might be different. But all we've done is to make a series of recommendations. The fight, if you will, would be in the PDP to say whether or not you want this or that.

Now, we can disagree, and we'll go – what I'm saying is bouncing it backwards and forwards here may not necessarily achieve all that much. But that was a higher point.

KATHY KLEIMAN: Could I go on to the question I had for Michele, which was a different question? Okay, let me go on. Michele, I understand there was a really – and this is the mind-boggling tough question of the morning. Sorry about this.

MICHELE NEYLON: You're not sorry. Come on. Go for it.

KATHY KLEIMAN: In this room, I understand there was a really interesting meeting between the registrars and the Board having to do with the validation...

CHRIS DISSPAIN: You mean yesterday?

KATHY KLEIMAN: Yesterday. With the validation and verification process that's taking place now under the 2013 RAA.

MICHELE NEYLON: Okay. So you're referring to where we gave the data on the number of domain names that have been suspended so far under the 2013 RAA.

KATHY KLEIMAN: Right. This is a question almost as complicated as the report. Sorry about that.

MICHELE NEYLON: Just go for it.

KATHY KLEIMAN: I understand that there was a discussion about law enforcement requirements and that a request for data from law enforcement ragarding –so it's all hearsay.

MICHELE NEYLON: I can tell you what was said, if you want, so it's no longer hearsay, because I was sitting there.

KATHY KLEIMAN: I want to tie it in to this meeting. I would like to ask you to tie it into what we're asking for here. I understand the registrars asked for data

from law enforcement about whether all the effort for validation verification is really worth the end product in the difficulty in the millions of domain names being taken down, and that there was a suggestion that before law enforcement ask for more, they have to show that what they've already asked for is working and necessary and producing the benefit, and the cost-benefit analysis is working.

Can you tie that in to what law enforcement has asked for from the EWG, what law enforcement has asked to be included in this report and tie it in?

MICHELE NEYLON: When you say you're going to ask me an awkward question and it's going to be potentially the awkward question of the morning, you really weren't exaggerating, were you?

KATHY KLEIMAN: Sorry, no.

MICHELE NEYLON: You're not sorry. It's okay. It's okay.

I'm going to kind of throw this back at you in reverse. The conversations that the EWG had with law enforcement were not specific to the EWG in that nothing – and somebody else can correct me if I'm wrong – but as far as I'm concerned, nothing that we discussed with them was new or novel.

It was more a case of an ongoing dialogue, a continuation of dialogue, that law enforcement had been having with contracted parties and with the broader community via the GAC and not via the GAC, with registrars, with registries, etc., etc., over the last few years. The difference is that it was dialogue as opposed to them kind of yelling at us, which was kind of nice.

There is a thing that came up previously in other meetings, and it came up yesterday. Is it worth the effort? Is there an actual benefit? Is forcing some level of validation going to actually lead to a reduction in whatever, be that fraud, be that identity theft, be that phishing, malware? Choose whichever form of DNS abuse you're most passionate about.

And I don't think that having that conversation is incompatible with what we've been doing because we weren't asked to come up with something that met this big long laundry list of things that the community and others have asked for with respect to WHOIS over the last X number of years.

This is just me, personally. If somewhere along the line somebody said, “Okay, there is absolutely zero benefit,” and what is being asked is ridiculous and is totally pointless and doesn't bear any relationship to anything, and you as the community decided that you were happy with not doing any of it, well then fine. Grand.

But that's not what we've been hearing. I don't know – the balance thing here, just speaking personally, I don't know how to get that right, because if you say to me, “Michele, hand on heart, do you believe that

validating an e-mail address or verifying an address is going to solve online crime?" Personally, no, I don't think it is because if I was going to go out and commit a crime, I would probably validate and verify.

Now the thing I have said repeatedly – again speaking personally, not speaking on behalf of anybody or anything – is that I am personally sick to death of everybody piling everything in on top of WHOIS and they're going to be using it as a proxy to solve the world's problems. You swear to God that going down the street and walking around London is somehow safer because of some rubbish WHOIS, whereas I could just as easily get hit on the head with a glass or something in the bar. I don't know. It's like this massive kind of dichotomy between online and offline.

UNIDENTIFIED MALE: Michele, you should turn the mic off.

MICHELE NEYLON: I could turn the mic off, but look, there are two parallel things. We were asked to deal with a big long list of things, which we did. And is it going to solve the world's problems with respect to crime and all that? I don't know. And I wish that law enforcement and the GAC would actually come to us with something tangible and with something saying, "Yes, this did solve something. This did prevent something." That would be fantastic. That would be great. Is it likely to happen? I doubt it.

KATHY KLEIMAN: Thank you for the tie-in across types of media.

CHRIS DISSPAIN: Yeah, absolutely. And I think Fab wanted to say something.

FABRICO VAYRA: Kathy, I wanted to come back to this, because I think it's really important. I just had a "aha moment." I think this second cup is kicking in.

Twice now you've asked – you've made the statement that we've made, from one meeting to the other, we've made optional mandatory.

KATHY KLEIMAN: Yes, I can show you [inaudible].

FABRICO VAYRA: It's in the report. It's in a chart, right. I was thinking back on how that happened and why it is every time you ask that I make this confused face. I do that often alone, but in response to your question, I do it too.

I think the reason is – I find myself, I'm in this argument or discussion I have with my U.K. friends, is it a banana or is it a banana. It's a semantic question, really.

All we were trying to do it, in the chart, change it to mandatory meaning that that field needs to have data in it. But I think what you're implying,

or you're interpreting, is that it requires additional data, meaning you must have an attorney, you must identify somebody new.

It's not at all. It's just saying that something needs to populate that field or be designated to that field. Just like when I order a pair of shoes or something or a tie online, I type in my credit card information and then I get to a field that is mandatory that says your billing address.

Now, I can put something new in it, or I can click the box that says, "Same as billing." It doesn't mean it requires additional information or I'm required to get an attorney or that I'm required to do anything other than so that when someone comes in – and the other question [Milton asked] is, "What's in it for the user?"

What's in it for the user is now there is not this empty field where somebody is writing you personally for a legal matter when you don't want to be contacted, or that they are writing you when you want to be contacted in relation to whatever data you've decided to add to or not add to.

It's just like the company knows where to ship the information. Do they ship it to my billing address or do they ship it to my mom's house?

CHRIS DISSPAIN: Kathy, I agree. I have some sympathy with your point. If I want to provide a legal contact, I can do so. I agree with that. But look at it from the other way around for a second, because I think this is a benefit to registrants, as well. If we have a legal inquiry – let's assume for a particular type of acceptable legal purpose, we have a legal purpose

inquiry. If we don't make the filling in of the legal box mandatory, then what information will we give the legal purpose query?

We'd have to go to another box to give them the information. I would rather give you the option of giving me someone else's details in that box rather than your own details as the registrant, and the option of giving me the registrant details in the box if that's what you wanted to do.

I'm not suggesting that my argument is better than yours. I'm just suggesting that there are different sides to it that work for both registrant and inquirer.

KATHY KLEIMAN: I hate to do this. I'm going to plead ignorance right now because I left all my notes about the database field back at my chair and came up to talk about something else, so I will be back to talk about database fields when I have my notes and when I have my hat on as a large-scale database programmer. We're going to talk a little bit more about this. I know Chuck wants to talk about permissible purposes, or something like that.

CHRIS DISSPAIN: And, by the way, Michele, it's banana. It's not banana. It's banana. You say banana; I say banana.

FABRICO VARYA: You probably need some coffee, too, because this is Fabrico, not Michele.

CHRIS DISSPAIN: I apologize, Michele

ROB RASMUSSEN: I confuse the two all the time, as well. And just to put – what Chris was just talking about, and my interpretation, as well and how we view it in the group, I think what we've done to a certain extent with these new, in theory, contacts is just inflict reality in that you are going to – if you register a domain name, there is definitely a chance that somebody is going to want to reach out to you on a legal basis. What we've done here is said, "Okay, that's going to happen." And they're going to reach out to you for abuse issues and whatever other issues.

CHRIS DISSPAIN: It seems Chuck is going to be usurped again because Kathy wants to say something. It's okay. This is what this is supposed to be about.

ROB RASMUSSEN: What we're doing, that purpose has been filled by the registrant this entire time in the current system. That's the way it is. What we've done is expose that.

I think what's happening is we're having a visceral reaction to [inaudible] and we had some of this in our own group. "Whoa, that's new and different." But it really isn't. We're exposing. We're saying the emperor has no clothes and this is what's going on. We're exposing

reality to how things are done and how people need to be able to contact.

KATHY KLEIMAN: I pleaded with you in Singapore and I spent hours with Denise asking if you were going to sit, in addition to holding many meetings with law enforcement and with people who act as private law enforcement, whether you were going to meet with free speech attorneys, freedom of expression attorneys and registrant defense attorneys to find out how this data is abused, how every field that has a positive use has a negative use, and how new fields you were thinking about might have negative uses.

I've checked with everybody I mentioned as a name, as an expert who deals with this data and deals with the abuse of registrants every day through WHOIS. Nobody was contacted. So let me ask you, did you sit down with any panel of registrant defense attorneys or free speech attorneys who deal with this stuff every day, who deal with the abuse of registrants of the WHOIS every day to find out what the implications – what the risks might be – of what's being proposed? Sorry, Chuck.

CHRIS DISSPAIN: Fab, you look as if you're reaching for the microphone.

FABRICO VARYA: I think I'm giving that confused face again. I guess if my point was to clarify that we're not asking for anything additional. Actually, in fact,

what we're doing is giving the user the option to not have to add additional information where they don't think it's necessary – i.e. when I order a shoe or a tie from online, because a shipping address is mandatory, it doesn't mean I have to come up with a new address to add in that field. How is that raising or triggering any different privacy laws or harm or anything?

Meaning, if Scott registers a domain – and let's diffuse this. There's also admin and there's tech. Let's stick to tech because that's a non-inflammatory subject, right? Let's stick to tech. No one has problems with technology and tech contacts.

When Scott registers a domain name, when it gets to the subject of mandatory collecting a tech contact, he's going to check "same as billing" because he's capable of answering his own technology questions. Me, the dumb attorney, when he gets to the registration and it has the field – one of many, along with legal and tech – abuse, I'm going to not check same as billing on tech because you'd be in the wrong box or calling the person if you want me to solve a technology question.

Instead, I'm going to say, check, Chuck is my tech person. Or my neighbor is my tech person. Or whoever. It's made to be easier. But if at the end of the day, I have no one and I don't care, you can call me and I don't care, I'll just say "same as billing." It's an option, but it doesn't require you to add additional information. And because of that, I don't see how it triggers anything different in abuse.

KATHY KLEIMAN: Because my mother said whenever you sign something, you're responsible for it. Whenever you check something, you're responsible for it. Legal contact means something. Abuse contact means something. And millions of registrants don't have that.

FABRICIO VARAY: I'm glad you're pointing this, because this is to Wendy's question the other day about a new obligation of accountability. I think we clarified when Wendy spoke that the registrant is already under the obligation to put in valid address and information.

I think the registrant agreement, when you sign it, also has a lot of verbiage around what you're legally responsible for, i.e. what you're on the hook for.

We heard Stephanie loud and clear on this. She was a great advocate for you guys. When you ask who did you talk to, we heard plenty from her on all of these subjects – every one of your questions from Monday to today, every point, we've spoken about this.

What we tried to do here by making a purpose-base driven model for which every time someone registers a domain, at the outset as they're registering it, they're highlighting all the different purposes was another educational piece and another option to actually highlight. Raise up to the level of lowest common denominator to let people know that someone may contact you for a legal purpose. That is an obligation.

That already, in the current ecosystem, with or without this, is an obligation that everybody signs to – your mom and my mom included.

And the reality is – and we heard loud and clear – people don't know that that's the case or they're not reading it or they're not understanding it.

Now you're going to have an agreement and you're going to get to a point where, if you didn't already realize what you signed for when you were paying, you're going to now be highlighted. And oh, by the way, someone may contact you because of what you just signed, there are obligations for tech, abuse, legal.

Again, what we are trying to do is actually make it easier for the consumer to, one, understand what they just signed on to; and two, the availability to actually assign other people, or themselves, but under full understanding of what it is they just signed. It's not to hide the ball. It doesn't create a new requirement.

KATHY KLEIMAN: [inaudible] optional [inaudible].

CHRIS DISSPAIN: Hold on, hold on.

FABRICIO VAYRA: And again, it's mandatory that something be there.

CHRIS DISSPAIN: Whoa. Hold it. Stop. Stop. I know Stephanie wants to say something. I actually think we need to carry on this discussion because I think it's

really important, and Chuck is standing there, so we have a choice. Can we break for a little while, take a little bit of heat out of it, ask Chuck's question and come back to it. Is that okay with you, Kathy?

KATHY KLEIMAN: I think Stephanie wanted to—

CHRIS DISSPAIN: I'd rather break it now and then we'll come back to it and Stephanie will be the first person to talk.

Chuck?

CHUCK GOMES: A few questions, first of all. Who is the chair of this PDP working group that's going on and was this approved – this PDP working group…

CHRIS DISSPAIN: What PDP working group?

CHUCK GOMES: Just stay with me, please? Be patient. You've been really patient so far. Did the GNSO approve this PDP working group that's going on right now? What I'm saying is we're getting way ahead of ourselves. What we are doing right now is what the GNSO PDPs, probably plural, will have to work with.

There seems to be an assumption that what you guys put on paper is a done deal. It's not. The Registry Stakeholder Group, at the very beginning when this process was announced, had one problem. We wanted to make sure that this group was not developing policy.

Now, what we've seen this morning, and probably will see more of, is illustrating the challenges that are in front of us. You guys have laid some things down. Are they perfect? I don't think any of us believes that. You don't either. Are there possible errors? Probably. Can things be worded better? I'm sure.

And we're going to have to grapple with all of that when we start getting into the policy development process. We're not going to resolve it today. I'm glad you can defend your case. I'm glad Kathy can defend hers. That's what we're going to have to do. And then we're going to have to try and come up with decisions, recommendations, for policy that most of us can support. Will all of us support it? Not going to happen in this area. It's going to be the same.

But we've got a place to start, and I think we need to get that into perspective. This isn't the place to iron all of that out. We could go on for weeks. Unfortunately, the PDPs will have to do that. But let's keep the right perspective here.

We could go on and try and improve the report indefinitely and fix all the – it will never end. We're going to have to do that due diligence when we do the policy development, and we're going to reject some things, we're going to accept some things, we're going to change some

things, according to how we come together in some sort of at least rough consensus in terms of what we're going to do. Thanks.

CHRIS DISSPAIN: Thanks, Chuck. Matt, did you have a – no? Stephanie, did you want to say something?

STEPHANIE PERRIN: I totally support the previous statement, just in passing, and Chuck was very patient waiting for the mic.

I just actually wanted to speak another language for a moment, and it isn't French. In this discussion of the paradigm shift, if you wanted to speak social construction of technology, it's to the heart of this argument about whether the words need to be correct in the charts and in the rest of the document. And as you might know by now, I believe we do need to clear up some confusion.

If I may use an analogy, as Fab does in his filling out the form to get the shoes, a chum of mine who lives in Washington told me years ago that they actually put the lines at the stop signs so far back from the intersection that, in order to safely execute the intersection, you have to creep past the line. Therefore, you're violating a law and you can be stopped at any time. That is what in the sociology social construction of technology we call an instantiation of power.

And what I see in the paradigm shift that we are working on right now, we have a system that, yes, says you should have workable contacts but

according to all the evidence – and not being an ICANNer for life like so many here, I only am relying on the evidence we've seen.

It doesn't work. So when something actually doesn't work for so many years that it's full of garbage and people get away with registering as Mickey Mouse, then that is an instantiation of power that is relatively weaker.

Now you bring in a system where you validate, then you do have to be very precise and careful about how you're calibrating that balance.

Now, yes, that has to be done in the PDP, and you can blame Kathy for getting me into this business and Michele for talking me into joining the Privacy Proxy Working Group. That experience has caused me to believe that we need some precision in what we throw into these working groups before they start fighting it out for the next few years.

And I would quote Mikey O'Connor, who came to the mic – was it in Buenos Aires or Beijing? – and said, "Whatever you do, give us more detail before you give this to the working groups or nobody is going to sign up for them." I think that's a fear. I agree with what Chuck Gomes was saying, but where do you find the balance that you are not precipitating into the working groups what I would call a new instantiation of power, and that's what I'm concerned about.

WENDY SELTZER: Thank you. Wendy Seltzer with a question in the spirit of Chuck's. To give information to the working groups that will be processing this, could we get an answer to Kathy's question about which privacy groups

and advocates on behalf of registrants you discussed with, you met with or heard from in preparing this material?

SUSAN KAWAGUCHI: We relied on team members. We have several team members –Carlton, Michael, Stephanie – that have that expertise. We relied on our own expertise. We relied on comments.

And because of a death of the family, did not attend two of our meetings, so London and D.C. I can't speak to that, but I only remember meeting with law enforcement for like 45 minutes once. So there has not been an over-emphasis on working with law enforcement.

Now, you could go back and see everyone that's commented. Everyone had the opportunity to provide comments to us and you've all done a great job of that, but I do not see that these scales were tipped one direction or the other.

CHRIS DISSPAIN: I think that's right. I just want to address what may be an implication that some of the changes that have been made, specifically to what Kathy was talking about, where made because of discussions with law enforcement.

In fact, my very strong recollection is the only discussions we had with law enforcement was basically about how to validate law enforcement. In other words, how do we find a way of making sure that a law enforcement query is actually from a legitimate law enforcement

agency? We had no discussion with law enforcement about the purpose-based contacts or anything.

JEAN-FRANCOIS BARIL: I think, Wendy, you are bringing a topic that many, many people are bringing this to our table. Number one, we have accepted all, 100%, of the comments, all of the [inaudible], all of the requests for meetings, we have accepted. Full stop. That's number one.

Number two, don't be confused about quantity and quality. And yes, we have Stephanie, we have Carlton, we have Michael, but above all – above all – privacy is for every one of us to incorporate. And if we don't take privacy seriously, we're not doing our job correctly. Full stop.

And I don't any more this is coming to us as a question – okay, it's only Stephanie. It's not only Stephanie. It's me. It's Carlton. It's Susan. It is everyone around this table been very conscious that, without the respect for privacy, we don't do our job.

Now, yes, we have had fantastic speaker for privacy. Michael, Carlton and Stephanie, as specialists, as the people who understand far beyond what I can understand. But our mission for all of us is to incorporate privacy.

If we don't have one dimension, one fundamental dimension in our equation that we have to solve not correct and not incorporate that, we have not done our job.

CHRIS DISSPAIN: I wanted to come back Wendy first and then back to you.

UNIDENTIFIED FEMALE: Lanre would like to talk.

CHRIS DISSPAIN: Oh, I'm sorry. Lanre?

LANRE AJAYI: If I may add, I think we spend more time on issue of privacy than any other aspect of the program. If you look at the major concepts, new concepts, new ideas, they came in the area of privacy.

For example, [inaudible] access is about privacy. Secured, protected stuff is about privacy. So most of the new introductions into the system is about privacy. I don't think privacy has been less discussed than other aspects of the system.

WENDY SELTZER: Thank you. I wasn't meaning to make any implications about the privacy expertise of anyone on the panel. I was merely asking the question "Whom did you consult with?" and I've gotten the answer. Thank you.

JEAN-FRANCOIS BARIL: Yeah, but the thing is, this is coming all the time. And you have to be convinced that we have done privacy big, big priority in terms of time, in terms of discussion, in terms of intensity. This has been very much put

on the table in a very vivid discussion and intellectual honesty. Very, very strong.

CHRIS DISSPAIN: Stephanie, and then I think we'll go to the next person in the queue.

STEPHANIE PERRIN: I think, as my colleagues might have politely said, I was a vocal pain in the neck on privacy at every meeting. That doesn't necessarily mean I was effective. I would just like to say for the record that I'm not an attorney. I'm not a data protection litigator. And Kathy's question actually was about the bar that defends people in domain. Somebody can phrase this better, probably Wendy, but not specifically about privacy.

So in that particular case, we had two [inaudible] out there. Nobody came forward to give comments from those particular areas. So I think it is an issue. Just want to clarify that.

UNIDENTIFIED FEMALE: I have a [WHOIS] question. Who is law enforcement?

CHRIS DISSPAIN: That is an extremely good question.

UNIDENTIFIED FEMALE: I live in Woodstock, New York, land of peace and freedom and there's a big peace sign in the center of town. When I first moved there 35 years ago, there were two policemen full time, and one part-time policeman. We now have 18 policemen full time and seven part-time policemen.

CHRIS DISSPAIN: That's not just because you moved there, presumably?

UNIDENTIFIED FEMALE: Well, it may be partly. I don't know. But in addition to those policemen, there are seven groups which are armed and come under the banner of law enforcement. There is the Ulster County Sheriff's Department. There is the New York State Police. There's the FBI. There is the Department of Homeland Security. There is the Department of Environment Protection. And more recently, the U.S. military has been cleared to actually take part in law enforcement in the United States.

Can any one of those people get information about me?

CHRIS DISSPAIN: You can understand how, as an English person living in Australia, most of that is a complete mystery to me. It's a policeman. But the answer is this is one of the most difficult problems with the current system. If you allow law enforcement a greater level of access, then you have to say, "What is law enforcement?" It's currently a problem that's being dealt with the 2013 RAA.

Who wants to address the law enforcement issue? Rod? Go ahead.

ROD RASMUSSEN: We asked that question to law enforcement personnel ourselves. And there's even more authorities, just talking the U.S., the IRS, the FTC. There's a whole bunch of people with enforcement powers or investigatory powers, and depending on the jurisdiction you're in, can obtain information about you within the current law of whatever that jurisdiction is.

And actually, that's about as close to a definition of law enforcement as you can get, in a way. If they have some sort of power within the regime or local jurisdiction you are, then they have some sort of access rights under some sort of process –typically due process, hopefully – to be able to get information about you.

If you take that as a baseline, then you can actually start thinking about how you would apply that. That's one of the reasons, as we were going through this, we were struggling with that same issue. How do we provide access credential to law enforcement, and then somebody mentioned the dog catcher is a law enforcement officer. You can get a ticket for you dog poop on somebody's lawn. Did you have that happen lately?

One of the ways that we moved this process forward was to say, “Let's take a look at the way this happens in the real world.” If you take a look at how we've looked at the validation and accreditation around validation, we've said let's utilize processes that are already in existence for de-conflicting and pushing forward requests for information. This has been an international border thing because this is where the real concern is.

Interpol has already stepped up to say, “We're interested” in providing a way forward to utilize the system they use for authenticating requests and the validity of those requests –because this gets back to a question that came up on the last session. How do I make sure that the law enforcement request, which could be legitimate within the country it is in, “I want to know who wrote this defamatory thing about the great leader.” They're in a different country.

Interpol already has a way of de-conflicting those and saying, “You can't find out about that. You can't use the system to do that. However, we will help you to find the pedophile who has been creating child abuse materials and posting them online.”

So there is a real-world system for doing a lot of what we're talking about already. That is a starting point. There are still questions around tax authorities and things like that as how they would actually utilize the system. However, what we've done is create a framework so that this community accredit those under rules that they would be able to get access to that information.

And that policy, the way we framed it within the document is there would be a panel or some sort put together to say, “You need to meet these criteria. And by the way, when you are accessing this information, this is what you're entitled to. You have to declare that as your purpose.” And that when that access is occurring, there is a chance to have that audited and make sure that abuse of that system isn't happening so that the dog catcher is not going in and pulling down the information of everybody who lives everywhere in the town, for example. That's how we've tried to address it within the document.

CHRIS DISSPAIN: And there is still a huge amount of work to be done. But it is based on a couple of principles which, if you don't agree with, then it doesn't really matter what the rest is about because one does not fundamentally agree with the principles.

There's a principle, effectively, that you've got to provide information in order to get a domain name. And secondly, then, there is a principle that law enforcement has a right to access that information, having defined what law enforcement is and being very clear, etc. So if you don't agree with those...

UNIDENTIFIED FEMALE: Wouldn't law enforcement – I mean, wouldn't they have to go to court to get that? It seems like any cop can...

CHRIS DISSPAIN: That's what we're saying. We're saying there needs to be a validation system and then there needs to be a permissible purpose. Rod?

ROD RASMUSSEN: And to clarify that, too, it depends on the kind of case and the kind of work that they're doing. You have particular incidents where you would have a court order, and it could be a sealed court order. This happens today where domains are under investigation because they're being used as the back end of a botnet and things like that.

Sealed orders come in and it's a court order and then the registries have to respond to that and provide information. Happens today.

There's also the more general kind of investigatory type thing where you're seeing some sort of crime occurring and you're trying, "Okay, who or what might be responsible?" That's a different level of information you might be able to get for that thing.

It's not just "you're law enforcement. You get to look at everything." I think that's very important to understand that that's not what we're talking about here. It would be more finely grained then that. If you're doing a preliminary investigation, you would get a lighter weight set of data. If you have a specific thing, with a court order, you can go in and get far more details about what's going on. And I think that reflects, trying to reflect how we do things in the offline world and trying make that show up there.

CHRIS DISSPAIN: It also happens in the online world in a number of ccTLDs. That is what happens and Australia being one, where we don't allow. We publish a very limited set of data in the Australian, .au, WHOIS.

We do not allow law enforcement to have unfettered access to the database, to what's behind the gate. They have to come to us with – we have a series of agreed protocols.

Admittedly, it's easy for us because we know who they are. We know who Australian law enforcement is. That's the real challenge when you go global. But it does happen locally, nationally, in a lot of ccTLDs that a

lot of things that we're talking about are already effectively exist. It's just a question of figuring out where is your bottom-line standard that you're going to adhere to and then how do you validate – accredit, if you like – and authenticate law enforcement globally.

Stephanie, you had your hand up, and then we'll move on.

STEPHANIE PERRIN: Yes. And I think you're question speaks to something that we did discuss in the group. We have said that accredited users of the corral, as I'm calling it, they get the data for particular purposes, and then they're not allowed to dump it into a giant database.

Now, the enforcement of that mechanism is already difficult in the world that we have right now. A number of Western countries, for many years, have been bringing in what they call joined up justice systems where, indeed, if I have a complaint about my dog barking, somehow that's going to show up on my passport information when I try to get into the United States. Things like that are happening.

Policing – what happens in police information system is a true challenge. Fortunately, not one that ICANN is responsible for. But we do need to figure out how to police that precision that we put on the release of the data. Otherwise, it's nonsense. Why build an expensive system if we can't police it?

CHRIS DISSPAIN: Absolutely. And I think as we all talked about and we all agreed, it's never going to be perfect, but at least we need to build in the checks and balances to ensure that we can spot patterns and see what's happening. When I say we, obviously it won't be us. Is that? Thank you.

David?

[DAVID GOLDSTEIN]: Just a brief note. I understand there are a lot of checks and balances built into things like the Interpol system between jurisdictions, but it's also my understanding that there have been accusations that their system doesn't work. One of the high-profile ones was the 2012 case of Hamza Kashgari. His alleged the Interpol system was used to prosecute for blasphemy, which, of course, should not be used under the system.

I just want to say it's important we have other checks and balances for people who are cautious, who are not fully confident in those system. And in particular, in the extremes, it is very important that...

I think it's a wonderful feature of this new system that it allows for the genuinely secure credentials that Stephanie talked about in the presentation on Monday. I applaud the committee for allowing for that possibility.

CHRIS DISSPAIN: Thank you, David. Kathy, do we want to revisit? Fred, are you heading to use the microphone? Sorry, yes, Susan, go ahead.

SUSAN KAWAGUCHI: No, no, no, this is totally different. Thank you. I never remember to turn on my mic.

This goes back to several questions of who did we talk to, and I'm getting the sense that maybe we need to tell the story a little bit more about how we went about our work.

Yes, there were two Board members, Chris and Steve, on the team. But staff supported us. Staff was not part of the team. We discussed issues and we came to hurdles and we said we need more information. And as a team, we said, "Who do we need to talk to?"

A lot of that, as I remember, is we wanted to talk to ccTLDs and how did Nominet do this? What's going on in the real world today? As a team, we decided together, these are the hard items we're having to deal with and maybe this is a resource. Staff, could you please provide that as a resource?

I do not remember any time that staff said to us, "You will talk to these people." Staff came to us and said, "These are people who want to talk to you. Do you want to talk to them?"

All the research and the discussion, any of the work we did was driven by the team. So it is a team consensus on this report. There is a dissent, and that's fine. But we made those decisions as we went through our work and then we asked for help.

So maybe someone should have come to the team and said, “Please, please, please, go talk to this person.” And then, as the team, we would have decided.

CHRIS DISSPAIN: Which, to be fair to Kathy, is what I think she said she did in Singapore, but nonetheless. Kathy, Carlton wants to say something and then we'll get to you. Okay, Carlton.

CARLTON SAMUELS: Thank you. That's what I wanted to bring up in terms of the privacy. We had a sub-team that was prepared to look at the data protection and privacy principles. We did not request from staff to meet with any outside team. What we did was that we agreed as a sub-team that we would look at the strongest possible data protection and privacy regime that existed and we looked at the principles that were enunciated.

I wrote the first draft for the framework for the discussions after that and we got together as a sub-team and looked at these principles. And where we thought we could augment the principles, we did that as a sub-team and then we reported to the entire group. And the entire group then had a discussion about those principles.

I want to emphasis that the privacy and data protection principles took up, relatively speaking, a lot of the discussion around it. I want to put that on the record. We did not ask for outside help. That is the way it usually goes. If we needed outside assistance, we would have asked staff to arrange it for us.

But we felt at the time that the approach we took was to look at all the privacy regimes that we could find, all the data protection regimes that we could find, extracted the principles, created a document that framed those principles, argued among ourselves about the ones that we thought were weak or whatever, and then we presented to the entire team. That was the methodology. Thanks.

CHRISS DISSPAIN: Kathy?

KATHY KLEIMAN: Carlton, no one's arguing that everyone here's put heart and soul into this report, and enormous amounts of time, effort. Unbelievable.

The questions that are being asked have nothing to do with the effort that went into the report. They have to do with the product that we're trying to decipher, which came out very recently. It's very long and very frustrating for those of us trying to decipher what the words mean.

The frustration you're hearing from the microphone isn't personal, guys. Nobody's trying to attack you. Everybody did the best they could. This is very complicated stuff and how privacy emanates out of free speech and free expression laws, versus how it emanates out of data protection laws, we've been wrestling with this for a decade. More than that. A dozen years. This is hard stuff.

But how John Berryhill, who represents registrants, knows how WHOIS data is abused and how registrants under the guise of trademark

infringement claims, it's actually anti-competitive claims. A big boy is trying to drive out a small competitor, a new entrepreneur who is entering their field, and they're using a trademark claim and they're using that data to find a home-based business. I've experienced that for 15 years. That's why I'm here, guys, because the abuse I saw 15 years ago was enormous.

I think Wendy and I were trying to plow further into whether you met with some of the registrant defense attorneys. It's not personal. You did everything. You spent all the time, but is there more? Were there other experiences, again, not just of those who use the data but those who are abused by the use of the data? That's just what we're pointing out, is that there are a lot of people on your panel that use the data. There are a few people in the world that specialize in the abuse of [WHOIS].

CHRIS DISSPAIN: I understand that, and thank you very, very much. Can you just help me? Because there are a couple of things that I'm not clear about.

If your starting point is that you register a domain name and you fill in the information in WHOIS, unless your starting point is, "I don't care about all of that. I'm just going to lie and put in Mickey Mouse," unless that's your starting point, which I don't think it is, then currently the situation is that the data goes in. Unless you proxy to hide it, the data goes in.

Surely, it has to be better for your small business, who might be subject to a trademark abuse, that the person who may be doing the abuse has to (a) go through a whole series of steps – not gates, steps – in order to

get to the information and (b) his, her or its use of the information can be monitored. Or rather, the fact that they requested that information can be monitored.

For example, I decide to go you for a trademark, I go to David to get the information in the system. We know he did. Surely all that stuff, but a whole heap more, has to be better than what is currently the case. Help me understand why that's not currently the case. I don't understand why.

KATHY KLEIMAN: That's the question you were asked to answer. And now you're asking me from the microphone. I'm still trying to understand what's been offered and then I can weigh is it better or worse.

CHRIS DISSPAIN: I understand and I'm not asking you to specifically asking you to answer it now.

KATHY KLEIMAN: If you have a bunch of validated data and it's all public – I brought the database fields up this time. That could be a problem if more of it's public than now and you're making assertions as to legal contact when you're really not the legal contact.

But that's the big question. That's the question we're all going to have to answer. I'm looking at everybody. Is this better or worse? But nobody

questions the goodwill that was done in putting this together, or the enormous effort.

Let's ask a question about accreditation because I don't want to go back to arguing about database fields yet. I'll do that in a second. That goes back to another point in my life. Database programmers have a hard life.

So, here's a question about accreditation and the ability to find abuse. Let me try this. On Monday, we had the president of the International Trademark Association, as I understand it, was in the audience. Let's say [INTA] becomes an accreditor of its members. Help me through the process of what you're thinking, not ultimately what will be adopted, as Chuck said, by the PDP. But, what are you thinking in terms of accreditation? If there are differences, feel free to share.

My understanding is, say INTA becomes an accreditor. It can't differentiate between its members because a trade association can't do that. So it accredits any law firm that comes to it. Who in the law firm has access to the data?

Let's say David – sorry David, I'm picking on you. Let's say David has a problem and is contacted by a law firm that's been accredited by the International Trademark Association and he wants to complain and he wants to find out who it was that contacted him. Because it's really not trademark infringement. The underlying issues is really anti-competitive activity. Trace me through the process.

CHRIS DISSPAIN: Absolutely. Just from my personal point of view, I would argue that if you are an overarching body like that and you cannot not accredit your members, then you can't be an accreditor, in my personal view, that actually defeats the purpose of being an accreditor. It just doesn't make sense to me, and I don't know if anyone here would argue with that. But it seems to me if you have to automatically give credits to your members, then you shouldn't be an accreditor in the first place. Is that right? That's the first point.

CARLTON SAMUELS: Yes, Chris, you're right. Furthermore, there is a standard that has to be adopted and we have to know what that standard is for accreditation. That is the idea.

CHRIS DISSPAIN: Rod, and then Stephanie.

ROD RASMUSSEN: I can address the process question there. This is a great question. It's like, great, now we've got accountability. How do we enforce accountability?

In this example, and [INTA] is one we discussed as a possible accreditor because they do have international reach, etc. You would create a set of standards, and this would be the policy development process that would do this. And you would have, okay, for this type of purpose, you have these types of standards. You, the accrediting body, whether that's

INTA or some other organization, says, “Well, we want to apply for our members. Members that want to use this system have to agree to that standard.” They don't all get membership. They have to agree to meet that standard. They get equal access because they are a trade association, but they still have to meet whatever the standard is.

From that point, something happens where somebody has a complaint. The key there is that person could take that complaint to the RDS operator or the oversight committee, however that gets created, and say, “I've got a complaint. My information was utilized for this.” Because we've been auditing and tracking, we could actually say, “Okay, this person or this group did access this information.”

That would then get pushed to the trade association who has agreed to uphold the standards and the purpose-based contacts and one of their members had violated that terms of service. Then you would have whatever the sanction regime is. Again, that's a PDP thing for us to figure out what that [inaudible], but that could be they don't get access to the system or there's a fine or some sort of something, some sort of accountability measure, that is put in place at that point.

CHRIS DISSPAIN: Yes. I'm not sure whether you said this or not, but equally, just because an overarching body accredits, the actual entity accredited has its own validation ID, so we would know it was them, rather than the overarching body, because I think part of what you said was they would appear as if they were making the query on behalf of the overarching body?

KATHY KLEIMAN: It's not clear.

CHRIS DISSPAIN: I don't think that would actually happen. That should not happen.

KATHY KLEIMAN: Is it going to be the body government or is it going to be Interpol that's going to be shown as the accessor of the data?

CHRIS DISSPAIN: That one I can't answer. Rod, go ahead.

ROD RASMUSSEN: It depends. The law enforcement one is kind of a special case because there are some issues around ongoing criminal investigations, which are much vastly different than a trademark type of case, or some other abuse issue.

The idea there is that you would have a unique identifier for using the system. Whether or not there's a proxy in between or not doesn't matter. There would be a way of tracking, either directly through the RDS or by going back to whoever is running the interfacing system and say, "This entity made this request for this data and there was an abuse that happened and we want to address that."

KATHY KLEIMAN: So if I have to go through a dispute process with the International Trademark Association to find out who it was that accessed the data of the registrant versus if I can go to the RDS and as easily find that gated information for the inquirer as for the registrant, which model are you thinking?

CHRIS DISSPAIN: Personally, I would much prefer for you to be able to go and find out who queried your database.

KATHY KLEIMAN: Directly?

CHRIS DISSPAIN: Directly.

KATHY KLEIMAN: Me too.

CHRISS DISSPAIN: That's my personal view, and I don't think there's anything in our report that would stop that from happening if that's what your policy said.

KATHY KLEIMAN: Does the report speak to it one way or the other?

CHRIS DISSPAIN: I'm not sure. I don't think so.

STEPHANIE PERRIN: Can I jump in here?

CHRIS DISSPAIN: Yeah, go ahead.

STEPHANIE PERRIN: If I had a whiteboard, I'd do a dreadful diagram here, but if you are under a data protection regime – and hopefully there will be either a policy that provides the same rules or a high level of rules, or you'll be in a jurisdiction where there's a data protection regime, you would have a right to find out who accessed your data.

Now, talking as an individual here for the moment, that right has to be free, Not something like a UDRP-type of process. So we will have to build a system for a data protection regime that provides you access. "Okay, who got my data, and I want to know exactly who. And I want to be able to correct it and ensure that there is a repercussion if there is a breach because if somebody…" – and frankly, the insider abuse tends to be over love or money. Ex-partner or anti-competitive.

CHRIS DISSPAIN: Or, anti-competitive ex-partners.

STEPHANIE PERRIN: And people who do that, in data protection regimes, there's supposed to be repercussions for people who do these breaches. So once you've built that system, it doesn't make sense to put business through some very expensive UDRP. You already have the mechanism built for the privacy side. I don't know why you wouldn't just get that data and away you go.

KATHY KLEIMAN: Because I don't live in a country with a data protection regime.

STEPHANIE PERRIN: We'd take you, you know, in Canada.

CHRIS DISSPAIN: You can move. It's not a problem. Or maybe we should incorporate the territory and country of ICANN, and then we can just do what we like.

KATHY KLEIMAN: Recognizing that we probably will be creating some kind of harmonization.

CHRIS DISSPAIN: This is true. And just so that we're clear – no offense to any Americans who are happy with their current system – but I think it is fair to say that this working group, pretty early on, moved towards looking at those benchmarks, non-U.S. based, non U.S. regimes, where there were data protection, privacy laws, etc.

There was dispute about which one was better than the other, and Stephanie was, of course, pushing the Canadian view and Michael was pushing the European view. But fundamentally, we all acknowledged that the U.S. thing, you've got to move beyond that to create something that will be workable around the world. Sir?

ADRIAN CHEEK: I'm currently in law enforcement. There's a whole different [inaudible] arguments. I'm not going to get into Interpol. My name's Adrian Cheek from the NCA. The question I've got is around the WHOIS.

We know the WHOIS is broken and the moment and we know most of the data on there is absolutely rubbish. But you've mentioned yourself this is probably not going to fix that. As a researcher and an analyst, I can use the broken data and still find my targets I'm looking for. I can use the terms and conditions which is are already out there on the registrars to actually obtain data. I've never obtained a court order in five years to obtain data. I've never needed to because there are rules already in place which I can use in whichever country I choose. China, no problem at all. Canada, a little bit more difficult, but we won't go into that.

There are already things in place for us to do this. Now, as far as I can see, putting a non-law enforcement hat on now, I can do 50,000 searches an hour, say, for example. A criminal...

Before I go there, has anyone got any law enforcement experience on the panel?

CHRIS DISSPAIN: That depends on what you mean.

ADRIAN CHEEK: Has anyone been a police officer or a cop in a particular country? This is another concern I've got. The approach the panel have had to the report has not been thinking like someone who uses something illegally. It's been a very clean approach. That's what I've interpreted from the report.

CHRIS DISSPAIN: I think you'll find that we all thought about this report as somebody doing something illegally. Rod was our expert on how people might use it.

ADRIAN CHEEK: From my point of view, then the validation for a company is absolutely fine. There's a company contact, etc., etc. But the criminals we see at the moment, I'm not worried about that. Customers do not look at the WHOIS data when they go to a website to buy something. This is one of our problems. They just go to the website, the majority of customers. They don't look at the WHOIS data.

So they don't know that the website that they are looking at has registered by John Smith of 10 Downing Street, which is going to fall outside of the validation period, or the accreditation.

CHRIS DISSPAIN: Let me slow this down a little bit, because we're in danger of getting lost here. I want to go back to the very beginning of what you said. Unless I misheard you, what you said was, "As you've already admitted, these recommendations won't change the accuracy of the data."

I don't actually think that's true. I think we've said it will change the accuracy of the data. We categorically believe that what we have put in place will lift, to a great extent, the accuracy of the data. However, if you are saying as a – and let's call it a criminal. Bad actor is a term we use quite a lot. Would they be able to get around the system? Yeah, sure, in the sense that they could validate something that wasn't correct. Absolutely.

But I want to make it really clear that we believe that the garbage that is currently in the WHOIS, there will be much less garbage and much more accurate data.

I'm going to come back to you in a second. Fab?

FABRICIO VARYA: I think we actually had a full discussion when we were in London for the second time or third time about this. I think what you're getting at, which is that criminals will register websites, use them to steal things, etc., before the validation process catches up with them. And by the time that it does or cleans them up or flags them or what have you, the harm's already been done. Is that where you're getting?

I remember we had a whole discussion about this and it was this whole discussion and it was three levels because it was syntactical and it was

operational, and then as Alex brought up, the identity part of it. We had lengthy discussion putting in context each one of those types of levels, how quickly you could or couldn't do things, what you could or couldn't flag and what that meant. Did you stigmatize people who shouldn't be stigmatized in the system just because they weren't able to return their postcard in time? Up until that point, a legitimate user would be flagged.

Those are types of things we struggled with. We went through systems, like could you do a credit card system? When you change your postal address in the United States, they immediately write you and ask you to pay a dollar with your credit card so that they could at least have two different ways of verification.

We went through systems to try and make it quicker, reliable. Could you do it through SMS, etc.? I don't know that there's any right answer because we have to balance what you're concerned about, which a lot of us on the panel were concerned about, along with like Lanre in his jurisdiction.

We had a lengthy discussion about how are you going to get the people in my jurisdiction? There isn't necessarily exact same postal system and accuracy. People don't use credit cards there. They use mobile cash. So we tried to identify and deal with the issue you're bringing up, but the problem is that every time we did, we found that we cast the net so wide that it actually left a lot of the world population in a little bit in a lurch.

What we didn't want – I remember, Stephanie, you and I talked about this – was we didn't want to start flagging people in the system just because our system of validating them or a proposal we would put up would paint them in a bad color until they were validated. As great as that would be, the net would be cast wide enough to catch the criminals and tip off potential fraud victims, in that bucket would also land a bunch of people who weren't fraudsters. They just – because of the system or the way the system operates, they, an example, didn't get their postcard back in the mail on time.

It's something that I think is a great question and something that I hope you can help Chuck and the group through the PDP actually wrestle with because we couldn't come up with a right answer.

CHRIS DISSPAIN: Back to you. Sorry, Stephanie. Just, let me say, we've got ten minutes, so if we could all try and be succinct, that would be helpful.

STEPHANIE PERRIN: I was gesticulating wildly because I have been making the allegation, and I don't have the facts to back me up because the facts on identity theft in my jurisdiction are not very good in my jurisdiction, and globally, they're not very helpful.

But, there is the risk that we're actually, with this validation process, driving identity theft because now you cannot register as Mickey Mouse and get away with it. We don't even have phone numbers that add up correctly right now.

We did say that we needed a full risk assessment. We did a little risk survey, but that's not the kind of risk assessment we need to determine what the impact of this is going to be. If it's going to drive identity theft, then we need to go back to the drawing board in the PDPs. So please, come to that.

ADRIAN CHEEK: Just the second part of that question. Even though the data is broken at the moment, I can use that data.

I've got a bad actor who's registering 5,000 domains a month. If I left law enforcement tomorrow, but carried on doing the work I do, because of what's now going to be potentially put into place, I then have to justify why I'm looking at the 5,000 at a time.

What's to stop the third party, whoever ends up being the RDS wherever they are, turning around and saying, “Actually, you've made too many requests over the past six months, for a valid reason” and then turning around and canceling my contract?

At the moment, I have protection because I'm law enforcement.

ROD RASMUSSEN: I'm the cyber-crime investigator on the panel here, so I deal with this all the time. We probably look up, I don't know, a quarter million domain names WHOIS's in a day for our system. Maybe not that much, but it's a lot. We have rate limits that we have to deal with and all that. Registrars know us very well as a result.

The way the system is envisioned is that you would be able to, I guess, for the lack of a better word, profile the usage based on who's actually accessing the data. We would fully expect that people who are looking into domains registered for botnets, which are typically thousands and thousands of them at a time, would be doing requests for those as they show up. This is getting back to how do you balance the use of the system? It's fairly standard.

CHRIS DISSPAIN: Also, it's what level of information for a botnet query? You might only need something, [inaudible] information.

ROD RASMUSSEN: Right. It would be a lighter level of information. Two other points I want to make on this topic. One is that if the criminal or bad guy or whatever you want is using a pattern, those patterns will still show up in the ways the data is put into the database. There would be, whether it's contact IDs or whatever that they're using over and over again, DNS servers. All that stuff that we typically use is going to show up as patterns.

The other thing that people tend to forget is that most of the domains that are used for abuse are actually innocent. They've been broken into somehow. This is where cleaning up the garbage is really helpful from my perspective as an investigator is that I can actually get ahold of somebody – the tech contact or the abuse contact that we're now providing – and really vastly improve the efficacy of our efforts to either find them for more information or shut down malicious activity. So that's a big win, I think, for moving forward.

ADRIAN CHEEK: Just one last point. Just from the profile side of things, yesterday I was looking at [inaudible] group. Tomorrow I may be looking at counterfeiting trainer group. How are you going to profile my usage based on the fact that I may not be looking at the same things every day, but I am making 50,000 requests for an e-mail address per day? That's a concern of mine because eventually someone somewhere will turn around and say, "Actually, there's no pattern to what he's looking for. It's just all completely random for different reasons. No more." And then I'm locked out.

CHRIS DISSPAIN: But who are you in the first place? I'm not quite clear.

ADRIAN CHEEK: At the moment, that would be law enforcement. But if I went into a private business tomorrow, I would still be looking at the same – at the moment, all the information is free and there's no restrictions to my accessing that data, but at some point potentially somewhere along the line, someone's going to be authenticating that and saying, "No." And that third party is a concern.

CHRIS DISSPAIN: Let Fab respond and then we do have to wind this up.

FABRICIO VAYRA: I'll be brief. As I mentioned to J. Scott when he asked his question in the morning, this is a PDP implementation situation. I think that for a lot of our report you'll see principles. You'll see recommendations. But for the precise reasons that Chuck mentioned, it wasn't our job, and we didn't have any fantasy that it was our job, that we would actually boil this down all the way through implementation. We tried to do as much as we could to supply the facts, to show our reasoning and what we meant as a guidance.

I, and the IP community, for certain, is very concerned about the exact same things. That's why I said to J. Scott today when the PDP process starts, when the community starts discussing, you need to hit on this point, because it really does all come down to what does authentication mean?

During the authentication process, that's where those bells and whistles and knobs and levers get adjusted. And you need to make yourself clear to Chuck, to James, who was here earlier and everyone else who is on the GNSO, and to the community, because it's vastly important because the devil is in the details.

A lot of us all were completely fine with putting out principles and recommendations showing our intent, but really relying on the community to actually put in the implementation.

We are not going to be able to give you an answer here, and we don't want to, in that we don't want to supplant what Chuck and the group are going to be doing with the community.

CHRIS DISSPAIN: All right. So, I think we've reached the end of our two hours. Fantastic.

I'd like to be able to say, “And in Los Angeles, this,” but I have absolutely no clue what in Los Angeles “this” will be. Except it will not be, “Well, the Board's accepted the report so go away and implement it.

We are expecting to enter into some fairly lengthy discussions with the GNSO about next steps. I think the Board's formal process will probably be to accept the report, “Thank you very much,” blah-blah, say all the usual things Fadi said and so on, and then move into discussion with the GNSO about things like we talked about the other day about what should we do next. Should we get legal advice? Should we do a risk analysis? Should we do this?

Then, the goal being to build a package of the experts report, plus ancillary documentation and information, clear up any misunderstandings with FAQs and so on, and then I think at some point – and it's not going to be tomorrow. It's highly likely to not to be before Los Angeles. In fact, it's practically guaranteed to not be before Los Angeles.

We would then negotiate effectively with the GNSO, “How do you want to do this?” Do you want to do a series of policy development processes on chunks? How do you want to work it out? Then get those happening. Resource them properly, because nobody is under the illusion you guys can do this on your own. You're going to need staff help and so on.

For those worried about the clash between the amount of work involved when it comes to the U.S. stewardship transition and the accountability piece and so on and so forth, my personal feeling is that

this will probably be hitting the road around about the same time as the other is finishing, assuming that we actually do ever finish the other, which is entirely up in the air at the moment.

I hope that's useful to take back to your constituencies and what have you. And I really would like to take the fear out of this if I can. I understand the people get very concerned about what things say and so on, and rightly so. But next steps are very, very much with the community, not with the Board. Okay? Thanks very much, everybody.

[applause]

[END OF TRANSCRIPTION]