DURBAN – Replacing WHOIS-The Next Generation Directory Service
Monday, July 15, 2013 – 14:45 to 16:15
ICANN – Durban, South Africa

NANCY LUPIANO: While we're waiting, I'd like to remind all of you to go to the dot ZADNA booth to get your beautiful beaded pin that will give you access to our gala. Once again, if you go to our host's booth, they make beautiful beaded pins with your country's flag on it. And that will get you into our gala Wednesday night. Thank you.

JEAN-FRANCOIS BARIL: If you can take your seats, we are almost to the point to get started. Okay. So I believe we should get started.

So very good afternoon. And warm welcome to this next-generation directory service briefing by the Expert Working Group.

I am personally very, very excited to be here today in Durban. And this public session materialized a very important milestone in our journey for this EWG. So for today's agenda, if we can get to the next slide here, we would like to propose to summarize, as briefly as possible, the essence of our initial report. And, in particular, we'll highlight the key findings and recommendations that we have already published. And then we'll utilize the maximum remaining time to organize an interactive an structured dialogue around a few questions that we are still having open and for which we'll need your precious help. And then we'll save some time at the end for question and answer more in the spirit of clarification for what we have already published. It's fundamentally important for us to create an environment where you feel very truly involved with the solution as part of the solution.

For the mandate, as you have probably noticed for more than a decade, very inefficient, almost broken WHOIS system, it's clear that the ICANN community has to find a solution. It's a must. And I believe we cannot any longer turn around these missing or broken processes on privacy, access, accuracy, just to mention a few of those.

The status quo is not also an option as we need to put our research into the complexity looking forward of this Internet solution. Hence, decisions from the board back in December was not only to implement the WHOIS recommendations from the review team but also to create the Expert Working Group to assess and redefine fundamental user needs and purposes for the next-generation registration directory services. It was also good that we received a clear mandate from the board to have a fresh look at this very difficult solution and to recommend a revolutionary approach.

Just as a reminder, many of you in this room, if I remember correctly, back in February when we get started we're thinking that this mission was almost mission impossible.

So, in practice, what we were given to do is solving this equation like who needs what as data and why in the best, best, best interest of the entire community of Internet.

This comes with defining or I would say redefining criterias and considerations related to the overall value chain from collecting to maintaining through validating and storing, disclosing data. And that was a concept that people should now feel very comfortable to share data.

I believe that the trust element and respect of the data integrity is a very, very important point, that we have taken that very seriously in our team.

The team -- so, as it has been said, there is no good project without having a great team. And there is no exception to that for the EWG.

So thanks also to Fadi for his generous recognition this morning.

But fantastic team by its unique diversity, technical ability to have very thorough, deep and extensive analysis on all key elements we examined.

[Talking simultaneously]

You're on the air.

CHRIS DISSPAIN: I'm on the air. Sorry. I apologize. Can I come off the air, please.

JEAN-FRANCOIS BARIL: But also a lot of fun into this group. Thank you to Chris and Rod. But fantastic also for its capability to work and to perform together. Very impressive skill, I should say, coming from the business side of the equation to reach consensus in an unbiased way despite very, very divergent interests that each of the 15 members represent.

So far, not surprisingly, I should say, but impressively further to our provision of our initial report on June 24th, I should say that we have received a lot of very positive feedback and encouragements. But, at the same time, you sent us a lot of constructive input and remarks and requests for clarification that, hopefully, we will use this session to help you to understand better what we mean by our recommendation and insights.

This is extremely helpful as it triggers further our analysis on the pros and the cons and guide us on the structure and the explanation of the who, what, and why. So, once again, like we've done in Beijing in the spirit of this EWG, each of the spokespersons from this table will be talking the name of the EWG and not in the name of the individual community they are supposed to represent.

Also -- and I think this will be explained further with Chris -- don't be afraid that, if we introduce also this famous timer just to help us to structure a little bit the debate later on.

So, without further ado, I will pass not the air but maybe the button to Michele to expand further on our initial reports.

MICHELE NEYLON: Thank you, Francois. I'm just going to go through this rather quickly since a lot of you in the room have probably read the report. Some of you might not have done so. And we're going to provide plenty of links so you can find it. Read the executive summary, but also actually read the report.

So we published our initial report back on 24th of June. It's based on a lot of analysis of different use cases of registration data. I prefer to talk about registration data rather than WHOIS because WHOIS is what we're trying to actually fix. Fundamentally, what we're proposing is to abandon the current one size fits all WHOIS paradigm as we feel it doesn't work particularly well or is broken, depending on which way you want to look at it.

The -- under our proposal, what we wanted is to bring the idea of purpose into the system so that it's not simply a question of looking up some data but why you are looking up that data. What is -- what are you trying to solve? What problem are you trying to resolve? And another key factor that we've looked at in every single thing is privacy. It had -- there has to be a privacy consideration in everything. And, of course, accountability and transparency and accuracy. Sorry, not transparency. Then, based on this, we formed consensus on these principles. And it's very important to note that, as a group, we've actually been working together towards solutions. I'd love to say it's been a rocky road and there's been lots of tears, but that's actually not the case. We've worked very well together collaboratively. We've put in quite a bit of time into this. And what we're presenting is what we all believe and have consensus on.

So these principles are applicability, international considerations, accountability, privacy considerations, permissible purposes. We also, of course, looked at what was not permissible. Data disclosure; data elements; access methods; validation and accuracy; standard validation service; contractual relationships; and, of course, storage and escrow.

In the more interactive part of this, we'll be reaching out to you for input. And, please, if there's something you don't like, make a suggestion rather than just telling us you hate it.

So what we've proposed is the ARDS, which somebody has already managed to rename into the TARDIS because they thought that was a cooler name for it. I'm sure somebody will have problems with the copyright around that, but never mind.

So in this model here you have on one side you have registrants, you are the ARDS sitting in the middle, and then you have requests just for data. So, when you register a domain name, be that directly via a registrar or somebody else, you provide data. That goes up into registries, into the aggregated system. And then, when somebody wants access to data of some kind, they have to request it out of the system.

Now, the key thing is that there will still be some data available in a kind of anonymous type scenario. But most of the other data is behind a form of gate.

A lot of advantages with the system, that you have a lot of data validation. And you'll also be able to put in proper kind of access controls for those people requesting access to the data, which would, hopefully, lead to a higher level of accuracy across everything and more security and respect for privacy.

And, as I said already, our initial report is based on consensus of the entire group.

And, of course, the other thing is there have been compromises. In my day job I'm a dirty filthy registrar. I've got intellectual property types.

I've got people who come from the info sec community. You've got people who have got experience in country codes. You've got people who come from a wide range of different viewpoints. The thing is this working together, this give and take, compromises -- and some of you may find that some of our suggestions might upset you a little bit. But we'd like you to have a look at the entire thing rather than just, you know, ripping it to shreds. Have a look. Ask us questions. We think it's going to provide a significant improvement over today's system. And we're asking you, of course, for feedback on this.

This is the next slide. At this juncture I'm going to hand you over to the master of ceremonies, Mr. Chris Disspain. Do you want the clicker, Chris?

CHRIS DISSPAIN: Thank you. I'm on again. Excellent. It's seamless. Seamless. Thank you.

Now I've got to learn how to work this thing. Okay.

So, guys, we're going to go through a series of questions. There will be a long session at the end. There will be a long session at the end for open questions and open mics. But we'd like to get focused discussion on particular areas that we really want your feedback on. And -- if there is any.

We're going to give seven minutes to each of the slides. It might look like there's a lot of stuff on the slides, but we've tried to put up the relevant information to ask the questions.

So we start with our potential advantages and disadvantages of the model, which we've listed up there.

And what we want to know from you is if you think there are any other additional advantages or disadvantages to the model that we've proposed. And, also, a very specific question, which is which of the data repositories should be authoritative? As a country code manager, my immediate response to that was, well, clearly, the registry needs to be authoritative. It's the registry that actually needs to have the authority to data. But others may have a different view.

So we have microphones in the usual place at the front of the room here. And in the usual way you come up and we record you. And, in the usual way, nobody is getting up except for Amadeu.

AMADEU ABRIL I ABRIL: I felt your pain of not having anybody here to ask questions here to answer. My answer would be the same as yours, the registry. And, as a matter of fact, I love many things in your report. I don't understand some of them. But, you know, I may ask a question later. And there are some things that I don't like. And the one I don't like is precisely this idea of the central repository.

Beyond creating a single point of failure, risk and easier access for hackers and FBI, what else are you trying to achieve there? The same thing can work just by having a set of rules and procedures but keeping the registries with what they have to do even contractually is having responsibility for the data that's in their zone.

CHRIS DISSPAIN: Does someone want to see if they can tackle that question? In essence, Amadeu, you're asking why we would have a central repository, in essence. The advantages are kind of up on the slide. Do you want to take it, Rod? Rod and then Michele.

ROD RASMUSSEN: The essence of the question is it creates a single point of failure/a really interesting target for hackers and government agencies, et cetera. So I think, obviously, we talked about this within the group. This is certainly a concern.

I don't know that it's any more of a problem than big registries have today because they have the same issues to deal with. There are centralized databases of lots of things. And, as new TLDs roll out, there's a handful of registries that have a lot of data already. So this is the same problem we all have. I think there's some advantages and disadvantages. One is a bigger target. Two, though, is you have the ability to increase your security functionality; whereas, a smaller dispersed amount might not be able to. As far as government access, we've already -- one of the proposals we have is to take a look at where this is hosted, the location, the more international nature. I think that's part of the policy development that comes out of this. But that's certainly an issue.

CHRIS DISSPAIN: Yeah. I think that's right. Michele, did you want to say something? I'm sorry. Lanre, go ahead.

LANRE AJAYI: Okay. Like any other systems, there are pros and there are cons. We recognize that as a challenge. But that can be surmounted. But, if you check it against other advantages listed, you will realize that it's still a far better option. That is a challenge that we recognize, and we're still talking about it.

CHRIS DISSPAIN: Thanks, Lanre. Briefly, Michele.

MICHELE NEYLON: I think Rod has covered a lot of this. There are, obviously, disadvantages which we're already aware of.

CHRIS DISSPAIN: They're up there.

MICHELE NEYLON: They're up there. But, of course, what we're looking at this, realistically, do the advantages outweigh the disadvantages? And at the moment we're going toward the advantages outweigh the disadvantages.

CHRIS DISSPAIN: Steve. Sorry. Can you just -- I apologize. I know who most people are. But, if you wouldn't mind introducing yourself at the microphone before you speak, I'd appreciate it. Thank you.

STEVE METALITZ: Thank you. Steve Metalitz from the intellectual property constituency. First, I just want to thank the experts working group. I agree you have made an enormous contribution here on a difficult problem.

I just want to make two quick points. First, on the advantages and disadvantages. I think one reason for thinking that it's more on the advantageous side is, if you think about the situation we're going to, which will be 1,000 gTLD registries rather than 20, it more closely resembles a situation we have now with registrars in the thin WHOIS environment. And I think there is a movement toward thick WHOIS in the existing -- in the legacy environment. And I think some of the same reasons would argue for the advantages of having the ARDS as you've described it.

The second point I just want to raise on your last question, on the thick WHOIS working group that's working in the PDP right now, I convened the authoritativeness subgroup. And we had a lot of discussions about it. And it's -- it surprised me to find it's a more complicated question than might at first appear. Authoritativeness. You need to understand what we mean by authoritativeness. And we found in the current environment there is no ICANN policy overall that says that registry data in the gTLD environment is authoritative. In fact, there is a policy that says in the UDRP case the registrar data is authoritative. So I think we need to understand what we mean by authoritative. It's not a synonym necessarily for accuracy, the highest point of accuracy. It's what can we all agree it will be the actionable data. So I just raise that as a response to this last question.

CHRIS DISSPAIN: That's a very good point, Steve. Thank you. Bearing in mind the time, if we could keep it short, sir.

UNIDENTIFIED: Okay. (Saying name). I would like to point to several short things. One is removement to joint WHOIS is quite opposite to removement to which all the system goes. We are going to more distributed systems, and the WHOIS goes quite opposite direction.

That's funny. Because it's known that distributed systems are more stable and more reliable. These advantages which I did not see here. The disadvantage is that legislation about handling personal data are different in different countries. I cannot understand how one entity on the world can satisfy all legislations. And our -- otherwise, those entities who provides data to these will wrote its own legislation in its country. I cannot see how it is addressed here. And for which data should be authoritative. Authoritative should be the data at the source.

CHRIS DISSPAIN: Thank you. Just very briefly. The same problem of dealing with national laws applies to every registry. Because the registries tends to be resident in any one country. And, unless you're going to limit your registrants to only registrants of that country, you'll effectively have the same issue. I'm going to take -- yes, sorry. Go ahead.

WILFRIED WOEBUR: Yes. My name is Wilfried Woebur. And the question is whether you are going to come back in under a different headline to the request for validation accreditation.

CHRIS DISSPAIN: Yes.

WILFRIED WOEBUR: Then that's it for me. Thank you.

CHRIS DISSPAIN: Can I take the remotes first? Pat, would you mind?

UMIDENTIFIED: Not at all.

CAROLE CORNELL: Hi. This is Carole Cornell. I have two.

Antoin: I missed an unclear jurisdiction of the ARDSDB is the first question.

CHRIS DISSPAIN: He's unclear on the jurisdiction of the ARDS? Okay. Good question. Open for discussion. Rod suggested the moon may be, in fact, the best place for us to put it. Second one?

CAROLE CORNELL: Thank you. This is from Kathy Kleiman. How do you ensure it is really a one-stop shopping for requesters? Won't the data now be in three places -- registry, registrar, and centralized repository? What stops a registry from responding to its local government or law enforcement or IP community? And the last question: how does it become a one-stop shopping with respect to the biggest registries are not centralized databases, i.e, dot com is decentralized?

CHRIS DISSPAIN: Sure. Michele, you want to briefly deal with that? And we'll go to Pat.

MICHELE NEYLON: Yeah. I think, if I understand the question, it's -- at the moment a registrar collects data, sends it to a registry or not, in some cases. And then you'd have the third system.

At the moment, yes. With, say, a thick register, say, dot biz, you could query the registrar or the registry's WHOIS and get back the data. But that's assuming that the registrar is maintaining a publicly accessible WHOIS server.

Under this model, the registrar no longer would maintain that. So that point is gone.

And one would also assume that, under our model, the registry would no longer maintain a publicly accessible WHOIS server.

CHRIS DISSPAIN: It's also the case, isn't it, that, in any event, whatever you do, the registry and the registrar are subject to their own national law in any event. So that's just a fact. Pat?

PAT KANE: Hi. Pat Kane, VeriSign. So, kind of to follow up on Steve's comment or question before, if you're a vertically integrated registry, it's easier to authenticate the data and, thus, be authoritative. But one of the things we've struggled with in terms of being the last or the only thin registry that we have today is, when you take the -- when you take data from a registrar, you don't have a business relationship with that registrant. So it's near impossible to accurately authenticate that data. So, thus, authoritative means something very different because you can't authenticate it in a centralized model or at the registry level either.

CHRIS DISSPAIN: I agree. I think we're trying ourselves up in knots on this authoritative thing. I know what I mean -- as a registry, I understand what I mean. It's where, if there is a gap between time, which one is the one that you can rely on is what I mean. But I understand that that may not necessarily be the case. I think we can take that we need to deal with the word, because we haven't dealt with the word. Very quickly, Michele.

MICHELE NEYLON: Yeah. I think I understand the concern here. I think it's a problem around terminology that maybe we need to clarify what we meant in that usage of that term. Because my view on it would be that that was the source that would have data that was of use to me and that was up to date, not whether that data was 100% validated. That's why I was looking at it.

CHRIS DISSPAIN: We're over time on this slide, but people want to talk about. We're going to run with it. Amadeu, briefly, please. Then back to Carole and then Becky.

AMADEU ABRIL I ABRIL: Okay. On the themes on this slide, I wanted to go back to the question of authoritative. And the answer is it's authoritative where the data is. And ADRS or WHOIS is only a subset of where the data is raised. And for data that some of this uses may be necessary like, you know, credit card information of the registrant is at the registrar. So probably you don't have a single answer, but the single answer is not certainly at the central repository that's only getting the data from other sources. That would make things more complex.

The other question regarding the centralized thing, yes for access, yes for many things, but not for keeping the data. You have not convinced me. Your answer is oh, dot com has lots of problems already so let's export the problem of dot com to dot travel, to dot cat, to dot (indiscernible) and all the news. No thanks, it doesn't work. Solve the problem where it is but don't try to export it by creating the life of those that have not created this problem, more difficult.

CHRIS DISSPAIN: Carole.

CAROLE CORNELL: Thank you. This question is from Michael Young. What are the next steps to prove the feasibility of technical implementation or to develop that further?

CHRIS DISSPAIN: So there's no doubt whatsoever that there are things that need to be done in respect to feasibility and that is, you know, at the next stage of this -- of this process. Becky. And then I'm going to close this line at this -- for this one and move on to the next slide.

BECKY BURR: Thank you. Becky Burr. I guess I just want to reiterate both the practical and the theoretical question about what are the advantages of the centralized model and why are they so much more -- let me just finish -- I mean, are they really so much more -- so powerful compared to a decentralized model that it is worth what will be a very long slog, I think, in terms of actually transferring data to a centralized place from a registry perspective.

CHRIS DISSPAIN: So I accept that. Some of the advantages include only having to accredit law enforcement agencies once through one place because they don't have to go to each registry, but it's a much longer discussion to go through and they're listed in kind of bullet points up there. But I'm actually going to move on to the next slide because we're short of time.

So I'll take your comment next time, sir, if that's all right. Moving to the next slide.

Ah, good, got a lot of picture, and the clock sits right in front of the most important part of the picture. So thank you. So basically what we're saying is that access to the data is going to become purpose-driven. Right now all the arguments about -- are about, you know, there's a lump of data and everyone has access to that lump of data. And what we're talking about is moving to a purpose-driven -- purpose-driven access. So the question is, does that satisfy users' needs? Does it satisfy everything that needs to be satisfied? Because sort of the principle is like well, I don't -- if all I'm trying to do is trying to figure out who owns a particular name, for whatever reason, it might just be because I'm about to buy a bunch of flowers on the Internet and I want to find out if this particular domain name is owned by a company that I know. That's one level, and that presumably would be a fairly simple, straightforward, anonymous query. But if I'm law enforcement and I want a whole depth of data for some reason and I've been accredited, that's a different need. If I'm a trademark attorney, a different need again. Take a real life example in Australia. In dot AU we don't publish the creation date of domain names for various reasons but we have a system where if you are a law firm and you send us a note that says we are -- we need to have this information for the purposes of considering legal action, we will provide it to you. That's a purpose-driven exercise. Sir.

NIC STEINBACH: Nic Steinbach from name dot com. It's cool that you guys are trying to like deter abuse before it happens with a gated system. There's some references in the report to I guess post bad action accountability so imposing kind of these vague penalties and stuff like that. I was wondering if you guys could just kind of clarify what you think those penalties would be, whether they're financial or access based or something like that?

CHRIS DISSPAIN: So thank you for the question. And it brings up a very interesting kind of overarching point here which is we are not trying to provide an immense amount of color and depth. Our -- our job is to come up with a recommendation as an overarching set of principles that will then result in an exercise in the -- in the right forum which is the GNSO to actually produce that sort of information. So it's not that we haven't thought about it or talked about it, but we're not actually about doing that because that is the job of the policy-making body. Rod?

ROD RASMUSSEN: Just to speak that a little bit. We have obviously discussed this kind of a point as well. This came up. And this is one of those areas where we -- we -- while I completely agree with what Chris is saying, there are several areas like this where we probably say something about it. If we haven't said anything about it yet, it's one of those areas we'd like to get feedback from the community on. So this would be one of those. Because there are many sanctioned options you can take. You mentioned financial, access, there's various other ways you can do that, and that becomes more of a compliance function at that point. It's part of the system. So it's an interesting area that we want feedback on.

CHRIS DISSPAIN: Thanks, Rod. Sir.

UNIDENTIFIED: Okay. Thank you. Great. My name is (saying name) from (saying name). Point is on the validation. And looking at the validation of requests, I'm wondering, are we going to have any kind of decentralized system whereby if I make a request, maybe from Legos (phonetic) and someone else have to respond to it, one, the time difference is there and there could be some element of downtime looking at the remitter process of each part of the world where person may be operating from. Are we going to have a decentralized way of validating requests? Thank you.

CHRIS DISSPAIN: I think the simple answer to that is yes. I don't think we anticipate there being time difference issues with the process. Once you're validated, you're validated, and obviously, depending on the level of validation it depends on how long it will take. If you're law enforcement and you're going to have access to a higher level of (indiscernible) that might take longer than if you're validating simply for the purposes of checking ownership details. James.

JAMES BLADEL: Thanks, Chris. James Bladel. I read through the report, although briefly, and I noted that you had a number of specific users and use cases, and I wanted to commend the group for identifying abuse as a use case. I thought that was important and creative. So kudos to that. But you also mentioned government law enforcement as another use case. Had you considered the use case of abusive law enforcement or governments that could misuse this data to round up a political or religious group or something of that nature, is that part of your -- yeah, I like your T-shirt, Michele.

CHRIS DISSPAIN: Yes.

JAMES BLADEL: You did consider it.

CHRIS DISSPAIN: Yes. Go ahead, Lanre.

LANRE AJAYI: And I think we emphasized a lot on accountability. Each stakeholder are meant to be very accountable. And if you're not, you'll get penalized.

JAMES BLADEL: Accountable to the provider of the ARDS system. Accountable to whom, I guess is my question. If the abuser is coming under the guise of law enforcement, where's the accountability?

CHRIS DISSPAIN: Well -- go ahead.

LANRE AJAYI: We thought of having a process for accrediting the law enforcement agency, but specifically how to do that, we are not confident. So it's going to be -- before you receive your credentials there's going to be accreditation of some sort, and if there's an abuse, one of the possible penalties, that the credentials are withdrawn.

JAMES BLADEL: Okay. Thank you.

CHRIS DISSPAIN: And James, just before you go away, two things. One, I want to make sure I understand your question. So -- so law enforcement becomes accredited, right? And so -- an arm of law enforcement or whatever it is becomes accredited, right, so that's the first step. What you're saying is if they abuse that accreditation, what is the result? Yes.

JAMES BLADEL: Yeah, that's mostly the point, Chris. What I'm really kind of driving at is that not all government use cases would necessarily be legitimate.

CHRIS DISSPAIN: True. And of course, in the jurisdiction that the law enforcement agency is in, if there are data privacy provisions then they're accountable to those if nothing else. But it's a good question.

JAMES BLADEL: So if the jurisdiction that hosted the ARDS was more lenient than that jurisdiction, they could use this as a bypass would be like one scenario. So thank you.

CHRIS DISSPAIN: Good point. Amadeu, I'm going to let some other people have a go first because they haven't spoken yet. Actually you have but anyway. But you said you would come back on this particular point, so that's fine.

WILFRIED WOEBER: Yeah. Just once again, my name is Wilfried Woeber and I'm having two reasons for being interested in this aspect. One of them being that I was with Susan on the RT4 and I remember that we did have our share of problems to find the definition of law enforcement. Because law enforcement is everyone and nobody. And accreditation of NSA -- oh, sorry, law enforcement is sort of a -- well, a non-issue. Because how do you prove that you are operating in a legal framework. But it's just an aside.

The other hat I'm wearing is the incident response community, in particular in Europe, and seeing in that area that the majority of cases which involve some sort of domain names is actually taken care of by non-formal law enforcement entities, makes me ask the question, how do you expect to have sort of accreditation for organizations or people who are not just the man or the woman on the street and trying to find who -- who is going to sell shoes in our country but sort of who needs sort of real technical up-to-date information and how do you expect to do that around the globe in the various security response or environments.

MICHELE NEYLON: I think we actually covered this as a use case. It was one of the ones Rod -- I think Rod and I were talking about this one, weren't we? We definitely considered this, that a valid use case would be in mitigating abuse.

CHRIS DISSPAIN: So a search, for example.

WILFRIED WOEBER: And how do you prove that to the accreditation machinery?

MICHELE NEYLON: So we don't -- as Chris said, we aren't getting into the nitty-gritty details of the implementation because that would have to go through the GNSO. I'll let Rod speak to that a bit more.

ROD RASMUSSEN: Yeah, too a lot of the organizations you are talking about belong to standard industry groups, right? So there are ways of going out and getting membership accreditation. The security community actually is pretty good about vetting other people in the security community.

CHRIS DISSPAIN: I think that's good. The answer is the security industry would take care of that. Because they're not --

MICHELE NEYLON: The security stuff works on circles of trust. You get into a circle of trust, somebody else validates you, revalidates you. I mean, I'm in several of them. Rod you're probably in some of the same ones. I mean it's -- it's kind of -- it's self -- I don't know what the word is, self-regulating, I suppose.

CHRIS DISSPAIN: But it's still a valid question.

WILFRIED WOEBER: Okay. So fingers crossed, but it still sounds like a little bit of hand waving. Thank you.

CHRIS DISSPAIN: Thank you. Next one.

PIERRE BONIS: Thank you. Pierre Bonis from AFNIC. The next -- the previous slide we saw the advantages and disadvantages linked to the centralized -- the new centralized database, and when I check this slide, I wonder who's going to accredit -- who's going to give the right to have access to this or that part of the data? Is it going to be one entity deciding for every law enforcement agency in the world? It puzzle me a little bit. I mean, this thing, to me, is not coherent with a centralized database. Otherwise, you should have to have different kind of access for each and every country that have a different legal environment on accessing the data.

CHRIS DISSPAIN: I'm not sure actually -- I understand the question of who's going to accredit law enforcement. I mean, and the answer is that's part of the -- that's part of the process.

MICHELE NEYLON: I think it refers to local law, I think. Are you referring to data privacy and local law?

PIERRE BONIS: Yeah.

MICHELE NEYLON: Stephanie.

STEPHANIE PERRIN: This is certainly where the details are going to be complex. You cannot allow the dog catchers in one jurisdiction to have access to the data just because the particular jurisdiction wants the dog catchers and everyone else to have access. So there will have to be basic policy that, of course, is not going to be decided by our group, set up that says right, here are the criminal law elements, here's the different types of law underneath that, and here is who, and it's a limited group. It is -- the concept here is that you will accredit certain agents in certain law enforcement bodies, they will have access, and they will produce -- and this is not a blanket access, like a country club pass. It is a access for a purpose. And there will be parameters in the purpose.

Now, this kind of accreditation is well-known in jurisdictions where there's data protection law already because, of course, that's how these things have been sorted out, right. You need a warrant for this, you don't need a warrant for that. So that's the thinking. And we do recognize there's quite a bit of work when you span it out over the globe, but what's the alternative. It's one of the strongest arguments, in my view, from a data protection perspective for a centralized system.

UNIDENTIFIED: Just very shortly, the alternative seems to be the decentralized organization because it's closer to the national law --

CHRIS DISSPAIN: But that doesn't solve -- look at the situation we've got right now, as well. I mean, that does not solve the problem because the only way a decentralized system works is if the information held is about somebody in that jurisdiction and the request comes from somebody in that jurisdiction. The moment the information is about somebody outside that jurisdiction or the request comes from outside of this jurisdiction, it breaks down. Because how do I know, in Australia, that you are a creditable law enforcement agency? So the whole point about this is that everyone has to go through the same process to be accredited once -- once -- since they're with 1,427 registries, once. And the checks and balances can all be put into place, and that's what the Policy Development Process is about, can be put into place to make sure that the barriers are as high or as low as is appropriate for the use case and for the -- for the level of data that is being called on. Amadeu, I know you're still there. Carole, I'm going to go to you and then I'm coming to you, Amadeu, and you, sir. Yes. Sorry, Jean-Francois.

JEAN-FRANCOIS BARIL: Interesting point because a lot of people seem to crystallize or mobilize their attention to this centralized portion of what we present or recommend. And I think we should extend our view. This is not truly centralized because we still have registries behind. I think you should think that into more the concept of a portal, a gateway, and to help to synchronize the data rather than just master the incredible fortress of data. I think if we think this way, I think it's easier to understand the rationale that we have put --

CHRIS DISSPAIN: I think that's absolutely right. I think that's right. We're getting stuck in this thing about it. It goes back to that whole authoritative thing again. We're getting stuck in that sort of loop whereas actually what we're talking about as effectively as you've said. Okay. Carole. The queue is now closed on this slide. Carole.

CAROLE CORNELL: Thank you. I have three, but I'll start with this one. Kathy Kleiman. Thank you for all your hard work. Question, once you become certified does the certified party have the unlimited access to the data but law enforcement can go on fishing expeditions, intellectual property, can harass domain name registrants, and individuals can use WHOIS data to find and stalk individuals. Could you please talk about the amount of data, number of times you have access, and the limit on abuse before it happens, not after.

CHRIS DISSPAIN: So thank you, Kathy, for your as usual measured view of trademark attorneys.

That's too much -- The answer is that's too much detail, I think.

I mean, it is a series of questions that need to be answered. Presumably -- certainly no fishing expeditions, I think we would all agree that. But from the point of view of --

UNIDENTIFIED: We consider that a nonpermissible use.

CHRIS DISSPAIN: Either with a p-h or an f. Michele. Jean-Francois.

JEAN-FRANCOIS BARIL: Maybe one point is the principle that is above everything is about accountability. And if you start to abuse the system, then of course you are going to be penalized. We have not been able to go in the detail of how and so forth and the how-to because I think it's beyond what we have in plan at the moment. But this is important element. And the supreme principle is to remember about accountability. If you get into this thing for wrong purpose, then of course you are wrong person.

CHRIS DISSPAIN: Michele very quickly and then back to Carole.

MICHELE NEYLON: Kathy's Kathy's question is an incredibly important one. It's a very, very important one, and I'm glad somebody asked it. This is something we discussed. This is something that we obviously saw as a massive threat, that somebody could go in, start phishing around, do all sorts of nefarious things.

So, no, it's something we have considered, and what we would like to see is a situation where, as they have to provide a purpose for the query, no they won't have have unfettered access, unlimited access to go off on a phishing expedition to harass people or do anything else.

CHRIS DISSPAIN: Absolutely. But the detail of the number of times and all of that is just way too deep.

Carol, back to you.

CAROLE CORNELL: I'm going to go on to more because they are somewhat related to this.

Antoin: So every individual would self-appoint himself as a law enforcement of his own jurisdiction and every person in the world can access this data. What difference with WHOIS?

And this next one, Michael Young went on to say: Would a centralized system allow a type of access appropriate for security services combating domain abuse? This is the hinted at in the report, I think. Is there any proof of purpose?

And you talked about purpose, but that was the follow-on to it.

Is there any proof of purpose with regard to requests? And that was from Sam. So --

CHRIS DISSPAIN: I think we've basically handled that, in my view. I think we've dealt with it.

Amadeu.

AMADEU ABRIL i ABRIL: Okay. I want to go back to the slide but not on what whatever is focusing which is who can focus what on the data side.

I think this idea is the best one in the whole report, the whole idea of, you know, different -- not everybody needs access to everything. It's not all or nothing. We need to have a gradual thing of who has access to what amount.

And in several circumstance I would -- I'm sorry, I don't remember if that was in your report because I have only read that once the first day, had no time to go back. But I would even be willing to consider that some parties need to have access to things that are not now in the

WHOIS, like the historical data that sometimes is very important; right? That's in the SRS but is not in the WHOIS.

Now, on the other part, everybody is completely right, details will be tricky in preventing abuse here. But regarding what Jean-Francois said, you are focusing on the wrong message here. The problem is, I do repeat, you don't need to centralize the data to do all this. What you need is to centralize is the access and the rules. And now my other question is is this centralized, but is this uniform?

MICHELE NEYLON: Amadeu, could you please slow down? I'm trying to follow what you're asking us, and I can't keep up.

AMADEU ABRIL i ABRIL: Okay.

UNIDENTIFIED: You're asking about six different things one after another. I'm trying to process each one and I can't. Slow down a second. Let's go back a little.

Okay. So trying to break out what you've asked so far, you have concerns about who has access to which data elements. We do, too. And we have been discussing that.

Your concerns about which data points or data elements would be considered to be more sensitive than others. We do, too. We have been discussing it.

Hold on. What else was there in there?

CHRIS DISSPAIN: I think Amadeu has made it perfectly plain that he is not comfortable with the centralized --

AMADEU ABRIL i ABRIL: The data. The data problem. It's not that model. It's just that -- And the question was whether this is also uniform; that is, whether the same rules apply for having access to the same set of data for all the TLDs, or they maybe different according to the TLD. Because some of them, for instance, may --

(Multiple people talking at once.)

MICHELE NEYLON: That's an interesting question and I think it's something we need to consider. So the question is does the data for all TLDs to be treated the same way? I don't think we have discussed that yet.

CHRIS DISSPAIN: Which is an exceptionally good question.

MICHELE NEYLON : Thank you, Amadeu.

CHRIS DISSPAIN: Before we go on I want to point out we are actually dealing with the questions we put up on the next slide. The questions you are asking us are exactly the questions we want to ask you. In other words, we acknowledge that these questions need to be answered.

Okay. Next.

FRED FELMAN: Hi. I am Fred Felman. I am from MarkMonitor. And I guess a couple observations and maybe some suggestions to help you deal with some of these more difficult problems.

First of all, one of the things I would note is that law enforcement agencies actually do participate in the research of issues, but the bulk of technical and probably practical expertise in terms of researching these issues is outside of law enforcement agencies. And when you look at, for example, trademark enforcements online, that's one example where this occurs outside of the law enforcement, their purview.

You will see also most enforcements with respect to malware and other issues also occur, you know, with companies like Rod's and others. So I think it's important to think about a broader security community, which it sounds like you're doing. The one thing I would note, though, is some investigations actually look malicious, and I will give you an example of some that I think might be interesting and might be helpful as you consider this.

First of all, it might look like a phishing expedition when you start to crawl through domain registration records looking for random patterns of how things are registered because there's a botnet actually using some programmatic way of looking. And you actually have to have some very large scale bulk access to decode these patterns to understand them. That's one example from the malicious code perspective.

Another malicious behavior that was identified by pawing through domain records is when we had problems with the abuse of the ad/drop grace period where we saw systematic abuse by registrars that were deaccredited because they were actually dropping and actually passing those domains during the grace period, thus extending infinitely their abuse of the domain naming system.

And to decode that, it actually took -- it took a very broad look at the domain naming system and these WHOIS records. And so you may have to figure out a way to accommodate that kind of investigation to avoid harm.

One thing I would say, just to think about Kathy Kleiman's issue that might help in all this, is considering commercial versus noncommercial use. Commercial speech is not protected and is not protected by privacy laws. You must actually -- you must reveal information about commercial speech. So maybe considering which domains are being used for commercial use and defining that clearly, and that might help you through that.

CHRIS DISSPAIN: And we have, indeed, discussed that at some significant length.

FRED FELMAN: So thank you very much.

CHRIS DISSPAIN: Thank you.

VICTOR: Thank you. My name is Victor (saying name). I am from Cameroon. I'm also a reseller of domain names.

Just before this ICANN meeting, I was having a problem with a customer. We use a -- an agent, a communication agency to create this Web site. And that agency registered a domain name by putting the registrant data for the communication agency. And it has been dealing with the customer for four years, and the customer is not yet happy with the service and want to move, and contact me, "Can you move my domain name from that company?"

First, I sent an e-mail to -- I check, I go online, use the WHOIS tools, check and saw that on WHOIS data, there is no mention of any information about the customer asking me to see how I can move the domain name.

So my concern is this work is going to restrict such action as me freely access the WHOIS information and see who -- I can say owns the domain names.

This work is going to accredit certain institutions to have access to such data.

CHRIS DISSPAIN: Yes.

VICTOR: The previous slide was showing the true cases. The end user can, at the end of your work, still have free access to the WHOIS information --

CHRIS DISSPAIN: Yes.

VICTOR: -- is my concern.

CHRIS DISSPAIN: A level of it.

MICHELE NEYLON: This kind of scenario, if I understand, it's the kind of thing we would use as a registrar and our staff would use. So, yeah, obviously you're going to have access to a lot of the data you need to do this.

Now, you might need to be authenticated, but that doesn't mean you won't have access. You just won't be able to access it in exactly the same way that you access it today, but you will be able to access it in order to do what you need to do.

And hopefully, the data you get in the future in this system will be a hell of a lot more accurate, up-to-date and useful. Because some of the time you go looking at WHOIS records for domains with a third party, and you can look at it scratching your head. You've probably seen this with blank lines, weird characters, numbers in the wrong places and all sorts of other junk be, which is hard to parse.

In this system, the overall quality of the data would be good.

But thanks for the question. It's a valid query.

CHRIS DISSPAIN: Thank you. Lanre.

LANRE AJAYI: In addition to that, a whole bunch of elements will be available for you to access without even authenticating.

So I guess it's just a couple of sensitive details that are behind the gate that you will require authentication before you can access.

CHRIS DISSPAIN: And that's one of the questions -- that's one of the questions for -- again, for further down the line, for policy, is if there is a principle that there will be a level of data that's available, open, and I think we all accept that there is -- some of it has to be open to anybody, then the question is how much of it?

And what should happen?

And if you look around the ccTLD world, you'll see wild variations in the level of data that's available.

So there are plenty of opportunities to work through that and figure out what the best thing is.

ROBERT GUERRA: My name is Robert Guerra with the Citizen Lab at the University of Toronto. I want to maybe build on some of the previous questions and comments. There have been questions with regard to law enforcement access, malware access. Another actor, and this is a lot of work that we do at the Citizen Lab, is actually do kind of malware analysis, but we're not -- for other purposes.

So the question is what's been thought about for researchers or academics that are either using it formal ware analysis or for others?

A couple points, perhaps, on a way to deal with that is us, a the the Citizen Lab, in order for us to actually involve some of the groups, we actually have to go through a formal research ethics approval. That can take six months or a year. And that might be a model for researchers if they have gone through that ethics approval to show.

So that's, you know, for us, an issue we might want access.

Related to that, and it's the data uses, and maybe it's another slide, I'm not sure, is once the data has been accessed, what requirements are you going to have on the requester to actually abide by privacy of that data? Are they going to be able to resell it?

We as a university keep the data private but that's a concern is once the data has been pulled, who is going to stop anyone from then creating a portal of their own and reselling it.

So if that has been envisioned or not is another point.

Thank you.

CHRIS DISSPAIN: So we've told you about commercial opportunities that exist in this model.

UNIDENTIFIED: We actually were talking about this yesterday.

CHRIS DISSPAIN: Go ahead, then.

MICHELE NEYLON: This kind of thing, resale of the data are things we have had concerns about. Rod or Lanre?

ROD RASMUSSEN: Actually, the first part of your question is about researchers in general. We actually call that out as a particular subgroup that has different needs than others. So we have actually addressed that in the report.

And I like the process you mentioned around the whole ethics, accountability thing. I think that's an excellent point to bring up.

As far as the resale and things like that go, what is preventing people from taking data and doing something with it once they have it? Just the same thing as today. Nothing; right?

So what we're trying to do is create accountability and then rules around what you can do with the data.

There's some open issues around there are people who have business models in this area, and there's pros and cons to allowing that or licensing it, et cetera. We're still working through that and that is actually where we can really use some input from the community as well.

What do you want to see happen in that regard?

And for what various purposes?

CHRIS DISSPAIN: Carole.

CAROLE CORNELL: I have two more questions. One is from Kathy Kleiman. Is it envisioned that the registrant would have access to WHOIS requesting his/her/its data and the purpose the requester has when asked, is asking.

CHRIS DISSPAIN: Stop. Let's Stephanie respond to that now.

STEPHANIE PERRIN: In terms of the individual requesting his or her data, that's a requirement under most data protection law. So the short answer is yes, they may have to go into the -- either through the gate to the distributed system or into the larger system, depending on what model is adopted.

But that's a simple accreditation of the owner.

CHRIS DISSPAIN: Thank you.

Carole.

CAROLE CORNELL: The next one, I'm sorry I don't know how to say the person's name, DEWOLE AJAO, and the question was more of a suggest. Registry operators working with layer local law enforcement might be able to accredit/validate any requests coming from a law enforcement agency outside using existing international law enforcement cooperation. I tend to agree that the system of access can be centralized but the data in answers should continue to come from the individual registries.

CHRIS DISSPAIN: Thank you. I'll treat that as a comment rather than a question.

So now that brings us to the next one which is the privacy issue. And we've talked about, in our report we've talked about this and we've talked about effectively, and I'll try to summarize this but I know Stephanie will help me out if I get it wrong, two levels. The standard kind of proxy level and how we would deal with that, and perhaps, more importantly, or more unusually, rather, this maximum protected registration.

And we're very interested in getting feedback on this about how this could be done.

This is where you have situations where you have seriously at-risk registrants who want to register names. And, Robert, thank you.

Go ahead.

You are the queue.

ROBERT GUERRA: This is Robert Guerra again with the Citizen Lab. I think this is an excellent point of the report. I think as you mentioned before, how you implement it is going to be a challenge. Being able to have -- this is definitely going to be law enforcement in terms of identity theft or protected individuals that may need access. There's also the issue of organizations that may want to register a domain name that may be at risk in a particular country. I'm thinking human rights defenders, free expression. And being able for them to qualify for some of the status may seem easy, but to have groups be able to attest for them or go through a vetting system may sound easy. The problem is there's going to have to be some additional resources for some sort of organization.

That's the problem. No one is doing this now. No one never knows who is going to register a domain name. They may do so.

So another idea may be have you thought of someone who gets a domain name and then wishes to switch to another status? So they're more public. They're a human rights organization, and the human rights organization knows there's a special status and switches them over to a more protected setting. That's what's going to happen. Organizations will start their activity online. People will see that information is online may put them at risk and then it needs to be protected. Doing it a priori sometimes may be hard.

And working with human rights organizations and others. But I think there's a lot of different issues that may require a whole separate conversation. And as a next step, I would say definitely engage the -- some of the human rights organizations that have been working on some Internet issues, that might be helpful to come up with ideas in terms of how this might scale. Because for a small number of cases, it's easy. Scaling it for the world is going to be the challenge.

CHRIS DISSPAIN: Stephanie, did you want to say something?

STEPHANIE PERRIN: I think you raise many valid points there, Robert.

I'm not sure you -- the model that we're talking about here would be using pseudonymous credentials to register, the whole point being that with current proxy services, there's no guarantee that that proxy is not going to disclose identity features of the group or the individuals behind the domain name.

So going backwards and forwards might defeat the sanctity, if you will, of that process.

We don't envisage scaling this out to the world of it's going to be hard enough to get it to work, because it hasn't been done before, to the best of our knowledge.

So I think baby steps at first. Let's get the truly vulnerable.

We are certainly inviting, and if those questions aren't clear enough, let me say from the mic here, we're inviting input and participation from human rights organizations to help us figure out basically the attestation of the individuals and groups who would merit this kind of protection. Yes, it is going to cost money, but anything worth doing is worth doing well.

ROBERT GUERRA: And just a quick follow-up. I'm happy to help in that regard.

CHRIS DISSPAIN: Thanks, Robert.

I will come to you guys in a second. There's a really important point to make here. This particular issue is one about which is a number of people, significant number of people think about passionately. And it's never going to happen if it doesn't go through this -- our -- by our, I mean ICANN's, process.

And for me personally, speaking personally, the biggest stumbling block of getting this through is going to be GAC, governments in ICANN, agreeing that this is acceptable, because they all say that they think the human rights are incredibly important but when it actually comes down to it, that's going to be a massive stumbling block. So we need to start, we, us, all of us in this room who think it's important, need to start thinking through that now and figure out a way that will work and be acceptable to governments.

Stephanie and then I will go to Vasily.

STEPHANIE PERRIN: Just a quick point. It should be well understood in response actually to the argument that this would come with expedited takedown in the event of alleged criminal activity. And we might have to have an expedited process to determine whether, indeed, it was real criminal activity.

CHRIS DISSPAIN: In whose jurisdiction?

STEPHANIE PERRIN: I beg your pardon?

CHRIS DISSPAIN: In whose jurisdiction is the challenge.

STEPHANIE PERRIN: That's not a cure all.

CHRIS DISSPAIN: I'm just saying.

CHRIS DISSPAIN: Vasily.

VASILY: I have seen a lot of problems which are very hard to resolve in the given models centralized database, and was several ideas expressed before. I try to combine them.

Just the one of Jean-Francois, considering with system as a portal, as a place for validated links to the stores of data. And data should be stored in registries, and only in registries. And then all registries will comply with local laws. We have no problems how to set privacy and so on. And the centralized system could collect a small subset of truly public data, and help to distribute that to all of them.

And to maybe to be a proxying agent for different law enforcements just to speed up the process of access to the registry's data in the -- our legislation.

In that case, a lot of problems connected to different laws, different norms of privacy will disappear. The registry will abide the laws of its registration. The portal will provide links to these registries and maybe speed up law enforcements of our countries to access this data. This as a proposal.

CHRIS DISSPAIN: Thank you very much.

Steve.

STEVE METALITZ: Steve Metalitz. I just want to commend you for taking up this maximum protective registration issue which as everyone said will not be easy but I don't think it's quite true it's never been done. I think you will find examples in the ccTLD world. There was extensive discussion about this within ICANN in 2003.

So how useful -- how transferable that knowledge is, I'm not sure, but there is some precedent for this, and it may be helpful to you.

I just also wanted to flag, if this is the superproxy and then we have kind of a garden variety proxy, if you will.

CHRIS DISSPAIN: That's right.

STEVE METALITZ: Is it your intention -- I know you said there should be accreditation standards and so forth. Is it your intention to flesh those out or is that something that's left to the policy development process or something similar?

MICHELE NEYLON: Steve --

CHRIS DISSPAIN: Hold on, Michele. Let Susan speak.

SUSAN KAWAGUCHI: So we are fleshing out proxy and privacy and trying to give those two true definitions, and we did look at dot NL and their process for protecting specialized populations. So we have looked at that, but I think we would advocate something broader than what dot NL does.

We do need your input on the proxy and privacy, but I think the work done on the WHOIS Review Team, the work done in the latest RAA, that we're on a path forward, and we just really need to make sure it works and isn't abused.

CHRIS DISSPAIN: Thanks.

Mark.

MARK BIRKELL: My name is Mark Birkell (phonetic) and I am wearing my spam filtering hat right now, and I have a question that doesn't relate to privacy.

It would be useful to me, in spam foldering, if I could take -- if I could access certain WHOIS data in, like, RBLDNSD format at high-speed so I can get a sense of how old the domain is and how many times the name servers for the domain has been changed recently as a way of -- I don't need to know who owns it or any of the privacy stuff, but I would like to be able, if this was centralized, to be able to read that data at high-speed without messing things up.

I was wondering if anyone had thoughts on that.

UNIDENTIFIED: Thanks, that's a good question. I mean -- unless Rod wants to talk to this, but that's a question of how the data was presented, really. The RBLDNSD format is one particular format. There could be other formats available. It's just a matter of deciding which elements we would consider to be gated or nongated and whether you'd need to be authenticated or not authenticated. So it's an interesting use case.

CHRIS DISSPAIN: Rod.

ROD RASMUSSEN: And it's certainly one that we're aware of, is you have automation processes around domain names for various purposes. That would be one where you would probably accredit various people to be able to access data in that type of format. But that's exactly the kind of feedback we need from the community, is to say how would we need to do that, who would we need to provide it, at what rates, and things like that. And then we can go from there and make --

[Speaking too quickly]

CHRIS DISSPAIN: I'm conscious we're going to run out of time here, but, Carole, off you go.

CAROLE CORNELL: Last one This is from Alajan (phonetic). In one of the reports I found a question that it looks was not answered. The question asks if this proposal will start a new RFC or sort of new proposal.

UNIDENTIFIED: In our processes to submit to the board and then possibly to go through the PDP process, I'm not sure the (indiscernible) rest are coming.

MICHELE NEYLON: I mean, I think the RFC thing may be possibly to do with the work going on in --

CHRIS DISSPAIN: Restful WHOIS and all that.

MICHELE NEYLON: That's more down to the technology of accessing the data. What we're looking at is the framework and design which then feeds into policy, not actually specifying the software.

CHRIS DISSPAIN: But we have talked about the possibility recently.

MICHELE NEYLON: Yeah, we have, yeah.

CHRIS DISSPAIN: Okay. Wow. This is some slide.

So this is the uses and the purposes. And it's pretty simple, really. Have you got any other ideas about uses and purposes? I don't know that anybody's got -- necessarily going to have any in the room. But we certainly want to hear from you. If you do have -- hello, sir. Go ahead.

MARK SEIDEN: Hi, I'm Mark Seiden. I have a question about privacy proxies.

CHRIS DISSPAIN: Okay. We'll go back to it. No problem.

MARK SEIDEN: You'll get back to it on a different --

CHRIS DISSPAIN: I'll get back to it now. You go ahead.

MARK SEIDEN: The question is will this mechanism substitute for the existing privacy proxy mechanism by providing protected data for registrants who want privacy, or will privacy proxies have to submit the true registrant data to this mechanism, or would the privacy proxies address be in this mechanism just as today it's in the WHOIS?

CHRIS DISSPAIN: So this particular issue is privacy, which is -- which is closed. Proxy is different, what Steve called a sort of garden variety proxy. And, in that instance -- someone want to pick up what we're going to do with proxies?

STEPHANIE PERRIN: We have been busy discussing the difference between what is now called a privacy protective service and a proxy service. Basically, the identity of the -- shall we call them all proxies -- goes into the database much as it does now. We are talking -- do you want to go into the issue of accreditation? Because the watch word for this entire system is greater accountability on all sides including proxy services.

MICHELE NEYLON: The thing is we're not suggesting for a minute the proxy privacy disappears. But, if the proxy privacy services in the future meet certain standards and have be to accredited and have to follow certain rules, then Steve over there is less likely to want to throttle me. He wants to throttle me. So we're not saying we're going to do away with that. But there's some interesting nuances about what would happen. I mean, we've discussed maybe the demand for certain types of services would disappear. But there are other valid use cases or privacy/proxy services that obviously aren't going to disappear.

CHRIS DISSPAIN: Susan, did you want to -- go ahead.

SUSAN KAWAGUCHI: I think one of the questions you were asking there, too, is would the underlying data from the proxy registration be in this database? And we have not come to a conclusion on that. That's still up for discussion. That's something we would love input from the whole community. And I think it's a hard issue to --

CHRIS DISSPAIN: You're talking about at the privacy privacy level, aren't you, the stuff we're talking about on this previous slide, not at the proxy level.

SUSAN KAWAGUCHI: No, we're talking --

CHRIS DISSPAIN: I'm drawing a distinction between what Steve referred to as the super proxy, which is the --

SUSAN KAWAGUCHI: He's talking about the normal proxy. And that's what I'm suggesting, too, was that that information that domains by proxy may collect if I use their service, where will that -- my information reside? We have not come to terms with that yet. So your input would be great.

CHRIS DISSPAIN: Okay. Thank you. Carole. We're just going to keep going until we run out of time. So let's just -- I've abandoned the slides.

A, I can't control them; and, B, nobody wants to read them anyway.

CAROLE CORNELL: This one is from Gillian Andrews. I'm an educator who makes some use of the WHOIS to help students understand possible biases in speech on Web sites. I'm wondering if educational use cases are considered. I'm not seeing them in the report. And, if so, what potential uses are considered? What recommendations did you have from educators?

JEAN-FRANCOIS BARIL: This has been done as a use case in research, so it is part of our analysis.

CHRIS DISSPAIN: So it is part of a use case? You're done. Jordyn.

JORDYN BUCHANAN: I'm Jordyn Buchanan. So some of the previous GNSO -- one of the various GNSO iterations on the WHOIS task forces took a look at this notion of this OPOC concept. But not getting into details of that proposal, but there was an intent there to look at making sure there was contactability as opposed to making information available. And that seems very much intermingled into this proxy discussion. Have you guys given any thought on whether there are ways to improve on contactability as opposed to just giving out registration data?

CHRIS DISSPAIN: Who wants to take that? Susan, you want to take it, since you're the proxy queen.

SUSAN KAWAGUCHI: I sort of live and breathe them some days. Contactability and accountability, as Stephanie said, is extremely important. We are looking at some principles for the proxy and privacy providers to, you know, to have to adhere to and be accredited. So right now, as the world stands, each proxy provider has their own process for if you have a right to see that information. So we'd like some of that standardized, and we're working on that. I'm pretty familiar with OPOC. There was some things with that to me OPOC would not work? But, you know --

JORDYN BUCHANAN: I think I'm asking a slightly different -- you say releasing information. I'm saying have you given thought to -- are there ways to -- is it in your remit, or have you given thought to the notion of making it easier to get in touch with the registrant or whoever the -- or the technical operator or whoever the relevant person is.

MICHELE NEYLON: Short answer, yes. Have we found a solution to all the world's problems including that? No. I mean, we have considered it. We have been discussing it. I mean, one of the -- the simple thing is this: Is that I could send an e-mail to the contact point for Google.com. It's highly unlikely I'm going to get a reply.

JORDYN BUCHANAN: Depends what you have to say.

CHRIS DISSPAIN: So we have a queue, and we have a deadline. So we're going to try to get through.

JEAN-FRANCOIS BARIL: Also not to mention that accuracy and data integrity are number one in our obsession, therefore, making things different.

CHRIS DISSPAIN: It's also important to remember -- and Stephanie said it -- it's about accountability. And there's as much accountability on the registrant as anyone else. Registrants should be required to provide their information. And then there are levels of protection that can be put in place to make sure that that information is not abused.

Mikey, I'm going to go to you. And I'm going to ask you, all of you, to keep your -- if you can, down to two minutes. Mikey. I know it's hard, but --

MIKEY O'CONNOR: It's hard. Very hard. This is Mikey O'Connor, for the transcript. This is really just a process comment for you. You have a situation where you've done a lot of fabulous work, but you've kicked a lot of really difficult issues down the line to a PDP.

And, to the extent that you can anticipate the difficult issues and prebake some help for the PDP participants, you will improve the odds that we'll get through a PDP. Because, at this level of detail, I'm certainly not volunteering for that one.

CHRIS DISSPAIN: So, Mikey, you're obviously psychic. This conversation --

MIKEY O'CONNOR: I have dents in my head.

MICHELE NEYLON: Mikey, are you saying you want more detail?

CHRIS DISSPAIN: Yes, he's saying --

MIKEY O'CONNOR: No. Actually I want -- I want more detail. That's fine. I'm always into that. But I think that one of the things that the WHOIS issue presents and the reason that you were formed was because there's also a conversational dimension to this or a political dimension or an argument.

CHRIS DISSPAIN: Absolutely.

MIKEY O'CONNOR: And, to the extent that you frame all the old positions very clearly but don't frame any strategies for driving through those deadlocks, we're likely to just tee up the same old deadlocks we've had before.

CHRIS DISSPAIN: You're absolutely right. The balance for us is to figure out how much -- some people will come to us and say you haven't given us enough information. Others will come to us and say you've given us too much. So there is a balance to be cast between those two things. And your feedback that you'd like more detail is much appreciated and understood.

Going to go to Malcolm and then Carole and then Jim and then back to Steve.

MALCOLM: Thank you. Can I make a clarification that related to the point that the previous person at the microphone was making? And that's that contactability and accountability are not the same thing. Contactability is being able to send a message to the person who is the registrants. Accountability is being able to lay hands on that person. These are quite different concepts for many different purposes. Many of your use cases can be satisfied by simply providing what we've got at the moment, which is a mechanism by which the registrant can advertise to the world at large, if they wish to do so, here is how you can reach me if you'd like to do so and I'm ready to receive messages at this address. Accountability is about making that compulsory so that you can lay hands on that person when they do not wish to be found.

Now, I have a question about the criteria issue relating to that compulsory nature. Because I think this whole review must be about the compulsory nature. Because, in my view, the WHOIS is a perfectly adequate means for advertising yourself if you wish to be found. It's only where you don't that the issues arise. Now, regarding the criteria I'd like to ask the panel whether they consider that jurisdiction is a relevant criteria for making my information available. Obviously, any registrant is subject to appropriate authorities within its -- within the jurisdiction where they are. But there are others -- other proper and duly accredited authorities and agencies around the world who nonetheless any given individual registrant is not subject to their jurisdiction. And it may be breaking their laws and has no obligation to do so. So is it the panel's intention so as to assist extra jurisdictional, as in people in separate jurisdiction authorities, to pursue registrations even when the registrant has no obligation to make themselves available to that authority? Or does the panel wish to limit the release only to those who are within the same jurisdiction? Thank you.

CHRIS DISSPAIN: The sounds of silence. Anyone want to take it?

STEPHANIE PERRIN: I'll take the easy bits. And then I'll pass it down the table to someone for the harder bits. Right, Michele?

Obviously, this group cannot harmonize law internationally in six months or whatever less time we have.

However, one of the issues we have discussed at some length is how we set some kind of harmonized standards for how these -- how ICANN functions actually operate and yes, every single registrar that is operating in a jurisdiction is subject to applicable law. That includes, obviously, my particular remit tends to be data protection law and whatever charter of rights applies in that jurisdiction. There's also trademark law. There's umpteen laws.

But the accreditation process that we discussed for law enforcement, hopefully, by going through a door, as an earlier gentleman at the mic pointed out, we can set some parameters for what we're looking for in the accreditation of these requests and channel them through one ICANN process.

CHRIS DISSPAIN: Thank you. We really do need to finish up quickly. So I know there's more to talk about on that issue. And we'll -- I mean, the easiest answer is just get yourself a ccTLD name, and you won't have a problem. Carole.

CAROLE CORNELL: Hi. This one is from Mark. As an old time Internet user and domain name registrant, I always thought I was giving my data for technical purposes. Is it now being provided for a broad array of purposes and even more in the future? Isn't my WHOIS data being repurposed? Is that allowed under the data protection laws?

CHRIS DISSPAIN: Well, we're not going to answer the data protection question. But yes is the answer, I think, in the sense that it has -- yes, you are giving your data for other reasons now. Jim.

JIM PRENDERGAST: Thanks, Chris. Michele and I had an exchange on a previous webinar that you guys had -- Jim Prendergast, by the way, for the transcript. It's beyond your remit. I know your answer. But I want to find out why.

My question during the webinar was we've got ccTLDs who are repurposing as Gs now. Dot LA, dot PW, and others. ccTLDs make up half the domain name registrations in the world. If the goal of this is so important to get more accurate and thorough WHOIS and validated WHOIS, what -- not force it upon ccTLDs, but what can we do to encourage ccTLDs to participate in this new regime?

CHRIS DISSPAIN: So, Jim, I think that's a really interesting question. I suggest you go to the ccNSO and ask them that question and see what kind of response you get.

JIM PRENDERGAST: Will you introduce me?

CHRIS DISSPAIN: I will introduce you. See what kind of response you get. I mean, we can talk about it. It's a sovereign issue and all of that stuff. But I understand your question. Steve.

STEVE METALITZ: Steve Metalitz. I just want to thank Jean-Francois for bringing back into the discussion accuracy. If you look at this in very, very oversimplified terms, the proposal from the Expert Working Group is currently the public has anonymous access, everybody has it, to very bad data. And the idea is there would be some restrictions to access. Not everybody who have access to everything. But in return, or to balance that, the data would be more accurate. So I think it really behooves the working group to stress and spell out in what ways its recommendations would make the data more accurate, who will be validating the data, how will they -- what will be the responsibilities there? Because that is really for -- I think for many people that I represent, that's going to be the selling point is it may be more difficult or there will be some hoops to get the data, but it will be better data. So -- and that, of course, is a core data protection principle as well. So I hope you can stress that as you continue in your deliberations.

CHRIS DISSPAIN: Steve, I know we're rushing, but I have a question for you. Would you accept the proposal that the mere fact that the data is not going to be widely available and open would lead to some improvement in the accuracy?

STEVE METALITZ: Yes. But that is not the answer. That's a cop out to say what was done to make it more accurate, to make it better verified.

CHRIS DISSPAIN: I completely understand. Okay. And finally?

UNIDENTIFIED: Thank you. I'll make it very short. Given the extraordinary amount of data and the improvement in the accuracy of the data, do you think that it will be given for free to anyone or is a certain commercial use of the data to be contracted in a commercial way going to be free or not?

CHRIS DISSPAIN: Lanre.

JEAN-FRANCOIS BARIL: I will start at a very high level. Of course, cost is a major consideration into this analysis and this thinking process. We have not got to the detail where I think we are ready to put some proposal. Overall I think, when we look at the overall value chain of all the elements who are making money or costing money, we need to put that in perspective. Now, I used to say do you agree to pay a little extra money for eggs which are not rotten or not broken? Probably yes. And today with -- you have access to rotten eggs or rotten data which don't exist or are not so accurate. So maybe to access data, we need to think this is a legitimate element of having some cost element here. Total picture is not yet ready, but we are in our journey discussing this point very heavily.

LANRE AJAYI: In addition to that, don't forget a bunch of data elements are going to be made available without authentication, which means you may not even have to pay for it. But there could be some value-added services that may require payments. And that may be good enough to offset some of the costs of operating the system.

CHRIS DISSPAIN: And on that egg metaphor, I think we're finished. Are we? Do you want to take it back? No, it's fine.

JEAN-FRANCOIS BARIL: I think we have many, many other slides. But I think --

CHRIS DISSPAIN: Hang on. It's the how to contact us slides.

MICHELE NEYLON: There's also a couple -- as a group, we are meeting with various stakeholder groups tomorrow, with three different stakeholder groups tomorrow. Not from lack of trying. We're reachable. We're contactable. We want your input. We want your questions. You can grab one of us in the hall, not too physically, please. I don't like being grabbed that strongly. There's all those contact details up there.

JEAN-FRANCOIS BARIL: With that, thank you very, very much to all of you. Thank you also to the Expert Working Group. Unfortunately, for personal critical reasons, five of us could not attend this meeting, in addition to Steve who has been busy in another session. I can feel and sense a tremendous will to help and to support. And this is great. This is really, really impressive. And thank you for being part of the solution. I think this is what we need. We need everyone from the community, as Fadi was saying this morning, to help to materialize a very, very important issue that we are trying to tackle all together.

You know from these slides and you know from us during this week to be in Durban how to contact us, how to access us. There is no proxy here, so we're totally capable to answer whatever is useful for you to be knowing. We had much more slides on the questions that we're posing to the ICANN community. And these will be distributed, so you get access to the slides. So please input also on all the slides that we have not been able to cover today, which are very, very important for us. The journey, I can tell you, continues with a lot of passion, a lot of trust. And with that, thank you very much once again for meeting with us today.

[Applause]

NANCY LUPIANO: Just an announcement: At 4:30 normally there's the session on Internet governance update. You're allowed to take a very brief break, but we're going to start as on time as we can. Thank you.

[END OF AUDIO]