BUENOS AIRES – Exploring Replacements for WHOIS – The Next Generation Directory Services
Wednesday, November 20, 2013 – 08:30 to 10:00
ICANN – Buenos Aires, Argentina

JEAN-FRANCOIS BARIL: I think we need to get started. Unfortunately we don't bring food to this meeting, but a lot of still some good meat.

So very good morning and warm welcome to this EWG next-generation gTLD RDS consultation with the ICANN community. My name is Jean-François Baril. I'm the EWG facilitator.

So for the agenda, we would like today to propose the following items.

After a very brief introduction just to position our work into context, we will give you an overview of where we currently stand with the registration data services based on our latest posted report.

Then we will explain the planning for the next steps looking forward, and hopefully reserve maximum amount of time for interactive and contributing dialogue with the community under question-and-answer format.

This is always very, very precious to us and I think that we will save 45 minutes for this one.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

Regarding the mandate and purpose, just to refresh on what you already know from Beijing and Durban, a year ago both directives -- in fact, this is the first anniversary, almost today -- implementation of WHOIS review team recommendation, specifically this RAA 2013; and redefine the purpose and provision of gTLD registration data.

As such, the EWG was formed and the first face-to-face meeting was in L.A. February 2013, so it has been recommended at this time a clean-slate approach, assessing the needs for next-generation RDS, collective maintenance regarding data, and proposed services solution to better serve the entire Internet community.

Regarding the team, a very critical success factor is to ensure, as always, that we get the best people. Not only to get access to the best experts with deep knowledge of interest of the overall ICANN community, but also maximum diversity in terms of country of origin, community origin, we are thinking including also and we very much appreciate two board members, Steve Crocker and Chris Disspain, acting as a liaison also to the board.

All of them are limited with the best of skills in order to prioritize interest of entire community by opposition to protect, in a selfish way, their own interest.

Also, having the capability to understand consensus.

And above all, all committed to very hard work to tackle an issue which has been said to be impossible in order to contribute for a better future of Internet.

As you can see, this is not only a question of brain -- and by the way, in a big excess in the community -- but rather a more holistic intelligence.

So they are there to reaffirm today that once again, in a very, very humble way, that those members have done a fantastic and impressive work, both from the quantitative and qualitative perspective.

So what has happened so far? From our initial report posted on June 24th, which was the basis for discussion in Durban, a tremendous amount of work to listen, analyze further, refine, test, investigate alternative solutions through analysis of the pro and the cons as you clearly mentioned to us, formal and informal discussions with many of you today in the room. Also understood -- we have understood that the level of the initial report was not substantial enough, far too high-level, because attention to detail is fundamentally important to progress in this so-difficult issue.

We have received 35 public comments and 100 responses to our online questionnaire. A big thank you for all of this input. This is very, very helpful.

As you have noticed from the status report and the response to the public comments, that we have very seriously considered all of them -- all of those suggestions and comments that you provided to us. Unfortunately, we have publishes those two very important reports, the status and the response, only on November 11th. Deep apologies for being quite late. But we have, I believe, prioritized freshness of information and later status on where we are on EWG rather than just the formality.

In any case, I am pretty sure that you have already been very eager to read this 84 pages by preparing this meeting, or at least -- at least been through this executive summary, and that you have understood from this recommended paradigm shift that this status report is strongly contributing to improve privacy, accuracy, accountability, which is also a strong link to the first two, data protection and ease of use.

So now this is my pleasure to introduce Susan Kawaguchi to address on why to replace WHOIS, the goals, accountability, and the data elements.

SUSAN KAWAGUCHI: Good morning. So there have been many -- several improvements recently with the 2013 RAA, but that doesn't fix all of the problems.

The biggest problem we have is absolute anonymous access versus accuracy. People don't want to put their real information into the record if they know anyone can take it and mine the data.

So -- do I have to push this?

So right now, WHOIS, even with these improvements and validation of data, is a problem. We still have limited ability to protect the privacy of individuals, ensure the integrity of the data, prevent use of another's valid contact details. That's a major problem with people taking other people's information and acting as that entity or individual. And also conforming to the many different data privacy regimes.

So it also lacks security features, auditing capabilities, and a consistent interface.

Having the data be consistent across the board would be extremely helpful just in looking at the data, but also being able -- you know, conforming to a central database.

So let's see here.

When we started, we started by reviewing all of the data -- the uses of the data in the current WHOIS and possible new uses. There -- you know, as technology grows and develops, there's new things that we might want to add to this -- to the record, the data that's in the record for domain name registration, and so we started looking into all the use cases.

And luckily, with our first report, many of you came back and -- and said, "Well, what about this and what about that?" So we've taken another look at what the data could be used for and what data was in the record and what data was missing, frankly.

As a -- I was formerly a member of the WHOIS review team, and on that team, although we had a large mandate to look at the WHOIS, we could only look at the current WHOIS.

So by joining this team and taking that knowledge and expertise that I gained there, it's refreshing to look at this with a clean slate and to be able to imagine what could be, for this record, instead of what is and what we're limited to.

So we've -- we constantly remind each other to, "Look, we don't -- we're not sticking to the old WHOIS. We're going to come up with what we need for 2020 or 2030, really, something for the future, but which will work today."

And so that forms our discussions.

We're going to provide an overview of the principles that we actually came up with for this. The very first topic that we focused on -- oops. Thank you. Sorry.

We identified the users of the registration data and why they needed it. You'll see the summary list on this slide.

We also realized that with all these uses, with all these different -- identifying the different needs and use cases, that we would also need policies and processes to accredit the permissible uses.

So if someone needs the -- the data, we need to look at why they need the data, what they're going to do with the data. And policies and processes are something we discuss. We haven't determined those.

So that -- the list of all the different use cases, all the different -- the data users continues to form our discussion.

So we've also -- in this slide, accountability is one of the key principles we've discussed. Why does somebody need the domain name registration data? Why is it in the record to start? Is there a purpose? We looked at each and every data element for a purpose, and we discussed it in detail. Is there one purpose? Is there more than one purpose? And if there's only one purpose, should we really include that?

And we came to the conclusion that, yes.

So we're also -- we need current accurately timely registration data, and that the -- there should be a contact in the data that is always reachable for -- so if there is a problem with a domain name, that someone can be contacted immediately and the problem resolved.

Mostly, those would be technical issues, but it's very important on the Internet that each and every Web site or any use of a domain name on the Internet, that someone is responsible for that.

And that there should be repercussions for misusing that data.

If the data is mined, right now we can't tell what people are doing with it. Some -- some of those instances, we -- we can see in the -- you know, or experience in the broader Internet use, but it's not always apparent what people are using the data for. And by designing a different data record for the domain registration and how it's accessible, then we could -- we could -- we would gain some knowledge of how people are using the data and why.

So, once again, it was purpose data collection, and we identified all the purposes and we established criteria to recommend which data elements should be mandatory or optional, and that took a lot of discussion, you know. Should this be available? Should it be mandatory to collect? Should it be mandatory to reveal, to show in the data? Does the registrant have the choice to make some of this available to the public, make it all available to the public, or not -- or very limited?

So all of those discussions were in-depth.

So if you read the report, which I know it's long but there's some good information there, we tried to answer these by recommending principles and rationale for data collection and disclosure, using those principles to classify all data elements, mapping data elements' names to those in the 2013 RAA, and providing examples to illustrate those proposals.

So we've tried to tie together all of our work from identifying the purpose of the data element all the way down to how it works with the 2013 RAA and the policies and processes that we think might be the use cases for these.

So Rod, I'm going to hand it over to you.

ROD RASMUSSEN: Thank you, Susan. So I'm going to go through several different elements here of the current work and do -- well, actually I need to change the slide here, huh? There we go.

Oh. The -- I would also make sure to point out this is still a work in progress. We're taking input for a lot of these things, but we're working through some really exciting stuff, I think, on how to deal with data validation and other topics I'm going to talk about here shortly.

We have put out, in this report, some new and if you -- if some of you have been around for a while, as many have, rather old concepts around data validation -- or at least the concept of how contact data is managed, to support data validation.

And the first part of this that I'm going to talk about talks about this concept of a data validator, which could be a registrar, which it currently is today, it could be a registry or some other third party which actually validates contact data.

The idea would be to have data validated at initial collection, whenever updates are made, and then periodically potentially through audit -- an audit -- regular audit process.

The -- this goes well beyond, I think, the 2013 RAA in the way we're proposing doing this, as well as adds this concept where you, as an individual or as an organization, have control over your information, not just in the one particular domain registration but throughout the system.

So you would be able to submit contact information, have it validated -- pre-validated for a first-time use, but then again kept updated not just for that one domain but for any domains that you happen to be working with. And for large domain portfolio holders or ISPs or abuse contacts or things like that where your role can cross hundreds, thousands, tens of thousands of domain names, this improves accuracy tremendously.

One change is reflected throughout the system. That is the -- the concept we are trying to get at here, to create both better accuracy and much better efficiency for everybody in the ecosystem.

The next area I'm going to talk about is in disclosure.

Obviously, if you have more accurate data, it's incumbent upon the system to be far more accountable when it comes to disclosing that data, protecting that information.

So the -- the new paradigm we're talking about here, this is the ability to access the information, is -- now, as we've discussed, I think, before, has got kind of two elements where you have a publicly available set of information available anonymously and a gated set of information which is available through a more rigorous set of access controls.

But the -- the overall elements available anonymously will continue to be provided, will include many of the various things that would be seen today as being from the registry, kind of metadata, if you will, and other items will be gated behind that.

And again, as Susan was pointing out earlier, this will be purpose-driven, as far as how access is granted to the system.

The gated data is the data that is identified at greater risk of misuse and requires protection.

The entities that would be able to get at that data would be authenticated and authorized to do so for the permissible purposes that they have designated that they are trying to use the data for.

So in order to do this, we've proposed before and expanded upon that in the report the idea of how you would credit various users of the system. I think this has been an area of discussion and feedback for us that has -- we have been very keen on getting input to.

We've worked with a lot of different people in various communities to get their thoughts on how we might do various sorts of authentication for people accessing this data. Some promising things there.

I'd like to point out that one of the, I think, thoughts that people have around getting at data and getting accreditation is that in all cases, it needs to be -- or in most cases, it needs to be instantaneous or, like, right away. One of the things that leads you to is the concept that this system must be extremely robust and we have to have this very large effort to accredit a lot of people ahead of time.

The act -- but looking at the actual use of this kind of data and many of the use cases that access does not have to be in, quote-unquote, realtime or accreditation done in realtime. So that's one of the things that we've kind of teased out from this, in that an accreditation process or a request to get information could go through a process where it is done in a more -- less than realtime fashion, I guess, in a -- have a request process and have that approved through a -- some sort of a validation process that then leads to data disclosure at a future time. That's an important thing to remember. We are not trying to build necessarily a way of doing this so that everybody can get access to any kind of information instantly.

The other key here, too -- just from the model, you can see, the diagram there, is that the RDS system itself would be responsible for providing the anonymous access and the gated access -- the gated access would obviously be through a far more sophisticated system using something like the RDS that's being worked through in the IETF process.

To bring this kind of home, there's a couple of -- there's an example here. And I'm sure that is probably too small for many people in the audience to see. Okay.

Apparently, I'm not loud enough so I will get a little closer to the microphone.

The record here is -- shows different types of data elements that could be published both in an anonymous request so they will always be public and those that may or may not be gated depending on the preference of a domain registrant or that particular role based on the purpose and the type of contact they represent, there are many more examples, I believe, in the report, in the appendix.

I encourage you to take a look at some of those and give comments on that. The idea here is in different types of access, you would get access to those different types of data elements.

And I already mentioned that for consistency, we will have all of this going through a single point of access. That's the recommendation. Again, these are all recommendations. And the reason for that beyond making that obviously efficient and providing a very simple method of doing is it would allow you to promote accountability and the tracking of sort of how people are using data and the purposes they are putting it towards would be accomplished from that point where then, of course, if you have somebody abusing the system, you have the ability to impose some sort of sanctions. And it also simplifies in theory at least the ability to accredit various entities where you have an accreditation scheme or you can have different types of communities being accredited through there community method but the accrediting of the accreditor, so to speak, would be through -- at least have a root at that level. And then I already mentioned we would use, existing protocols in order to carry this off.

That concludes my section here. I will let Stephanie take over, I believe.

STEPHANIE PERRIN: Hi, I'm Stephanie Perrin. I am going to be very brief because we need to make up some time so that you will have time at the mics. So this will be a brisk trot through privacy. But I would encourage you, I'm around until Saturday morning. If you have questions, please, I would be happy to discuss further.

So basically in addition, of course, obviously applicable data protection law has to be observed. That would be your first floor of data protection.

We have looked at privacy and proxy services. We're proposing to change the name for privacy services to shielded services for greater clarity.

And we are -- we have some details in the report about what data elements would appear in the directory using these services.

We have proposed a secure, protected credential system that would enable domain registration by individuals who have genuine threats on their health and safety. There are proposals in this report for how -- the kinds of structures that would have to be set up to facilitate this. The technical end of providing pseudonymous credentials is the easy part. It is the attestation for the groups that would be eligible to receive these credentials that is the hard part.

And another element that we have proposed which I'm discovering may not be well understood in this community, which there's not a whole huge amount of depth of folks who've dealt with international data protection harmonization issues at the nuts and bolts level, and that's really what binding corporate rules are. They were a proposal for global corporations to harmonize management practices to protect data.

And we are thinking that would help protect -- whichever model we choose for the registry, it needs to be protected the same way across the different feeder schemes. So that -- that was the proposal. And I'd be happy to discuss that further with you.

FABRICIO VAYRA: Good morning. Can everybody hear me okay? First off, thank you guys for being here early in the morning. We really appreciate it knowing that you guys actually care about this. This is great. And we're not the only ones just here in the room talking to ourselves. I really, really appreciate that.

So we're going to go over some of the models. And I assume everyone here read our initial report and understands in our initial report we had proposed an aggregated model. No surprise that we received a lot of comment on the aggregated model proposal. Some really strong support, some who suggested we should not have an aggregated model report, aggregated model.

But one thing that was really highlighted from the comments we received back is that we needed to do more to show what analysis we had done to reach our recommendation and to actually put on paper all the hard work that we've done up until then and going forward based on the comments.

So what have we done since receiving the comments? Well, we really expanded and deepened our analysis that we had from our prior report. The update now contains a comparison of six different models that you see here up on the slide and really shows the criteria that we used to compare all the different models. The criteria includes security, jurisdiction and privacy, accreditation, operational impacts, including performance, implementation and some operational costs.

In these models, what you will see is that we compared our regional models, bypass models, opt-out models to WHOIS.

In the end, what we've come down to is we've focused very heavily on two models. And that's a result of the work we've done up through our initial report and as a result of all the great comments that we've received as a result of our initial report.

So let's go through some of the models real quick, the two in particular, the aggregated model from our initial report and then the federated model. Let's talk a little bit about what these models do and what the differences are.

I think the differences are very important to highlight in particular because what we hope you will find is that in looking at the federated model in particular, it's meant to address a lot of the comments that we received to our initial report.

So the aggregated model, just to sum up, what it does is the registrars collect data when a registrant registers a domain name. The registrar then sends that data to the registry for storage, and then the registries would push up that data periodically to make an authoritative -- holistic I should say, copy, excuse me, at the aggregated RDS.

Every time a user wanted to get access to data, they would either anonymously to get certain pieces of data or through a verified gated system always go through the aggregated RDS. And that's what would be the interface for all data.

Now, the federated RDS really came about as a result, as mentioned, your comments. And the difference here is that the data still flows from the registrant to the registrar to the registry but then that's where the information stays. So in essence what we end up with is what we would end up with in the -- what seems to be inevitable, the thick WHOIS model across all registries, what the RDS would do would be the holistic interface for everyone trying to access that data. It won't prevent registries from offering their own interfaces should they want it or services based off the data. But all outside users, both anonymous and verified, credentialed through the gated system, would operate through the RDS which would have a realtime access to all the different registries.

So the main difference here is that there is no copy being sent up through to the RDS. And we're going to talk a little bit about jurisdiction in a bit. But if you think about this, this is just one example of how a federated model answers some of the questions that you sent in. It starts to answer some questions around jurisdictional issues because at this point, the data stays and remains at least from a storage standpoint at the registries. We still obviously have to tackle things of data in transit, stuff like that.

And then I pass it on to Carlton, I believe.

CARLTON SAMUELS: Good morning, everybody. Let's talk about some of the jurisdiction concerns and applicable law. We would recognize that from the initial report, we took stock that there were jurisdictional and applicable laws pertaining. And there were some local differences that we would need to adjust in terms of data protection and privacy regime.

Since that time, we worked to get a better understanding of the challenges posed by the jurisdictional considerations. And we have looked at some approaches that potentially address and accommodate some of the conflicts in applicable law.

We've done some updates to the report. And if you read the report, you'll see there extensively documented.

But the findings, if I could summarize them for you, the jurisdictional concerns, they're not unique to the RDS. They exist today. And they will be magnified with the new gTLD program. Recall that we know of about 20 gTLDs with expansion in the gTLD space. We will have many more interfaces. So you need to think about scaling, how the system would scale.

The WHOIS waiver process now used by registrars to resolve conflicts, it's just not adequate. It will not scale. We know this. And with so many jurisdictions, we have to find a new method.

So ICANN is not a treaty organization, but what you need is some kind of framework that is akin to treaty. So we thought binding corporate rules might be a way, might be a way to raise the level of data protection for -- by the RDS and improve the standard across all jurisdictions. So that's where we are. It's still a work in progress. And we hope that you will work with us to further define where we go with that.

FABRICIO VAYRA: All right. Seeing our initial report and seeing the update, which is 80 plus pages long, I think it's clear, if it wasn't already, that reinventing WHOIS is a difficult task. We hope that the direction that we're headed, some of the recommendations both posted in our initial report and as seen in the update, are a real reflection of the comments we received, puts us in a better place, and puts us in the right direction.

But as Carlton said and as we heard Jean-Francois introduce, this is a real work in progress that I think needs continued interaction with the community. We've benefited greatly from your comments. And we want more of those comments.

So to start with, thank you for everything that you did up until now. It really helped, and you will see our update really move further into the right direction.

We hope that this update clarifies some of the things that we had put in our initial report. The initial data shows how we drilled into things previously and how based on your comments, we've continued to drill in and refocus on different models.

It's really meant to be a dialogue. And so although it's a thick -- thick report and you probably haven't had enough time to read it, those who have had time to even read parts of it, we hope that's been a good basis for dialogue up until now. We're not stopping there.

After we have this Q&A session during this period, we're also having a session this afternoon which is really meant to be a workshop, roll up your sleeves, let's go through all the different topics. And we really want to hear from you and interact with you so we can take that feedback and continue to form things.

We also have an open email address that you can write to us. That will be open until the end of January of Q2 -- Q1, sorry.

And so what are we going to do going forward? We're going to go ahead and look at the -- continue the dialogue. We're going to look into certain topics for research including validation, accreditation, the different risk and impact that our proposals are having, different proxy practices. We're not trying to reinvent the wheel. We're trying to do some best practices here.

We're going to take all that information and all the comments that you gave us today, this afternoon, through the emails and we're going to reconvene, examine all that data, and hopefully by -- after ICANN 49, we're going to go ahead and put out a final report that will feed into the process, into the PDP process, board, et cetera.

So here's the data. You know, interact with us at the workshop. There's the time and location, the mailbox that you can submit your ideas to us. And then you can see all the feedback that we received, and comments, on the link here. And I believe this will be posted, so that if you don't want to write this down or take a picture of it, you know, you'll be able to find it somewhere else.

But please, please give us your feedback because it's the most valuable thing to us in our work.

CHRIS DISSPAIN: Okay. Thanks.

So now it's your turn, I think. I hope.

You can give us your feedback online but you've also got an opportunity to come to the microphone right here, right now, and talk about whatever you want to talk about.

But we're going to put a little bit of structure to it, if you don't mind.

Can I get the next slide up, please, whoever has the clicker? Who's got the clicker? Cool.

So the first two topics we're going to talk about are improving accountability and improving quality.

Here are some sort of questions for you to think about. You don't have to answer the questions, but as thought starters: Does the proposed data collection strike an appropriate balance? Must legal persons make more data public? What organizations might accredit RDS users?

And on quality, it's: Would validation proposals address the causes of inaccurate WHOIS data? And are there benefits, limitations and impacts of reusable contacts?

There's going to be plenty of opportunity for open questions as well so if you have other things you want to say -- Wendy, Mike -- but does anybody want to talk to those two things?

If you do, come to the microphone.

MICHAEL PALAGE: Mike Palage. So I guess this goes to quality, and in -- first off, great work, Herculean task you're undertaking. I'd like to talk about some of the new fields that you're proposing to incorporate. Specifically, registrar and registry jurisdiction. And I guess this goes to the quality point.

What I was struggling with as someone who's been involved with registration authorities over the last 15 years, have been involved in litigation, that jurisdiction thing kind of jumped out at me. And is that just meant to be exclusive or your principal incorporation? So again, I look at someone like an Afilias. Incorporated in Ireland, has different subsidiaries in India, in the United States, in Canada. And I'm just mindful of how, when something works itself into an ICANN obligation or a contract, certain people will begin to interpret that as having legal significance.

So again, if you could perhaps expand or share a little on what that means or what you were trying to get out of that, that would be helpful.

CHRIS DISSPAIN: Thank you. Does anyone want to talk to that? Carlton?

CARLTON SAMUELS: Yes. Yes, thank you, Chris.

It really is a -- if you noticed, I said that because the registry -- where the registry is is going to depend on jurisdiction and applicable law.

Sometimes some of the purposes for which registrant data is collected has some impact on the applicable law and jurisdiction, so you need to have a sense of what applicable law is and what jurisdiction.

So this is informational. You start with that before you go anyplace else. That's the idea.

CHRIS DISSPAIN: Fabricio?

FABRICIO VAYRA: Yeah. And, Mike, let me just say that I think actually, the points you just brought up probably took up three to four hours of our time just -- I mean, precisely for what you're saying.

So again, work in progress and definitely it's one of the things that, you know, we're wrestling with.

CHRIS DISSPAIN: Mike, can I ask you a question?

So if I understood you correctly, what you're saying is that it's challenging because you might be in multiple jurisdictions or there's another problem?

MICHAEL PALAGE: So let -- perhaps this could hit home a little more specifically.

If you look at ICANN, who itself has been named in litigations over the years, it has always stated and argued that it only could be sued in California. So it's always tried to get out of other jurisdictions and get that transferred back to California.

CHRIS DISSPAIN: Right.

MICHAEL PALAGE: So I just think as ICANN looks to internationalize, recognizing that this industry does have a global footprint, I'm just mindful of what that means and what legal significance other people may seem to impart upon this data.

Because what we've learned is people will take this data and try to impart upon it different legal significances, so I think if you do require this, it would be really helpful to explain what it's for or what it means or what it doesn't mean.

CHRIS DISSPAIN: Okay. Because if I'm a corporation and I know that I'm making a choice by putting a jurisdiction into the WHOIS that is actually going to be jurisdiction from the point of view of legal -- for legal reasons, I might choose a different jurisdiction.

MICHAEL PALAGE: Correct.

CHRIS DISSPAIN: Okay.

MICHAEL PALAGE: And just to, again, give a real-life example, for a long time a lot of the litigation involving dot com names were brought in the Eastern District of Virginia because that is where the servers were located. There was a lot of litigation that then began to go where -- out to the Ninth Circuit because that is where VeriSign's corporate headquarters at the time were located.

There is a difference in legal interpretations of whether domain names constitute property in the Ninth Circuit --

CHRIS DISSPAIN: Right.

MICHAEL PALAGE: -- whether they constitute a service in --

CHRIS DISSPAIN: Yeah.

MICHAEL PALAGE: So these are things that have real-life ripple implications, and I'm not saying it's a right thing or a wrong thing. I'm just trying to raise that.

If I can, one more thing on improving the quality of data, and this has to go to the original registration date which you have proposed to be collected.

And you say "the original registration date" meaning the date that the domain name was first ever entered into the database. If it is later deleted and then reregistered at a period in time in the future, you still want that original registration date.

As someone who has been involved in transitioning registries from back-end providers -- I was involved when PIR mitigated from VeriSign to PIR -- all of that historical data from VeriSign was lost, and as we move to a market where registries will begin to mitigate, I think it's important to realize whether that actually will be able to be accounted for.

And also, from an operational standpoint, if some -- if a domain name is added within the add-grace period, does that mean that it was entered into the database or does that data only kick in once it's matured into a full registration?

So again, not being critical. Just trying to highlight some questions from an implementation and operational standpoint.

CHRIS DISSPAIN: Yeah. Thanks, Mike. Stephanie. Sorry.

STEPHANIE PERRIN: I just want to add to that. In terms of complexity, it's an oversimplification to say that the RDS is where the applicable data protection law would go. That's not a given at all because as you say, it's different and it will depend on the jurisdiction. It might be where the individual is in some country law.

So that's why we went for the binding corporate rules, to try to at least regulate that up to the same level so we had consistent practice.

MICHAEL PALAGE: Keep up the good work.

CHRIS DISSPAIN: Thanks, Mike. Wendy, you're next.

WENDY SELTZER: Thanks. Wendy Seltzer, and, yes, I will have plenty of comments later on, but here, in particular on the question of validation's relationship to quality, I think it's important to note, as you do in places, that, you know, validation is only one of the reasons for low quality, and so improving the privacy protections both through the gated access and through alternatives is as important as the validation.

CHRIS DISSPAIN: Next slide is privacy, so we're coming to it.

WENDY SELTZER: So -- yeah. And you note in a footnote that the working group is considering how many fields to require validation on. My recommendation would, as you might expect, be a very minimal number there because of the costs of those validations and -- both on individual privacy and in monetary costs and the costs to --

CHRIS DISSPAIN: Okay. I might have a question for you when we get to privacy, if that's okay.

WENDY SELTZER: Sure.

CHRIS DISSPAIN: I put you on notice that I have a question for you. Garth?

GARTH BRUEN: I'm sorry if my question doesn't fit into these categories.

CHRIS DISSPAIN: That's okay.

GARTH BRUEN: Okay. I already spoke to Carlton the other day about the language aspects so I'm not going to ask about internationalization.

I do want to talk about the technical aspects, and I'm wondering if you have spoken to people who write third-party software that works with WHOIS or specifically with WHOIS clients. Because I've actually spoken to a number of developers around the world who have built tools for Linux, have built tools in Perl and C and other implementations. They're not even aware that this project is going on. And they're starting to get concerned that what they have built for the underlying structure, for the glue that holds a lot of the Internet together, is going to break.

So I'm wondering if this is something that is coming up in your discussions. Especially in terms of Port 43.

CHRIS DISSPAIN: Rod?

ROD RASMUSSEN: Sure. Thank you, Garth. Yeah, we've -- well, Scott Hollenbeck is actually on the expert working group. Unfortunately he couldn't be here and he's deeply involved in this at the IETF level, et cetera, and certainly looking at what fields are presented and how they're presented and all that has been a consideration in this along the way.

The display of data and the production of data we're looking to provide in a very standardized way, and it actually should improve the ability for people to access and parse new data on an automated basis. Obviously within purpose and through accredited -- you know, at least if we're talking gated elements.

So I think in the long run, we're talking about a much more robust system.

In the short term, there may be some transition issues that we run into, but we're not talking about doing this overnight either.

I would posit that it's going to be well-documented, well-publicized. We're going to be moving and evolving the system to use this and it will be using, you know, standard XML libraries or JSON or some sort of things that are, you know, very standard, very easy to use. So I think those concerns are definitely part of what we've talked about and we'll be offering some recommendations specifically about that, if we haven't already.

GARTH BRUEN: Yeah. I just --

CHRIS DISSPAIN: Hang on. Michele, you wanted to say something and Fab you wanted to say something. So Michele, first. Then --

MICHELE NEYLON: Yeah. I'll just keep this brief.

With respect to the replacement of the WHOIS, I do understand where you're coming from. There has been some discussion in the IETF about offering some kind of clients that would act as a kind of middleware between current WHOIS clients and a replacement for WHOIS, because the replacement-for-WHOIS discussion has been going on for some in technical circles, as you know. I mean, we're on the same mailing lists, Garth. So, I mean, you know, it's not that we haven't had these discussions. Our proposals here would be to lean on the work in the IETF and what we've been looking at is, you know, working with them in terms of, you know, what's supported or what isn't supported, but the kind of third-party stuff, the IETF is dealing with.

GARTH BRUEN: Yeah. I just think we may need some sort of outreach because these guys and gals wrote this stuff 10 years ago and it just works.

CHRIS DISSPAIN: Yeah.

MICHELE NEYLON: Well, if it's written well, it will probably continue to work, but not all of it just works.

I mean, some of it doesn't work when you launch a new TLD because it's incapable of doing a lookup to find the servers.

I mean, it depends which version of Linux you use, you know.

CHRIS DISSPAIN: Let's not get into too much detail. Fab?

FABRICIO VAYRA: Yeah. I was going to ask, I'm glad you came up to the stand and -- the mic, and is there any way we can lean on you to energize those folks and give input in?

And here's why. We -- we end up in a little bit of a conundrum if we're going to do risk assessment, impact analysis, because a lot of that deals with cost, and if we have the intel from your folks and yourself, it gives us ideas of what's already out there. I mean, we've already said we don't want to recreate the wheel, and so in any way we can lean on existing work, we want to do that, especially if it works. And that will help us a lot analyze. And cost.

GARTH BRUEN: Yeah. You're not reinventing the wheel but you're replacing the spoke and the wheel might fall off.

Because some of this underlying technology, you know, like I said, has been -- was written 10, 12, maybe even 15 years ago, and, you know, the people who wrote it, they've left it alone and they're very happy with leaving it alone. And these are open source folks, free software folks, and you'd be surprised at how much other stuff out there relies on its work.

CHRIS DISSPAIN: Yeah.

GARTH BRUEN: And I don't think we -- it hasn't been tested and that's what I'm concerned about.

CHRIS DISSPAIN: Okay. Thanks, Garth.

Just one second. I'm going to just run through the other topics because there's no point in us trying to keep to one topic. It's not going to work. So we've got accountability quality, privacy, jurisdictional considerations, the models themselves, and support for technical protocols.

So you -- let's just have an open discussion about any of those or, for that matter, the color of the carpet. Maria?

MARIA FARRELL: Very nice carpet.

Okay. So I've got a couple of points to make. I suspect they may be issues you've struggled with already but I just want to raise them again I suppose. "Must legal persons make data public?" I think there's a global movement for greater transparency of corporate data, and -- for reasons of tax avoidances and such, so personally I would think yes, they should, and few people would object to that.

"Which organizations might accredit RDS users who need gated data access?" I think that's a really tough one, because how -- what's the business model for that? How are you going to make, you know, an organization that can accredit all sorts of people around the world and actually make money out of it? I'm going to give an example.

Last year, I was the -- well, I still am the wife of a soldier but he's no longer a soldier. So last year I was the wife of a serving soldier who was in Afghanistan, and there were very -- and I was blogging about it, and there were very, very clear rules of the British Army and the MOD about, you know, you're not supposed to say where you live, it shouldn't be publicly disclosable data. Now, if I want to blog about that and have a WHOIS record, obviously I can't do both of those things at the same time.

That's difficult for me, but I think it's difficult for you because how do you go about for, say, those seven months at a time accrediting me as a British Army wife?

Because I'll tell you what, our welfare office is too busy dealing with, you know, guys coming back with no limbs. They're not interested in WHOIS records and that sort of thing. And that's just a really -- you know, that's just a small, almost silly example. This is really hard to do, it's really expensive to do, and it's almost impossible on a global scale.

And finally validation, and I think validation is really difficult in terms of addresses. I know Michele and I were speaking last night about how, in Ireland, I mean, my dad gets letters that come to "Paul Farrell, Cary" and that's -- you know, we don't have postal codes. We don't do anything like that. We have large town lines.

In Ethiopia, I've done some work. Basically you don't have an address. You get told "Go to where the near -- where the large Coke sign is and go near there and ask somebody." I mean there aren't postal addresses. And that's a major -- that's the capital city of a major country in east Africa. So that's a problem.

Finally, just a question or a suggestion.

I am the GNSO Council liaison for the PDP on privacy and proxy accreditation services and there's some terrific work in your report about it and I know a couple of people from the EWG are going to take part. It would be great if we could call on you to provide some of the input and background information you already have provided in this report to help our deliberations as we go forward. Thanks.

CHRIS DISSPAIN: Thanks, Maria.

Very quickly, Michele.

MICHELE NEYLON: You know, just thanks, Maria. I mean, the PDP and our work here, I mean, the two should work together. I mean, this is one of the things that the GNSO Council has brought up. We're all conscious of it. Duplication is just a massive waste of everybody's time. So the more we can actually cross-fertilize, the better.

CHRIS DISSPAIN: Thank you. Sir?

ALEX DEACON: Hi. My name is Alex Deacon and I just have two clarifying questions, first for Rod on data validation.

You had mentioned that data validation is about the format and then there's operational and then optional identity validation.

Can you kind of dive in on what you mean by "operational data validation"?

ROD RASMUSSEN: Sure. This is from SAC58, SSAC58, which we did a -- I'm a member of SSAC as well, and we did a -- basically a taxonomy of validation --

ALEX DEACON: Okay.

ROD RASMUSSEN: -- and released that I think about a year ago or so. Maybe even less than a year ago. And the idea there around operational validation is actually being able to establish that so, for example, an e-mail address works --

ALEX DEACON: I see. Okay.

ROD RASMUSSEN: Or a telephone number works --

ALEX DEACON: Works. And someone is at the other end.

ROD RASMUSSEN: Yeah.

ALEX DEACON: Okay. So I'll read that SAC.

And just one other quick question to Fabricio.

You were talking about the federated model and you were talking about registries in that model could still provide direct access to their data. I wasn't quite clear what you meant by that.

Is that above and beyond access via the RDS or -- or in addition to?

FABRICIO VAYRA: Yeah. We're just basically saying that, I mean, the data would be there so if there's -- if they wanted to have a portal themselves, they could, but -- just because the data is going to be at the registry level in thick. But for -- you port as you need it, and basically anybody who was validated or needed validator credential data would have to go through the RDS.

ALEX DEACON: But they would still be -- the rules -- the authentication and authorization rules would still apply to that level?

FABRICIO VAYRA: Yes.

ALEX DEACON: Okay.

CHRIS DISSPAIN: Okay. Steve?

STEVE METALITZ: Good morning. Steve Metalitz with the intellectual property constituency.

I want to thank the expert working group for all the work that you've put in and all your efforts to respond to many of the concerns that were raised, or questions that were raised in the initial comments. I don't think anyone's really had any time to review what you've published in any great detail, but we look forward to doing that.

I have a couple of questions, but the first one, I guess, is relevant to what's on the screen and that's on reusable contacts.

It wasn't clear to me whether you were proposing that this would be the -- the only path for registrants or whether it would be an optional path.

I can see the advantages of this for large portfolio -- holders of large portfolios of domain names. I think the domainers should be giving you an award for this because they will benefit tremendously from it. But I'm not quite sure the -- that it would appear the same just to an individual or somebody with just a few.

So that was my first question is: Is this intended to be mandatory or optional?

ROD RASMUSSEN: So it's kind of both and I'll explain why.

From a system perspective, it would be mandatory. From a "how a user actually interacts with the system" -- so say you're an individual user and you go to a registrar and I want to register one domain name, that would all be kind of background stuff, right? Basically the user interface would assign you a credential and all that. You could use it optionally, but the theory here is that you're managing a domain through your registrar and you would not really notice that there's this contact management thing, unless you wanted to take advantage of it.

So it's really more of the implementation side would make it fairly optional.

But from a systems perspective, the idea here is you would have that contact handle -- if you remember the old (indiscernible) handle -- and whatever the scheme would come up with, and we've actually been talking about how to make that work so that you can move that from registry to registry and registrar to registrar and use that across the entire system. That would all be baked into that, and then you could take and manage that if you ordered another domain name somewhere else. You could actually pull that information in and manage it from there as well.

STEVE METALITZ: Thank you. That leads me to my next observation. As I said, there will be a lot of issues we will want to comment on. But one thing that really brought me up short in this document was on page 14. And I think you basically recapitulated it in a slide where you listed what data elements would be accessible to members of the general public who make a WHOIS query. And it is pretty shocking that there is only four of them or five of them. One of them will be meaningless because it is that handle. It doesn't really tell an individual user anything. That's just a number or string of characters.

Now, I understand you're working on a clean state here. But the reality is that ever since we've had -- since before we've had the worldwide web, certainly ever since we've had it, members of the public have been accustomed to having this window into who's accountable for activities on the Internet. And it's got many flaws and many shortcomings. And I understand that there will be a gated access path, and many people will use that or many people could use that.

But I just think our suggestion in our comments was that as you withdraw material from the public domain, you should explain why that was necessary to do that in your clean slate. I don't really see that in the report so far. So I'm just kind of suggesting that as a headline, you may find a reaction that this is a proposal from ICANN to shut down public access to the Internet. So since that is not your intention, I'm sure it's probably important to explain more why you're recommending that so little information about domain name registrants be available to members of the public.

CHRIS DISSPAIN: Steve, thanks. I only want to comment on it because we have ten minutes to go. And I want to get through the queue. Otherwise, it's not fair.

It is a fair point. But just to give you an example, we publish in Australia in our WHOIS even less data than is being suggested. So there are different levels depending gTLDs and ccTLDs, okay?

But if it's okay, we need to move through the queue. So thanks, Steve.

Wendy.

If I could ask you, I know you have got a lot of things to say. We really do have to speed up. Wendy, off you go.

WENDY SELTZER: Thanks, Wendy Seltzer. I want to thank you for the additional analysis in this part, particularly the risk-based analysis that appears frequently and I'd like to urge you to go even further in that direction of analyzing the risks to various parties of having to collect this data of having to keep it safe against potential data breaches. So the secure, anonymous credentials offers one way for everyone in this system to limit their liability for having lots of data around that could be spilled.

I also wanted to ask a question very specifically about some of the different steps in reveal and take-down that you spell out around proxies and particularly when you spell out some of the hierarchy of responses that a proxy provider could take -- say, reject the reveal, positively affirming the proxy's liability for further domain use. And as I've asked before about various provisions in the RAA, I wonder sort of by what right does ICANN have to impose that liability on the proxy provider and liability to whom.

CHRIS DISSPAIN: That's not a WHOIS question. That's a legal question.

WENDY SELTZER: It appears in the WHOIS report.

CHRIS DISSPAIN: I understand that.

[Laughter]

The reasons behind it, I mean. We need to be really quick.

MICHELE NEYLON: Wendy, some of this stuff we're still working through. I think one of the -- this is why there's the PDP on privacy and proxy, which will also take some of the stuff we've done, stuff that others have done in the past and tried to get it to a point where it works better for everybody. And these kind of questions of liability, yes, they're important.

As a registrar, I don't want to be liable for stuff that I'm not directly involved with.

CHRIS DISSPAIN: Okay. Did you have something else?

WENDY SELTZER: Great. I will look forward to talking with you further about --

CHRIS DISSPAIN: And you will be putting --

WENDY SELTZER: -- the protections -- (multiple speakers).

CHRIS DISSPAIN: And you will be putting comments in, I would imagine.

Thanks, Wendy.

Kiran.

KIRAN MALANCHARUVIL: Thank you, Kiran Malancharuvil from MarkMonitor. I want to applaud and thank the Expert Working Group for their work on this, especially the privacy proxy piece.

I wanted to thank you for your work on expanding upon -- upon the legitimate uses for privacy and proxy services, and I wanted to encourage further attention on our advocacy point which we've communicated in our comments and we'll communicate further about a commercial and noncommercial distinction to be sure that in the case where there is a commercial actor where they're accepting donations, where they're selling products, in order to protect consumers and protect consumer trust and confidence and their rights in the marketplace on the Internet. We want to make sure that the information about registrant data is always public in those circumstances. And so thank you for that opportunity.

CHRIS DISSPAIN: I think that's a really interesting point, and we have discussed it. It raises some interesting questions, which is how do you know.

You tick a box that says you are, but you might tick a box that says you're not. It is a huge compliance task, but I agree --

KIRAN MALANCHARUVIL: It is a herculean task, and we appreciate that. And we think it is very important to protect consumers. And so we appreciate your work and your support on that.

CHRIS DISSPAIN: Thank you. And, Mathieu, the last word from the audience goes to you.

MATHIEU WEILL: May I have the last word?

CHRIS DISSPAIN: The last word but not the last word.

MATHIEU WEILL: Mathieu Weill, CEO of AFNIC, manager of dot fr. I want, first, to acknowledge the work of the working group. I am very pleased to see that the aggregated model has been put in perspective with the federated model. That was one of our recommendations, and I look forward to further discussions. I have a lot of detailed questions on that that I won't bore you with right now.

I'm also pleased to see you are considering ccTLDs as a this model. Chris, we are very sensitive to this.

We think dot fr is an interesting model. We have some shield services coming along. We can definitely share even cost things with you with pleasure.

My question is actually a clarification question. I have read part of the report. I tried to find the answer, but I haven't been able to. I struggle to understand how you address the jurisdiction issue and what you mean by "corporate binding rules" or something. I'm not a lawyer, not even a U.S. lawyer. And I'm totally at a loss to understand how you basically address the issue of is a government from another continent going to be able to access according to its jurisdiction data from registrants who are on the other side of the world and why. Depending on where the aggregated data is, how can we address -- how do you plan to address this?

I think you have to realize this is going to be the way -- this discussion is going to be framed at least in the GAC. And I fail to see the answer in the report. It may be underway, but I'd like to have clarification.

CHRIS DISSPAIN: That's because we're still talking about it. I know Stephanie wants to say something.

That's because we are still talking about it. Let me point out, however, that under the current system, we have actually got exactly the same issues. It's just that it happens to -- where's the registry based, et cetera.

Let me let Stephanie --

MATHIEU WEILL: Would what would be the point of changing the system if we're not addressing this?

CHRIS DISSPAIN: Let Stephanie respond.

STEPHANIE PERRIN: You raised -- we skipped rather lightly over the jurisdictional issue.

CHRIS DISSPAIN: Absolutely.

STEPHANIE PERRIN: Believe me, we have talked about them. Unfortunately, our colleague Michael Niebel who you may know is on the commission, was very focused on that topic as well. And the data protection is only one of the jurisdictional issues. There's also the litigation issues that come up in jurisdiction.

CHRIS DISSPAIN: Yep.

STEPHANIE PERRIN: There is consumer protection. Some countries have regulated for consumer protection on the Internet and some have not. So, frankly, one of the things that I -- as the lone privacy nut on the panel, one of the reasons I liked the central model is that it permits a harmonized central area where you can apply rules. And one thing that may not be strong enough in the wording of our report is we want the -- whether we go with the distributed model or the central model for the RDS, if it's in an area with strong data protection, then the rules for access will be within a data protection regime. And that's well-known to countries where there is data protection authorities --

CHRIS DISSPAIN: Exactly.

STEPHANIE PERRIN: -- that have set up legal procedures for what you get and what you don't get and what your purpose is and all the rest of that. Does that help? We are thinking about it.

MATHIEU WEILL: If I can reformulate, it would be part of basically the RFP for the RDS to look at which jurisdiction they want to set up in --

CHRIS DISSPAIN: Possibly.

MATHIEU WEILL: -- in order to get better data protection?

CHRIS DISSPAIN: Possibly. Or that decision may be made by us. It should be set up in a jurisdiction that we're comfortable with, right?

MATHIEU WEILL: Okay, great.

CHRIS DISSPAIN: Fab wanted to say something. Really quick. Okay? Fab? Carlton. Okay, Carlton.

CARLTON SAMUELS: I just wanted to get back to the jurisdictional issue. The fact is that you are quite right, where the debate is raised, this is going to be important.

So what you want to start with is a place where the protection rules are strictest. And you create the framework that is based on the strictest so that makes it harmonize across the board.

And binding corporate rules is one way to ensure that the practices surround the access and transfer and so on and publication is there too.

CHRIS DISSPAIN: And, Fab, very quickly.

FABRICIO VAYRA: I wanted to quickly address Steve Metalitz and Kiran, their question about taking away free access to data. I'm glad that Steve took the approach he did to come in and say that maybe what we need to do is explain a little bit more. It is clear we probably do.

In thinking about it, especially when Kiran walked up, it made me think the ICANN meeting is free and accessible.

CHRIS DISSPAIN: Yes.

FABRICIO VAYRA: But You still have to show up at a teleprompter and type in your name to get your badge. And that's, in essence -- not to super simplify it, in essence, what we are trying to do because we really believe accountability has a lot of implications in the system, not the least of which will hopefully incentivize people or make people feel more comfortable about giving true data if I know that it is Kiran or Steve that's accessing it.

So we do need to do a better job of explaining and not to do it quick thrift here. The reality is we are not trying to take it away. We just want to make sure once you get past some very basic data of system generated and maybe a name and email for contacts, that we at least have a way of verifying who it is who is asking for it, not try to take it away. Just balance out if I give, I also like to know who I'm giving it to. That's that.

Real quick, before you close, I would like to take a moment, if you would join us in thanking the staff who has helped us greatly in all of this. Some of these folks quite literally don't sleep leading up to our meetings. And we wouldn't be able to sit here, show you pretty slides, even have a report to give if you it weren't for them. So this isn't to say we're done. It is still a work in progress. I think they need to be recognized. So if you could just join us in thanking them.

[Applause]

CHRIS DISSPAIN: Stand up, Margie. Stand up, stand up. Okay. Don't stand up then.

See, I'm a director of the company. They won't work for me. They do as they like.

I thank you, Fab. That was very important.

I hope you guys realize how important your feedback and input has been for us to get to this stage from the first report to this stage. So please keep it coming. It's really, really important. I'm going to hand you back to Jean-Francois.

JEAN-FRANCOIS BARIL: Thank you. Thank you very warmly for all your comments today. I think it's very, very precious. The EWG journey continues. So what we have published on November 11th is a status report which means by definition work in process.

So as such, we invite all of you for the session we will have this afternoon at 4:30 for this workshop on refining few difficult issues.

I can continue to affirm or so that privacy, accuracy, accountability is -- or are at the center of everything that what we want to do with this EWG.

I was also very, very glad that Fabricio mentioned the outstanding work that Lisa, Margie and Denise are providing to the staff -- to the EWG because you have no clue on the level of creativity from the community but also from the EWG and thoughts on how to digest, assemble, and make it relevant on the report is quite a challenging task.

So also a big, big thank you for all of you contributing to the next generation of RDS. Thank you for your attention.

[Applause]

[END OF TRANSCRIPT]