

Explore the Draft Next Generation gTLD Directory Services Model Webinar**Monday, 8 July 2013****TRANSCRIPT • [Announcements](#)**

Margie Milam:

Hello, everyone. My name is Margie Milam, and it's a pleasure to welcome you to this webinar today, entitled, "Explore the Draft Next Generation gTLD Directory Services Model."

Before we begin, I'd like to remind all participants of the housekeeping items. This webinar is being recorded, so if you have any objections, you may disconnect at any time. At the end of the webinar, you'll be given an opportunity to voice your comments and questions during the Q&A section. Your lines are currently muted and will be opened at that time for the Q&A section. In the meantime, you are more than welcome to submit your questions or comments via Adobe Connect through the Chat pod. The slides and the recording and the transcript will be made available following the session.

The goal of this webinar is to provide you with an outline of the Expert Working Group's work on the gTLD Directory Services proposal. The Expert Working Group on gTLD Directory Services--we refer to it as EWG--published its initial report on June 24, and today's webinar will focus on the recommendations and the model described therein.

And with that, we'll turn to the facilitator of the Expert Working Group, Jean-Francois Baril, who will walk you through the mandate and the purpose of the Expert Working Group.

Jean-Francois Baril:

Thank you very much, Margie. On my behalf, it's also my real pleasure, along with the Expert Working Group, to be with you in this webinar and to have the possibility to present our initial report on Next-Generation Registration Directory Service.

So for today's agenda, on Slide Number 2, we have prepared two main sections. The first one, hopefully for no more than 50 minutes, seven of us within the Expert Working Group will bring you through the different important elements of our initial report, starting by our mandate and purpose, then our consensus on the key findings. We will explain also the methodology we used. Then I'll recommend the principles and features. We will also suggest a model with, of course, the pros and the cons. And then our next steps, including areas that are still open for us and also some more practicalities on how to comment on this report.

The second part, as it was highlighted by Margie, the second part of this webinar, which means 40 minutes, it's probably more important for us, as we are still under building mode. And I would like here to really insist that we are still on the construction mode. So this is a Q&A session where, hopefully, we capture your brains and your hearts

through your constructive and precious comments, which will guide us through this project in order to maximize the efficiency of this dialogue.

If we switch now to Slide Number 3, what is the mandate and purpose of the EWG? What are we trying to solve here? Well, why we accepted that current WHOIS system is broken and has been for a long time. So to address these critical elements, the ICANN Board took a two-pronged approach--on one hand, directing the implementation of the WHOIS review team recommendations. On the other hand, forming the Expert Working Group in order to redefine the purpose and provision of gTLD registration better, starting from a clean slate. So in essence, WHOIS what is better and why.

The Expert Working Group has then taken this opportunity to assess and to propose a paradigm shift to address fundamental user needs and purposes in the perspective of the next generation. In the best interests of the entire community of today and also tomorrow, we are working to define criteria and considerations relative to collecting, validating, storing, disclosing, and maintaining those gTLD directory data--balancing, of course, Internet community needs for privacy and confidentiality, enabling directory accuracy and better protection are among the prime objectives of this EWG.

Now switching to Slide Number 4 and to present the team. So as I said, we would not be here today without the exceptional team who have created this time this initial report. Of course, and by far, not perfect at all, but I believe presenting already a solid foundation and a measure of improvement compared to the current WHOIS situation.

One of the major characteristics for this theme, and it is in this case business critical, is the outstanding collaboration between all members, which has led to this very impressive capability to reach consensus on all key principles that we operate under today. Everyone is, of course, coming from very diverse backgrounds, very diverse directions as well. But still, we worked to converse very rapidly on those principles, and I would say with an unbiased attitude.

But now, and without further ado, it's my please to introduce Rod Rasmussen to describe in more detail the initial report and our key findings. So, please, Rod?

Rod Rasmussen:

Thank you, Jean-Francois. If we could go to the next slide, please. And thank you to everybody on the line. Good morning, good afternoon, good evening, good night to you, wherever you are in the world. I see we have a great crowd, and we really appreciate your interest and your feedback to what we are doing here in our efforts to redefine Registration Directory Services.

So, as mentioned earlier by Margie, the report was published just a couple of weeks ago, on June 24. The findings were put up on the ICANN website, and we have requested community feedback at this point during our process. We've already gotten a lot of feedback, some very constructive, some not so constructive. We are looking for as many comments as we can to help us, guide us through the rest of our process here.

So we took on the mandate here from the Board and did a very in-depth analysis. We're going to go into the various aspects of that, how the process works and the way we came up with what we have come up with as a proposal so far. But we really wanted to focus on the use and purposes for what registration data is used for today and where it's heading in the future and took it from, as Jean-Francois mentioned, a clean slate approach.

In the end, we've recommended a very large paradigm shift--depending on your perspective, of course. But we're looking at abandoning the current WHOIS system, and that is kind of one size fits all built for the 1980s or '90s and moving it into the modern Internet age, and replacing it with a system that is driven through use case, how people, users, organizations, use this kind of information and also provide the kinds of goals that we were talking about with privacy, having accurate data, and accountability for all

parties involved, whether that's the people providing the infrastructure, people putting data in, or the people requesting data out. And next slide, please.

So at the end of the day, and we're going to get into this through the rest of the webinar and, obviously, as detailed out in the report as well, we came up with this ARDS, or Aggregated Registration Data Service, where you have a model that has the various actors, et cetera, in here being able to put in, store, and access data in a more modern type of system that allows us to best satisfy the needs, purposes, et cetera, of the various, myriad stakeholders out there that are trying to have data around their domain name registrations in a place where they can take care of whatever their needs may be, which we will get into.

But the system itself is fairly straightforward, and it looks fairly familiar, at least up until you get to the point of the ARDS. But registrants still enter data into their system via registrars. The registrars are responsible for updating the registries, which are the authoritative repository of that data. That has not really changed from today's thick WHOIS model, if you will, at least from that side of things. However, we have the ARDS system, which then takes copies of that information, and that's where you have your data access that is purpose-driven.

Some of that would be public access. I know there have been some questions about the supposed removal of public access. That is not part of the system. There would still be public access to a certain level of domain registration data, but there would also be different gated access based on authenticated users and their various needs that they need for accessing different kinds of data.

And that's really it. That's the system. It is a paradigm shift, but it's one that you can see is fairly straightforward to think about from what we're doing. And we will get into more details on this later in the presentation.

So the next slide, please. So to just wrap up the introduction portion before we get into the details, this report, we put this together over, gosh, the last four or five months, so it represents a lot of work, a lot of dedicated time towards exploring the various issues, uses, users, of the system. A lot of going back and forth, really ferreting out a lot of issues. There's still more work to do, but I think that we've gotten it to a point where we have a proposal, need some public input, and want to move forward. But this does represent a consensus view of the entire Working Group.

And we realize this is not going to satisfy everybody; nothing ever will. But I think that we've come up with a solution that balances what everybody's goals are and is definitely a major improvement over today's system, where we have a lack of accuracy, a lack of accountability, a lack of usability, and really, a mess. So we are hopeful that this will provide a way forward for us to work on and that your input at this point will help us further refine our suggestions here.

And as we move forward on the process here through this webinar, through Durbin, and then later on through the summer and to the next meeting in Buenos Aires, we really want to put together a final recommendation that can be taken. But we need your feedback for that.

Looking through the report, and I really encourage you to read the whole thing, is there a better solution out there? If not, what are some suggestions on--I guess if there is, what are they? And if you have particular points that you think could be improved, please offer that up. What we aren't looking for is, "No, this won't work. Go away." That's not helpful or constructive. We need to move forward.

And as you're looking at this, remember as well what we did. We looked at this from all perspectives, all uses, all purposes, and tried to make sure that what we recommended could cover most of those needs. So if I can move to the next slide, please.

Methodology. So digging into a little bit of how did we come up with what we have come up with, so we sat down in late February or early March, whenever our first meeting was, and really did a full, almost like a, if you've ever been on a product management team or an engineering team, if you're taking a look at providing a new kind of service for a market that may not be serviced by a product or isn't being serviced very well, what would that look like? What would the needs be? Who are the people using this kind of service? What are their desires? What are their pain points? What are the things that aren't working well?

And we leveraged all the great work that's been done by a host of other teams, looking into various things that have come before us, looking at the WHOIS issue. We also took that clean plate approach, as like, okay, going back to the drawing board, how would we do this without--we're not going to try and tweak this. We're going to try and, if we were starting fresh today, how would we do this?

So we had boards and boards full of diagrams and lists of people and the things that they do and all of that, and then dove into a use case modeling process, where we would take a particular point of view--let's say a domain registrant, for example. What do they need to do? They need to get domain information in there, and they want to be able to maintain ownership of their domain. So we take it through that whole process, what all that involves, who they would have to interact with, like a registrar, and then fleshed out that entire use case to provide the kind of information that we need for knowing data elements and security requirements--all the things you'd need to develop a product or service.

Okay. And so we did that and iterated over and over and over again, across all these use cases and came up with lists of the various similar types of activities. There's a lot of cross-pollination, if you will, or a lot of overlap with what different purposes of things are and kind of rank-ordered those, and also tried to group users together and the purposes together as well so that we could get a better understanding of what various types of people want to do and what they're trying to do with it.

So go to the next slide, and we'll get a summary of the various users. And these are not hard and fast. One thing to take away from this report as well is that we've come up with a series of potential users and potential uses, we know this isn't quite 100% comprehensive. And if there's other use cases and people we haven't thought of, or you don't think are covered well by our bucket system, feedback we'd like to get.

But in general, we had this clock, if you will, a cloud of user types that we've identified as having similar characteristics. Registrants, obviously, the people who have the domain names and are using them for various purposes, are an obvious one. Internet technical staff, people who need to interact with domain names to keep them running or to have them communicate with each other. Obviously, individuals using the Internet, trying to get to places, find out about the places they're going to, et cetera. I'm going, by the way, clockwise around the diagram here.

Researchers, this is the types of folks who are doing just general research on the Internet, and that could range from studies on infrastructure to people using the Internet, but oftentimes, they need to figure out what kind of domains there are out there--the commercial and noncommercial, for example, or other things.

Various kinds of non-law enforcement. LEA is law enforcement agency. That's what that acronym stands for. Various types of non-law enforcement investigators. This can be anything from ICANN compliance to UDRP investigators or something like that, where it's a non-criminal, non-abuse incident response type of situation.

Bad actors. We know that there are a lot of people out there who are misusing the WHOIS, et cetera, mining it for spamming and things like that. Law enforcement and operational security, incident response type of purposes, intellectual property owners protecting their trademarks and brands, et cetera. Businesses using the Internet for providing goods and services, et cetera. Online service providers, typically ISPs or Web hosting companies.

And then the class of registrant we paid particular attention to is this protected registrant. And I believe Stephanie will be going into that in more depth in a little bit later in the presentation. So that is looking at the class of user who maybe needs special protections.

Next slide is purposes. So taking all those users and their various needs, et cetera, we had literally dozens to hundreds, I would say, of use cases. We've boiled them down into these buckets. There could be more. Again, I emphasize we need to get your input on other things they're using that they don't fit into these buckets.

But everything from controlling ownership or who has the right to use a domain name, to various technical issues on the Internet, to the various individuals trying to use the Internet for what they need to do in researching domains, either thinking about that for purchase purposes or just general research at all. Enforcing a contract. Obviously, you have abuse and other legal actions you take; for example, UDRP or other trademark types of actions.

I already mentioned sales, and then just getting the Internet to work at all, you need to interact with the registration system. And there are lots of different services--for example, digital search rely on WHOIS information in order to issue a certificate for a particular domain name. So those are, and the paper goes into far more depth than these, and a long list of all the purposes and users.

So I'm going to turn this over now to Carlton, who will run through the next section. Carlton?

Carlton Samuels:

So next slide, please. So as people will tell you, we are a very diverse group. And when you have a diverse group, the first thing you probably need to do is, as we go from a clean slate approach to this, is to consider some principles that we would wish to adhere to as we look at the desired features and principles.

We looked at the use cases, and we decided that these principles would guide us as we move forward. They are capability of international considerations, accountability. Privacy was a big one. As you probably would know, there's been, at least there's a significant body of opinion that suggests that the reason why we have such poor with data is because of privacy concerns. And we looked at permissible purposes, we looked at data disclosure, data elements. We need to decide fully what those were. And we needed to assure that whatever we did in collecting registration data, it must be valid and accurate. And we thought we should at least embrace some kind of direct validation from the start. And the question of storage and escrow came up. These were just guiding principles as we talked about features and what it is that we want as outcome.

Next slide. So I want to drill down a little bit on the privacy principles. I earlier mentioned that privacy was significant to the quality of WHOIS data, and so we spent a lot of time, the group, in thinking this through. And what we came up is that we should at least embrace the idea that there would be an enhanced protective registration service required, and we should go a little beyond that and say that there should be some level of registration service in which the personal data of the registrant would be highly restricted for use.

We had a look at the types of property provider accreditation. You probably would know this was one of the major outputs from the WHOIS Working Group final report. And we spent a lot of time thinking about what we wanted to do with private property. We were of the same mind as the Working Group, that in any private property provisioning situation, it should be accredited and managed. And we are not quite done with it yet. There are still some thoughts that we are mulling over. And in due course, we will make those available to the community.

Here's the thing about law enforcement. It was of the view that law enforcement is a use purpose, but because they would want heightened access to data, then there should be some kind of mechanism to license their requests to make sure that we know what they would be doing for and purposes. And this is controversial that there should be some other for accommodating domain registry detail credentials. I mean, if you look at secure, protected credentials, it simply means that the person who is making the registrant, we would wish to accommodate, we would wish to consider accommodating a situation where that registrant is highly protected, is what that means. We are still thinking this through.

Next slide. So data elements. Well, it's straightforward. We know that the transaction is between registrant and registrar. We're still insisting that elements that's collected by registrars, they are stored by registries, and notice that we are adopting the idea of this thick registry model, and the reasons for collecting that data must be for a purpose, purposeful collection.

We actually understand that there should be some mechanism to allow for extendibility of the data set. This is a very critical area, because as you would understand, the data elements themselves, why we collect them and where we store them, is at the heart of the conundrum of privacy and all those kinds of issues. So this is something that we thought long and hard about. Next question.

Data disclosure. Well, you would request the registrant data, and we would wish to know that when it is disclosed, there's a mechanism to manage and control that. So the idea is that it is copied from the registries, registries being the authoritative source for registrant data. And it's aggregated by the RDS, and you will only get data from the RDS based on purpose. And what you get will be driven by the purpose. That's it. You'll get only so much to satisfy the purpose that would have been established.

Here's something that I think is slightly misunderstood. We still embrace the idea that there should be a minimum data set that is available for full public disclosure. We are also of the mind that even with full public disclosure of this minimum data set, we should put in place restrictions to deter bulk harvesting. As you probably would remember, a lot of the spam that we get is generated from bulk harvesting of WHOIS data. We would wish to frustrate that as we go forward.

So there's a minimum data set that we should publicly disclose. Those that are not publicly disclosed altogether should be kept and held behind some barrier. And we therefore have this concept of gated access to the other data other than the set that is publicly disclosed. We still would require that the requester is identified, and the access is also going to be purpose-driven. So it simply means that you're not going to get away from knowing who the requester is and the purpose for the request, regardless of the fact that it's behind some restricted entry door.

I think the next slide is my final slide. So access methods. This is a lovely pictorial that was developed by Lisa and Margie. And it encapsulates pretty quickly what is certainly our theme in the first few slides before now. Think of a case as any request. So that is John Q. Public, and you will make a query against the RDS. And notice that it is an anonymous query. And what you get from the RDS is the set of data elements that we would have defined as always publicly available. So anyone, anywhere, any time, can

access this finite set of data elements for any purpose, save that we would wish to see instituted mechanisms to deter bulk harvesting.

The other situation is an authenticated requester, and authentication means we have to know who you are and for what purpose you request the data. In any event, you would make the request against the RDS. Because you are approved, we would know who you are, we would know what the purpose is, and we would know what data elements you are entitled to by virtue of purpose. And that is returned from behind the gate. So this now is the role of access methods that we are proposing.

Notice very clearly that we are saying, if you are an authenticated requester, it is not that you have access to the entire data set that is here. You will only be granted access to the elements that fit your purpose. It's very important to get that idea, that it's not just because you are authenticated, then you are free to roam the RDS. I think next slide.

Michele Neylon: Thanks, Carlton. I'll take over from here.

Carlton Samuels: Thank you, Michele.

Michele Neylon: Okay. This is Michele Neylon here. I'm just going to go back over part of this slide here on the access methods before I move on to a few other points around this. As we've said several times so far in this presentation, there seems to be a misunderstanding in some parts of the community that we are proposing to remove public access to WHOIS, or rather, to registration data. That is not correct.

What we're looking at doing, and this is something which has happened in several country codes, is we're looking at differentiating between anonymous public access so that any random user, using whatever methodology, when they do look up versus a known user that has authenticated at some level, so the idea being that an anonymous lookup will give you back some data. And then, in return for you authenticating yourself with the system and sharing some of your data--in other words, the idea of some kind of accountability--you will be able to get access to more data. But as my co-presenters have said, it's all down to purpose.

Now, the other thing as well, which is, just so it's clear, what we've been talking about here is in terms of a concept. We are not saying that either one technology or another technology should be used to run this. So, for example, the work that's already been done on the IETF in WEIRDS--which is a horrible name, but hey, it's what they ended up with--and there's no reason why the work in WEIRDS could not work within this system. Because what we're talking about here is the principles around controlling how the access is given, on what data is accessed, depending on how this is done. And as others have said, of course, we've done all this, working on the basis that the current system of WHOIS is no longer fit for purpose in 2013 and beyond.

So just looking at this slide here, you can see this idea. If there's any requesters, kind of the idea of anonymity, the general public, then that request will only get back a subset of the registration data. But, of course, as Carlton said, we wouldn't want somebody to just use that to mine or to harvest data from the system. And then if they're authenticated and they provide details of why they want access to the data, then they will get back more data--more data from the system, and depending on what their purpose is, the level of data that they get back, the type of data they get back, will be controlled. Next slide, please.

Of course, a key thing in any discussion around WHOIS up until now has been around the quality of the data. And under the 2013 RAA, there are provisions there with respect to the validation of data. Our proposal here, we are suggesting that the data should be validated syntactically. Now, what that means is that, for example, that you would check to see that a telephone number, for example, is a possible telephone number. This is not

the same as verifying that the telephone number is 100% correct, but we're talking about making sure that you don't have rubbish data.

Again, we're talking again about--we've also discussed various other concepts around I'm going to higher levels of verification and validation or to be able to reuse certain data points. And this would all be standardized. Next slide, please.

Now, another thing which is very, very important and cannot be underestimated is the concept of accountability. So the entire ecosystem in our proposal has to have a level of accountability. So as a registrar, I have a responsibility. For you as a registrant, you have responsibilities. And the registry has responsibilities, too. So every party within the ecosystem has responsibilities. So each one of these must be respected, and if they are not respected, then you can see some action being taken; there are repercussions.

So the idea would be that you have current, accurate, and timely data, so it's kept up to date. It's valid. That ultimately, the idea is that the registrant and their other contacts are reachable and that they are responsible and that there are repercussions if they provide bad data into the system.

And now I will hand over to Faisal. Thank you.

Faisal Shah:

Thanks, Michele. As Rod and others mentioned, the use cases and the purposes for accessing the registration data really drove the design principles that are listed in the initial report. The EWG looked at everything from creating greater accountability, as Michele said, and a future design to privacy considerations, with the ultimate goal of ensuring that at the end of the day, access to all this information would be purpose-driven, and you've already seen us mention that here today.

So we took those design principles and basically focused in on three different areas--the collection of the data, how the data comes in, maintenance of the data, how it is stored, and then the disclosure or display of the data, and Carlton and Michele talked a little bit about all those.

With respect to the actual storage and maintenance of the data, the EWG looked at a number of potential designs and reviewed the report by the Zone File Access Advisory Group, and Rod was a member of that group. And that group had looked at a number of different designs, including centralized or repository models and distributed or proxy models. And then the EWG ultimately settled in on an aggregated model. And as Rod said, a pretty straightforward model, since it best fit the user needs and purposes that we had already identified for a new Registration Directory Service.

So you'll find in the report that the EWG is suggesting that a neutral international third party be created called the ARDS. The ARDS would be tasked with holding a non-authoritative copy of the data elements collected from the gTLD registries. The ARDS will contract with the registries to have the data copied and provided to the ARDS and then updated periodically in the system.

So essentially, a certified requester would ultimately pull information directly from the cached data within the ARDS, but the EWG also recognizes that there is some latency in this model, since the data isn't real time. So in some cases, the requester will also have the ability to access the real-time registration records from the respective registry through the ARDS.

Now, this body will also be tasked with validating inquiries, licensing requesters, applying data principles, providing public data, and it will ultimately be responsible for auditing, access, and spot-checking data to ensure greater accuracy, as well as handling accuracy complaints. And under this model, registrars and registries would be relieved of

their obligations to provide that cumbersome 443 and public access to the registration data.

So on the next slide are some of the advantages of this particular model. Instead of having to go to over 1,000 registries to get the data that you need, a consumer interested in data from multiple registries would now have one point of contact--in effect, a one-stop shop. Requesters will be able to come to one place now to get their information. And the ARDS is responsible for managing the contractual licensing of the data that's coming in from each of the different registries.

Another advantage to that is potential improvement to transport and delivery. This body can enable a consistent information display format as opposed to having diverse data formats from hundreds of different registries. It can also provide support for data in multiple languages, in multiple scripts and character sets, and it can also provide better search capabilities.

There could be greater accountability in the validation process and access as well. And as Michele said, accountability really is a principle that's woven throughout this particular document. Now the ARDS can monitor who's actually accessing the information as to who will have a gate and can also monitor how the information is being used.

ARDS can audit the data with random spot-checks, and it could impose certain penalties and certain consideration associated with bad data or improper use of data. Then maybe reduce costs and burdens on registries and registrars again. We talked about relief of the 443 or Web access obligations. And this in turn could potentially reduce bandwidth costs.

It could facilitate a process to satisfy local data privacy laws. Having the data in one place could enable the ARDS to better store and display certain information in conformity with local laws. So how the display is tended and managed by the ARDS.

The model might minimize transition implementation costs. Again, this file contemplates pulling data to one location and managing that data there as opposed to trying to implement changes across thousands of registries.

Other advantages, the ARDS can enable an accreditation mechanism, and we talked a little bit about that--privacy and proxy provided, for example. This mechanism will allow requesters to be able to be qualified for special purposes in receiving the data. The ARDS can also perform random accuracy checks and thereby provide accuracy reports, then hold the cached data.

And some of the things that we've kind of mentioned here, it could enable ancillary services to meet certain uses and purposes such as cross-TLD domain, domain name lookups, reverse WHOIS, providing historical information on registration data.

And now going to some of the disadvantages on the next slide, obviously, the elephant in the room, it's a big data repository of highly sensitive information, so security is going to be paramount. Because it is a repository of big data, it might be subject to misuse, either by an insider, or it could be subject to some type of external attack. Another disadvantage is that registrants and registries could collect and store the data, but they are no longer in direct control of delivery of that data, and there may be some registrants and registries that are uncomfortable with that.

And finally, data latency. The data is not being updated in real time, so this may present a problem. And I would venture to say the frequency of updates would then become really important here.

So those are some of the advantages, the disadvantages, an overview of the system, as we've heard from a lot of presenters about the overview. And now I'm going to hand this off to Susan.

Susan Kawaguchi:

Hello, all. You've heard a lot today, and we've done a lot of good work. So hopefully, we haven't confused too many things, but we have a lot of work left to do. So key to all of this is the privacy recommendations. We're looking at this from lots of aspects and understand the importance of privacy. It's key to a new system working. But we also want to balance individual privacy and commercial use of privacy. So that's one of our key issues that we'll be working on at our next, in Durbin, at our meeting there, and ongoing.

Also, the required data elements. We have some thoughts on this, haven't fleshed it out completely. Accountability will be key there.

And then the prevalidation and accuracy--we are not suggesting that we will be removing some of that responsibility from the registrars as they collect the information, but we are seeing the ARDS as a vehicle to improve all of that, and maybe even create profiles that companies or individuals can use that is completely prevalidated, and so they only have to go through the process once. And as long as nothing changes, they can just use that information in their registration.

Risks and impact analysis--that's foremost, also, in our thought process. We have not given this a tremendous amount of thought yet, but intend to before the final report.

Storage and escrow requirements--we continue to get information from many parts of the world on their own requirements, the local laws. So we're looking at that. Cost impacts and ways that this might be borne. The costs could be significant, but right now, the costs are significant, either to the individual registrant, registrar, or registry, and those that are protecting Internet users.

And then we're also looking at a variety of access methods, the multi-modal access methods and protocols, and we'll continue to do that work. Next slide.

So we need your help. I was on the WHOIS Review Team, and the information and the comments, the input we received, was crucial to our work there, and I see it as crucial to our work now. So I urge all of you to read the report. It's long, but it's not too difficult. And we need comments by August 12. We'll be meeting again at the end of August, and all of your input will definitely be considered. We're going to continue our work on the open areas and, hopefully, we're aiming for a final report before Buenos Aires that we will publish again. We'll deliver this to the CEO and the Board, as it was requested; it was a Board request. And we'll also provide input to the GNSO for PDPs.

So that's it, and I think we're open to questions.

Chris Disspain:

Hi, Susan. Thank you, that's awesome. Can we go back to the previous slide? Great. I'm going to--Margie, you can take it in the second half. Keeping to just, for everybody to be clear, these are the ways that you can comment. The public meeting in Durbin a week today is an excellent opportunity for those who will be there to talk and interact with us. And then there's all the usual other ways. There's online questions or comments by email and so on.

Margie, do you want to just deal with housekeeping before questions?

Margie Milam:

Sure. These are the housekeeping notes, and then, Chris, if you could just moderate the questions. Right now we're going to ask that all the lines be unmuted and we'll open the floor for questions. We'll take a look at the hands in the Adobe Connect Room and create a queue.

- Operator: Listen-only mode is now off.
- Margie Milam: Excellent. And then, Chris, you can manage the queue and assign members to answer the questions, okay? And then if you're on the bridge and you don't wish to be, please make sure to unmute your lines. Press star-six to mute, and to unmute, press star-seven. Go ahead, Chris.
- Chris Disspain: Okay. So I guess most of you will have used this Adobe Room before, and you can raise your hand in order to ask a question. And Bill, thank you for doing that so I can see--and Chuck. Fantastic. Before I go on to the questions, I see Steven Metalitz has been busily typing away in the Chat Room as well with some questions.
- Can I ask that when you have asked your question, if you put your hand down. That means that I can manage the queue properly. If you leave it up, I'll end up ignoring it, and if you want to put it up again, you won't get hurt. And for those with us on the Expert Working Group, if you feel a particular need to respond to a question, please put your hand up as well, and I will spot that and ask you. Otherwise, I'll just throw it to whoever I think the appropriate person is. That applies to staff as well.
- So Steve was actually, before any of the hands went up, Steve Metalitz was typing in the Chat Room. Can we go back to Slide 16? Thank you. Steve says, Slide 16, "validated operationally"--does the Working Group plan to define that further? Can somebody online just quickly respond to that before I take questions over the line? Okay.
- Michele Neylon: I'll take this since that was the slide I was doing. It's Michele speaking. Steve, good afternoon, how are you? Time stamp validation--no, I think what we're talking about there is that it would be time-stamped. If there's a revalidation, the revalidation would carry a time stamp.
- Chris Disspain: That makes sense. And Steve's other question was "validated operationally."
- Michele Neylon: Well, I'm sorry. I'm looking at two questions from him.
- Chris Disspain: Yes, you are.
- Michele Neylon: The name/contact should also be validated operationally. Again, a lot of this stuff around the validation and the validation of everything else is we're looking at improving the overall quality of the data and, so let's say for argument's sake, if a name is provided that is completely and utterly wrong, like Anonmouse, just as a stupid example, that that wouldn't pass validation. Higher levels of validation and verification are things that we have looked at. I think that kind of covers what you're asking, but if it's something more specific, please let us know.
- Chris Disspain: So you're first off on the voice questions. If you're off mute, go ahead.
- Bill Smith: Okay. Thank you. And first I'd like to thank the Expert Working Group for I'm sure what was difficult work. I was on the WHOIS Review Team with Susan and know how difficult these things can be.
- I've refrained from commenting so far because I've been doing a lot of thinking about the draft report. And there are many aspects of it that I think are quite good. I have some serious concerns. They relate to what the minimal data elements would be. I don't think that has been clearly specified, and so that is an issue. If the minimal set is the null set, then it's not a very good compromise solution.
- Another point is I think there should be a security review of this. I remain extremely nervous and concerned about a centralized anything when we are doing things with the

Internet or at Internet scale. Privacy, absolutely, is an issue and must be addressed. But also, we must consider the privacy--more appropriately, not really privacy, I don't think necessarily privacy--but the safety of the individuals who in fact are attempting to provide and protect the privacy of others on the Internet. And so having a centralized system where authenticated access occurs and having centralized data of that, I am very concerned about that on an international scale. And so I plan on writing these things up, but I still remain concerned about those things. But again, I appreciate the work of the group.

Chris Disspain: Thank you, Bill. I'm not sure that any of that requires a response.

Michele Neylon: I think one part of it does require a response, Chris.

Chris Disspain: You go ahead, Michele.

Michele Neylon: Sorry. I just want to be 100% sure that people are very clear about what we are and aren't recommending with respect to data. There is no acceptable concept of a null set of data, because ultimately, there is no way for a domain name to resolve on the Internet if the data set is completely null and empty. It just won't resolve; the domain won't resolve.

What we have done is we've looked at it in terms of building up the data set in order for a domain to resolve and then building from that. So in other words, getting the domain from being an entry in a database to having name servers, to having other bits of data around there. And if it wasn't clear in how we described that, that's what we're doing, is looking at it in terms of building up the bits of data that you'd need to have a domain resolved on the Internet.

With respect to the privacy concerns, this is something that we have looked at in detail. So this is one of the concepts that we have put forward is the idea of this extra level of privacy which would have to be managed by some kind of third party. And again, I think any of these questions are things that may require clarification are very, very welcome. Thank you.

Chris Disspain: Thanks. And before I move on to Chuck, just one other point, and it's an overarching point. I think it's very important to remember that it's not the job of this Working Group to write the detail of the policy or even to recommend or make proposals. It's our job to provide an overarching basis from which the GNSO can then move on in conjunction with the other parts of ICANN that are involved in the policymaking process to actually make the formal policy. By definition, some of the details will be a matter for policy. Chuck, over to you.

Chuck Gomes: Thanks. Chuck Gomes. And let me join Bill in thanking all of you for the long hours of work, not only that you've already done, but that you will do going forward. I appreciate that very much.

I have four pretty much unrelated questions, and I'll take one at a time so that if you want to respond, you may do so. The first and most important is it's my observation that purpose is awfully important in the model that you've proposed. But I couldn't find anything that says how purpose will be validated. So it seems to me that that could be gained terribly easily, unless I'm missing something. Could you respond to that, please?

Chris Disspain: Thanks, Chuck. I'm sure someone's going to be happy to respond to that while I'm waiting.

Michele Neylon: Chuck, this is Michele, who's happy to respond, as ever. Do any other members of the EWG want to respond, or is this going to become the Chris and Michele show?

- Chris Disspain: Hang on. Just before you do respond, I just wanted to say that Chuck, it's a valid point, that we worried about purpose to a great extent, and it needs to be validated. So, Michele, have a go and then I'll ask if anybody else wants to say something.
- Michele Neylon: Okay. Thanks, Chris. Now, Chuck, this is something that we've looked at in two ways. First off, we think that the amount of data and the sort of data that a requester should have access to should be tied to the purpose for which they're requesting the data. Now, obviously, of course, not everybody is honest, and people will probably try to abuse the system. Actually, let's rephrase that. People will try to abuse the system; there's no "probably" about it.
- This is where, I think, the kind of thing about the gated access and the validation of everything is going to come into play. So, for example, if, say, you have a requester who says that they're going to use data for one particular purpose and then goes off and uses it for some completely different purpose, then that requester should be blocked from the system, potentially forever, maybe just for a short period of time.
- I mean, it is a very valid question, how best to deal with that. I think the idea we were looking at--and again, actually, this is going to, I think it was Bill's query earlier about something to do with data as well. He said we didn't get into the operational implementation specifics. That doesn't mean we didn't consider things, but the thing we wanted to do was to work on principles and ideas that we'd agree with, obviously, taking into consideration what was possible, but we didn't want to get bogged down in the minutiae of it.
- Chris Disspain: Thanks, Michele. Chuck, the other point I was going to make in response to you--I know you've got other questions; I'll come back to you in a second--was to your point about gaming. It's a valid point, but I think--and I know you don't look at it this way, so it can be used a lot of times as an excuse for never doing anything, because the reality is, everything can be gamed. The current system is totally gameable. If we're going to judge what we do merely by the fact that it's possible to game us, then we'll never change anything. The question is, what's the mainstream going to do rather than, "Is it possible to game us?" But nonetheless, you had a good point, and I know you didn't mean it that way. Question 2?
- Chuck Gomes: Yes, before I go to Question 2, Chris, let me say that as you know, I go back to the days when dot-com and dot-net and dot-org had a purpose, and we tried to--
- Chris Disspain: You mean as TLDs or as WHOIS?
- Chuck Gomes: We tried to control that. What we found out was that we were--and I think Michele already kind of hinted at this--we rewarded those who were dishonest and penalized those who were honest. And so all I'm saying is not that this shouldn't be explored, but I think that's a crucial area that needs to be addressed, and it's not an easy one. So thanks.
- Chris Disspain: Agreed.
- Chuck Gomes: My second question, what's the value in the model of having registries in the middle between ARDS and registrars? What value add do registries contribute?
- Chris Disspain: So do you mean, rather than just having the data flow directly to an ARDS?
- Chuck Gomes: I didn't follow that.
- Chris Disspain: Are you saying that by asking what value do the registries contribute, do you mean that the alternative would be to have the data flow directly from the registrar?

- Chuck Gomes: Well, that would be an alternative, but I tried, in looking at the model, to see what value a registry adds, other than being someone who receives data from registrars and passes it on to the ARDS. So I'm not seeing any value add on the part of the registry, other than adding the cost, and maybe there is something I'm missing. But it doesn't--I'm not criticizing the model overall. I actually personally think it has a lot of good things to it. But I'm not seeing how registries add any value in the middle.
- Chris Disspain: So I'll have to throw that out to someone on the phone.
- Susan Kawaguchi: Chris, this is Susan.
- Chris Disspain: Yes, Susan, go ahead.
- Susan Kawaguchi: Yes, I would like to respond to that. We did look at that somewhat, and in the current status of things, the registrar has a relationship, or a contractual relationship, with the registry, so there's a point of accountability between those two, and then also with ICANN. In what we were looking at, there was no contractual relationship between the ARDS and the registrar, for example. So we sort of left the system alone as the status quo and how other gTLDs operate, and also, we looked at ccTLD operations. And so we felt like that would be points of accountability for the registry to be able to make sure that the registrar was providing them the information. They would also know all of their records. They would have all the information, and so we felt we would leave that order of doing business in place.
- Chuck Gomes: Well, Susan, that's really not--this is Chuck again. That's really not the point of accountability that we have now. Registries are not accountable for registrar WHOIS. ICANN is through the RAA.
- Susan Kawaguchi: That's true.
- Chuck Gomes: I would just point that out, and I would hate for this to just be another opportunity for ICANN staff to avoid accountability and pass it on to another third party, as they very commonly do.
- Susan Kawaguchi: I agree with the RAA statement, but the registry does have some accountability to intaking that data from their registrar. Now, maybe that's not strong, and the registrar does have to respond to ICANN's queries on inaccuracies. But we still felt that relationship should stay as it is. Now, that's something that used to be of value.
- Chuck Gomes: But that's what I'm saying. It's not staying as it is. It's changing, the way you're proposing it.
- Chris Disspain: Chuck, I think that's right, to an extent. I mean, from my personal point of view, and you know that my lens tends to focus on the ccTLD world, But I felt strongly that it was important that the registry was still the authoritative font of the data and that the registry was the place where you would go to make changes. And so, therefore, their involvement in the process was critically important. But since I may not be picking up, necessarily, the nuances that you're suggesting--Michele, did you want to say something?
- Michele Neylon: Yes, I mean, far be it from me to want to take Chuck on directly, because that could get dangerous very quickly. But I think Chuck is looking at this from the perspective of the operator of commonness, which is thin, so VeriSign doesn't have any visibility on the WHOIS registration data, so couldn't be held accountable before because they don't see it. That wouldn't be the same case with a thick registry, nor would it be so with a sponsor TLD. I think there might be more of a kind of a shared responsibility there. If, for example, you have the case of .xxx, they actually have an entire community membership concept, I mean, just as one example.

So I think I know where Chuck's coming from. I think something that may be, if Chuck wants to follow up with us offline on this so we could see if we can thresh out some of the finer details, it would be really appreciated, because Chuck does--you have a lot of experience, and I would really, personally, I would love to see input from somebody like you. Thank you.

- Rod Rasmussen: This is Rod.
- Chris Disspain: Rod, go ahead. Go ahead, Rob. Hello? Anyone there? Hello?
- Carlton Samuels: Let's move on until he comes back.
- Chuck Gomes: Thanks. This is Chuck again. Thanks for the dialogue on that. Is that Rod?
- Chris Disspain: Can you hear me, guys?
- Carlton Samuels: Rod has been dropped from the call. We can hear you fine, Chris.
- Chris Disspain: Okay, sorry, I apologize. Chuck, you go to Question 3.
- Chuck Gomes: Okay, thanks. And thanks for the responses on that. I'm more than happy to dialogue further on that.
- Third question, one of the things that was good that you anticipate doing is a risk and impact analysis. But there didn't seem to be any indication as to when that would be done or by whom, going forward. Where does that fit into the next steps? Is that something that would be done before recommendations to the Board and into the PDP process? And any idea who might do that? Or would that just go out as an RFP?
- Chris Disspain: Good question. Does anyone want to comment? I mean, we don't have a slide up for that question, Chuck, but does anybody want to comment on it?
- Michele Neylon: It's Michele. I can make a comment if you wish. Or let somebody else go first.
- Chris Disspain: Well, I wanted to go to Margie to talk about the risk analysis. We've talked at great length about risk analysis. We understand that it needs to be done. I'm not sure that we've actually reached a conclusion on timing yet.
- Margie Milam: Yes, this is Margie. I think that's right. We haven't really settled on the next steps with regard to that. That's one of the questions we've asked the community, is how best to do that.
- Chris Disspain: Chuck, I think the question was part of the challenge with all of this, which is we're very conscious, but we don't want to use the (inaudible) have in respect to making policy to this. We just want to provide a series of boundaries, if you like, a gated area within which the GNSO can make the policy. And so questions like Bill's questions about risk analysis and so on and so forth have to be looked at and put through that lens. And we don't know whether it's more appropriate for us to do it or it's more appropriate for it to be done as part of the policy development process.
- And it's a really interesting question on which, I think, we're very keen to get feedback from the community. And if the general feeling from the GNSO side of things and generally from the community that it should be done by the Working Group, then fine, we'll do it. And if there's a general feeling that it's something that should be done as part of a PDP, then we'll back away and let that happen. So I think that's where we are with that. And I'm going to come back to you one more time.

- Chuck Gomes: This is Chuck again. My suggestion, and I'm not claiming to represent the GNSO on this, but first of all, I don't see a risk and impact analysis as being something that's developing policy. But I think it would be more beneficial, or would speed things up, if it was done earlier rather than later. In fact, it would be great if that was done before any PDP in the GNSO was ever started, because it would provide very helpful data.
- Chris Disspain: That still may be valuable input on that, and sure, that makes sense. Let's move on to your fourth question before we spend all of the time just with you.
- Chuck Gomes: Okay, Chuck again, and this one, I think I picked up a small answer on this. On your slide, as well as in the report, you list that registries and registrars no longer control delivery of registration data, and that was listed as a disadvantage. It wasn't clear to me why that was a disadvantage, but I think that was hinted at in that maybe some registries or registrars will look at it as a disadvantage. It didn't necessarily look that way to me, but I don't know that we really need to discuss that any further unless anyone has anything to add. Thanks a lot.
- Chris Disspain: Thank you, Chuck.
- Michele Neylon: Chuck, this is Michele. Just to respond to you, I think part of what we were looking at with pros and cons was trying to see what you as a community might perceive as an issue. And I know from some of the feedback we've got from existing and future registry operators, that this kind of idea of handing over control to a third party is something that they're concerned about, whereas for others of you, you probably see it as being a positive thing. So I think it was partly preemptive. Thanks.
- Chris Disspain: Thanks, Michele. Chris, you're next in the queue. You probably need to take yourself off mute. Still can't hear you. Star-seven will take you off mute. Okay, I'm going to move on to Steve and come back to Chris. Steve, go ahead.
- Steven Metalitz: Thank you. This is Steve Metalitz. This kind of builds on one of the questions Chuck asked and some of the other answers. I think, first of all, let me just echo what people have said about the thanks due to this Working Group for all the work they've put in, and I think they've come out with a very good product. And there's still a lot of questions about it and issues, but I think they've really moved the ball forward in a relatively short period of time.
- My question really has to do with how this fits in with other things that may be in process within ICANN. And I'll give, in particular, the example of the proxy and privacy accreditation process. Since we now have a completed RAA, and the specification on privacy and proxy service has an expiration date, so the expectation is that this accreditation system has to be in place by that expiration date. And yet at the same time, we see the EWG saying, "Well, we still have more work to do on privacy and proxy accreditation, so wait to see what we finally say about that."
- I think it would be helpful to get some guidance, whether it's from the Working Group or from the staff, about how these different pieces fit together, and specifically whether there would be any reason for holding up on efforts to start work, and I say that from the perspective of someone who is unaware of any work that's gone on, on it, although there may be some that I don't know of, to start work on privacy and proxy accreditation, or should we be waiting until the final report of the EWG comes out, or perhaps even some point after that? Thank you.
- Chris Disspain: I can respond to that. I think I may disagree. In my view, very strongly, we shouldn't wait for anything. This is a standalone piece of work, and I would hate to find it being used as an excuse for not dealing with stuff. And frankly, we don't know how long it's going to take. After we come to our final conclusions, we don't know how long it's going

to take the following policy development process to work with what we've got. So I would be saying everything should proceed as normal.

Margie, do you want to comment on that since you're working on that privacy and proxy stuff at the same time?

Margie Milam: Yes, sure. As you know, the RAA was just approved by the Board, and that is an interim specification. So as part of the conclusion of the RAA work, there's supposed to be a PDP kicked off on the issues that are remaining. And clearly, the privacy and proxy ones are remaining issues. And so I don't see a reason to wait on that.

I think the work of the Expert Working Group, if we stick to plan, would be done in October, and that absolutely would include some measure of recommendations related to privacy and proxy. And the PDP, if it's kicked off early, is not going to be completed by that point, and they can just use that as a reference as well. So I don't see any problem in kicking all this stuff off immediately rather than waiting until the Expert Working Group concludes its work.

Chris Disspain: Thanks, Margie.

Steven Metalitz: Thank you very much.

Chris Disspain: Okay, we've got time. So do we have any other hands up in the room? Or anyone else who wants to ask a question?

Michele Neylon: Chris, do you mind if I make a couple of comments, just in relation to what has just been discussed?

Chris Disspain: How could I possibly stop you, Michele?

Michele Neylon: Well, you could always try politely to shut me up. I mean, the thing is, I think one of the things that--I mean, Chris has said this, Margie's said this, and Steve was asking about it. And I think this goes back, again, a little bit to the risk analysis question as well, in some respects. This is a big paradigm shift that we are proposing. We're not talking about modifying the existing systems, we're not talking about tweaking, we're not talking about putting a Band-Aid on a massive gash. We're talking about building a new system from scratch that goes back to basics and starts from first principles or whatever way you wish to describe that.

So in the new RAA, which has just been approved by the ICANN Board, there are several issues around WHOIS that are addressed, including a standardized format and the app for display. There's various things around validation. There's also stuff around verification. And with respect to privacy proxy, there is an interim specification.

Now, the thing is, that while it is labeled Interim, you will also notice that in other areas of that document of the RAA, there is language referring to future replacements for various things, because we know that this group will provide some kind of output, and that that will be fed into some other form of policy development process.

So just to reiterate what others have said, I think that what we're going to do is going to take a long time for our output to be fully implemented and fully operational, and so pausing any other work would be a bad idea. But in terms of the risk type things, it's very important when people look at changing policies or working on policies or introducing policies, that they should be conscious of what will be impacted, what will be affected by those changes. Because there is an issue where potentially one or more entities or organizations within this entire thing, the ICANN community, could be working on the same thing at the same time or having an impact on the same thing at the same time. And that could cause more problems than it solves. Thanks.

Chris Disspain:

Thanks, Michele. So I think we're probably at the end of the Q&A at this point. If I could just remind everybody that we've got plenty more opportunities to make comments, lengthy comments in writing, in email, et cetera, and also face-to-face comments in Durbin at our special session on Monday. And I'd encourage everybody who can be in Durbin that's interested to come to the session and to continue this discussion and conversation.

And with that, I'll hand it back to Margie.

Margie Milam:

Yes, thank you very much, everyone. What we will do is have the recordings and the slides and the transcript posted on the webinar page. And then for those of you that are in Durbin on Monday, July 15, 14:45 to 16:15, we'll have a session that will focus primarily on the questions that we presented to the community to try to get information on how to do our work after Durbin. So we'd look to see you there, and you can also provide input at the email address that's also in our announcement. It's input-2-EWG@ICANN.org. And again, thank you very much for participating in this webinar.