
MARGIE MILAM:

Good morning, good afternoon and good evening to everyone. My name is Margie Milam. I'm a Senior Director at ICANN. It's a pleasure for me to welcome you to the webinar for today, which is answers to the top ten questions about the proposed Next Generation Registration Directory Services to replace WHOIS. 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 this time.

At the end of the webinar you'll be given an opportunity to voice your comments and questions during the question and answer section. The EWG will receive a copy of the chat transcript. Please note that the chat transcripts are being archived, and we ask that you follow the ICANN expected standards of behavior. Your lines are currently muted and will be opened at the Q&A section. IN the meantime, you're more than welcome to submit your questions and/or comments via the Adobe Connect chat pod.

If you do not wish to voice your comments or questions during the Q&A section, please mute your line by pressing *6 and then to unmute it press *7. The slides, the recording and the transcript will be made available following the session on the announcements page. Today we will more deeply explore the key features of the proposed Registration Directory Services – the RDS, as we call it, which is the foundation from which the gNSO and the community can develop a new global policy for gTLD registration data.

This is designed to protect personal privacy and ensure greater accuracy, accountability and transparency for the entire ICANN ecosystem. The

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.

goal of this webinar is to help you understand and ask any questions you may have about how the proposed RDS tackles some of the difficult questions, such as difficult data privacy issues, validation challenges that have often degraded data quality and accuracy, and also how it strikes a balance between access and accountability.

With that we'll turn to Michele Neylon, who will serve as a moderator today.

MICHELE NEYLON:

Thanks Margie. Good afternoon everybody, or morning or evening, depending on which time zone you're in. As previously mentioned, this entire thing is being recorded and if you don't want a public record of something don't put it in the chat because it's all going to be logged and published. You have been warned. Our Agenda for today's webinar: a basic introduction, to give you some background as to where this all came from. Then we're going to look at the top ten questions we've received in relation to our Final Report, which was published a couple of months ago.

We'll also provide links and some updates on next steps. Links to both the Report and various other documents. Then we'll open things up to a Q&A session. During the Q&A session you'll be able to ask questions either via the chat or using your voice and the Adobe functions. I'll be looking after that as well. Next slide. What is this EWG? EWG stands for Expert Working Group. It's formed from outside the normal process in that we were chartered by the ICANN Board and CEO. The question we

were asked to answer was, is there an alternative to today's WHOIS to better serve the global Internet community?

For those of you who've been following ICANN for a long time, there have been multiple studies and multiple Working Groups and other studies and research things and papers looking at WHOIS and looking at ways of fixing, changing, tweaking, various aspects of domain registration data – in other words, WHOIS. However, they were all looking at it in terms of modifying what currently exists. In the case of the EWG the idea was to start from the ground up. Rather than trying to fix what already exists, let's build something new, which would hopefully address all of the issues, the use cases, etcetera.

The Membership of the EWG was global; it came from a variety of different countries, and several of the EWG Members are joining me on this call today to go through some of these questions, so you'll hear lots of different accents. We come from a broad range of expertise, different types of backgrounds. We have people from all over the place with different experiences.

We worked together closely over the period of about 16 months or so. We had multiple face-to-face meetings, lots of phone calls, and hundreds and hundreds of emails. The statistics and the breakdown of all that is actually in the Final Report, if you're so inclined to have a look at it. Next slide please.

The EWG, our Final Report, we came up with this proposal for what we're calling the Next Generation Registration Directory Service. As it's ICANN we're getting ourselves a nice new acronym, the RDS. The idea

being to strike a balance between accuracy of the data, providing access to the data, dealing with issues around privacy, and also we introduced the concept of accountability within the entire system. Our proposed solution collects, validates and discloses gTLD data for permissible purposes only.

Now, this concept of permissible purposes only is something that is relatively new – the idea being that not all possible uses of domain registration data should be permissible. We know there are certain people or certain groups who might want to use domain registration data for nefarious purposes, for illegal purposes, or to do generally bad things. Under the current paradigm the access to domain registration data is pretty much open to the world. Anybody who wants access to the data can do a WHOIS lookup and there are no real limits around what data they're able to access.

We would think that as a result of this, the overall quality of the data isn't particularly good, nor are registrants' privacy rights particularly well protected. Under the paradigm that we're suggesting, the access to the data would be more protected through the purpose-driven gated access concept. All of this is covered in gory detail in the full Report, which of course you can download via the ICANN website.

At this juncture we're going to move onto the top ten questions that we've received about the RDS. At this juncture, I'll hand you over to Susan.

SUSAN KAWAGUCHI:

Thanks Michele. What makes the RDS different? We gave a lot of thought to this. Current WHOIS provides a one-size-fits-all public access to anonymous users. The RDS would require that you tell them who you are and why you need the information before you would have access to additional data. There is some public data that's available and we'll talk about that later. There's also little accountability or abuse remedies currently, and limited individual privacy protection or the ability to conform to differing laws. The rules engine in the RDS could conform to applicable law in whatever region the registrar or registrant resided in.

There's a limited ability to ensure data integrity currently, but the RDS would require validation of the data. There's a lack of security and auditing capabilities in the current WHOIS. Auditing would be much easier with one centralized source of the data. There's cumbersome contact management now. With each and every registrar currently you create your own registrant profile, but in the RDS you could use one profile, one set of data, universally, across all gTLDs.

There's inefficient communication – you don't know where your data is. You've got to remember which registrar you're with, and looking up a WHOIS record currently is cumbersome. The proposed RDS was designed to address all of these current WHOIS shortcomings and circumvent those problems. Scott Hollenbeck will present the next slide.

SCOTT HOLLENBECK:

Thank you. Scott Hollenbeck here. Question number two is, did the EWG choose a centralized model for the RDS? As others have mentioned, we spent a lot of time talking about many different things,

and one of the topics that we spent a very long amount of time on was exactly what a service like this could look like, and the different ways it could be implemented and deployed. If you look at the current slide you'll see a number of possible models. Without going into a detailed description of what each one is, if you look at the Final Report you can see each of these in very gory detail.

What we thought was that a synchronized model, which had formally been called "aggregated" would be the most efficient way to marry the needs of all of the consumers and producers, while allowing us to meet as many of the requirements as possible. We use the term "synchronized" because it describes the way data is being moved from producers to publisher in a consistent, secure, safe manner. We also asked IBM to look at these different models and give us a rough idea of the costs that might be required to implement and deploy each one.

The synchronized model came out looking very favorable. So in the end, this was the model that we suggest is the best way to meet all of the requirements for the community. Thank you. We'll now move onto the next slide. Stephanie?

STEPHANIE PERRIN:

Hi. It's Stephanie Perrin here. The next question is, does the RDS eliminate free public access to data? It certainly restricts public access to data so that sensitive data, personal information, is only available to persons who have become accredited and shown their legitimate reason to access that data. We're also proposing a rules engine that will enforce data protection law, which may not necessarily be the case in all

instances at the moment. There was concern expressed during our consultations that people would not have public access to the data they need.

In fact, they will still get the basic domain information and they will get names where the name has been released, and that would of course include businesses who have a keen and vested interest in releasing their name. It might not necessarily include individuals, depending on their relevant data protection and their choice, but there will always be contact data for technical resolutions, the key concern being the promotion of Internet stability and meeting basic DNS needs.

The short answer is it eliminates some free public access, but it provides the necessary free public access, and so people will still be able to, in an unauthenticated way, log on and get the information they need for basic domain registration questions. Onto the next slide. It's Scott again.

SCOTT HOLLENBECK:

Thank you Stephanie. In this slide we're asked the question, what would I need to do to access gated RDS data? As Stephanie described a moment ago, one of the recommendations we made is that there are some differences in terms of data that's considered available to the general public and data that's considered private and needs to be protected, and would only be disclosed under certain circumstances. If you look at this slide you'll see something called an "authenticated requestor". You may be wondering, "What exactly is that?"

Well, this is a person who requests credentials from an accreditor of some sort. We have a new actor introduced into the ecosystem. We're

recommended that there be agencies or entities that are authorized to receive requests, review them, and issue credentials for access based on stated permissible purposes. For example, a law enforcement officer would need to apply to an appropriate agency to determine if this person is who they say they are, and if they are authorized to perform queries, with the purpose of law enforcement access.

When a requestor requests to receive these credentials they can present them to the RDS in the context of making the query, where they will provide their ID, their purpose, and if the RDS can validate these credentials and request they will return a response that includes a combination of the public data and the appropriate gated data. Next slide. Susan?

SUSAN KAWAGUCHI:

Thanks Scott. What new data will the RDS collect? Today you'll see the image at the top of the slide is the current WHOIS data chart. With the RDS we looked at all the possible communication points and permissible use and decided on a few somewhat new concepts. Today, the new data that the RDS will collect is other communication methods. You could have your SMS listed as a data point for contact, or your LinkedIn profile – any other new communication method, as the Internet evolves. We also came up with the purpose-driven RDS, which is we've decided on PBCs – purpose based contacts.

There are several roles that we decided on, including abuse, technical, legal and business. You can designate third parties as your purpose based contact for those specific purposes. Those would be the contact

points for your registration. In the new data record associated with the domain name registration, available to the public would only be the registry and the registrar information, which is needed to manage and run the domain name, your registrant contact ID, and an email address associated with that registrant contact ID. You'd always be able to contact the registrant, but you may not know their name, physical address or telephone number without telling the RDS who you are and why you need that information.

Then the PBC contact IDs would be available, but just the ID numbers. If you needed to contact somebody for an abuse issue with a domain name, you would have to tell the RDS once again who you are and why you need it. So we've limited the public access of data, but by validating and verifying information in the data record, once you told us who you were and why you need it, you would get validated information to get that contact that you need. Onto the next slide.

LANRE AJAYI:

Thank you Susan. The question on this slide is, what are contacts and what are contact IDs? Contacts are simply the visible blocks of contact data. What are contact ID? They are unique identifiers that make domain names' contacts the contacts. Contact IDs are made available publicly to anonymous users, while contact data are mostly gated. [unclear 00:19:38] accreditation and authorization to be able to access contact data, in most cases. Whereas anybody can access contact IDs because they are made available publicly.

[unclear 00:19:55] accountability and stability [unclear] or via [unclear]. The concept of purpose based contacts. Every domain name must have some purpose based contacts and they must also have registrant contacts. Some of the purpose based contacts are mandatory for these domain names, like two of them are [unclear 00:20:32]. Every domain name must have their registrant contacts. They must have abuse contacts. They must have technical contacts, abuse contacts and legal contacts. Whereas [Internet 00:20:44] contact is optional. Privacy and proxy provider contacts are only required for those who need [unclear 00:20:54] published. Next slide please.

The question on this slide is, how would the RDS improve data quality, privacy and security? [unclear 00:21:19] to registrants to give accurate data, for the need of improving data quality. The RDS gives registrants and contact data enormous control over their personal data. The [unclear 00:21:35] ensure that their personal data, because [unclear], each data can be made public or [unclear] incentive for registrants to provide accurate data; thereby improving the data quality of the RDS.

More importantly, the [unclear] the registrant provides has to go through some form of validation to ensure the data is accurate. There are three types of validation. One is [practical 00:22:12] validation. Two, operational validation, and the third one is [identifier] validation. The [practical] validation is mandatory for all data elements. Operational validation is required for most of the data elements, while the [identifier] validation is optional. These are the measures that are taken to ensure that the data that's supplied through the RDS is of good quality.

I'd like to hand it over now to Stephanie to talk about how the RDS improves privacy and security. Over to you please.

STEPHANIE PERRIN:

As both Scott and Lanre have explained, there's a great deal more complexity in verifying who is requesting access to data once inside the RDS. That in itself is going to be of great assistance in protecting personal information so that it's not willy-nilly given out to anybody, and there is some accountability in the process. Apart from that, we've also recommended a privacy policy for the RDS that would stretch across ICANN in its interaction on WHOIS and data gathered for registration purposes.

We've also recommended that we create a rules engine that would automatically apply data protection in jurisdictions where the individual is entitled to it. That happens in some cases, but it's a bit hit or miss right now. This would do it in a holistic and hopefully easier for registrars manner. We have endorsed the concept of privacy proxy services, as a way of allowing an individual to ensure that their own personal data is not in the RDS.

We have proposed a secure protected credentials service for individuals at risk; persons whose lives or safety would be imperiled if their name and address were associated with the domain name on which they're active – and that covers a wide gallant of persons who are entitled to free speech. It also removes the registrars from the loop, where individuals or groups who might be pursuing people show up at the registrar demanding the name and address of individuals or groups.

That would be the most secure way of protecting your information and it would introduce the new concept at ICANN – namely anonymous domain registration. I think that sums it up. Onto the next slide please.

CARLTON SAMUELS:

This is Carlton. Central to our deliberation was the interest of registrants. They're a very important stakeholder group. The question is a direct, how does the RDS make life simpler for individual registrants? There are a lot of ways. I'll enumerate a few of them. Registrants will have more visibility into what their data is used for. Remember, it's purpose-driven access to the data, and so you'll know who's accessing the data at some point and what is the data being used for, because those elements that are gated, we would know who is qualified to access that data and what use they'll make of the data.

You have a lot more visibility into how that is used. You can still update in the new RDS, so you have virtually one point where you can go and update all of your data. That makes it easier. You have greater flexibility and control over what data is public. Because it's purpose-driven data access, you have options to deter fraudulent use of your data. You really give a place for all of the RDS users to see and learn about who you are as a registrant.

All in all, you get greater assurance without any niggling problems that have existed with the current WHOIS; privacy, data protection, security and all this. Policy is uniformly applied and you have some assurance of privacy, protection and security. Access to the data is limited to those with a need to know, and those that access your data will be held

accountable for the use of that data. We did think seriously about the benefits to individual registrants. Michele, next slide?

MICHELE NEYLON:

Thank you Carlton. I'm going to look at this in terms of costs, because obviously this is a key consideration. The question we have been asked is, how would the RDS impact registrar and registry costs? We looked into this in quite a bit of depth throughout our deliberations. From our perspective, the RDS should not be a profit center. It should not be away for anybody – ICANN or a third party – to generate revenue. It needs to be run on a purely cost recovery basis. It will cost a certain amount to run it, it will cost a certain amount to secure it.

All of those other things are not going to be zero amounts, but it shouldn't be a case of turning something that is at the moment perceived as being free, into a way of generating revenue. Now, at present there are costs in the system; in the current WHOIS, in the current way that domain registration data is collected and handled; both by registrars, registries, and by others. However, there might be a perception out there that it's free. It's not.

With our proposal, you move a lot of the responsibility that currently lies around both registrars and registries around the handling of the data, away from them. Specifically looking at gTLD registrars, registrars would no longer be obligated to collect or to validate the WHOIS contact data. The registrar would be collecting pre-validated contact IDs from registrants. You'd be getting an ID number of something, rather than

having to worry about is the address syntax correct? Does the postcode correspond with the town, and a whole lot of other issues?

Contact validation; the compliance aspects around that and all the data protection burdens, these would all move to the validators, because the registrars wouldn't have to deal with that at all. That would mean that the registrars would be able to get back to focusing more on the technical aspects of the domain registration – in other words, providing the DNS services, providing the other services – within the DNS. Both registrars and registries would no longer have to provide WHOIS services, because the data storage process and everything else would all move to the validators.

The Port 43 WHOIS, and other ports – because obviously there is Web-Based, etcetera, these would all shift over to the synchronized RDS system, but registrars and registries would be able to provide updates to the system over EPP, which as we know is the standard way that registrars and registries communicate. For the last slide on this bit I'll hand over to Scott.

SCOTT HOLLENBECK:

Thanks Michele. The last question, how will the RDS address WhoWas and reverse WHOIS needs? First, if you're not familiar with what reverse WHOIS or WhoWas is, let me explain that. With a traditional WHOIS query you ask for information about a domain name and you get a list of contacts. Reverse WHOIS flips that around a little, in that if you're given a contact you can ask about the domain names that that contact is associated with. WhoWas is a service that allows you to view and review

snapshots of historical information – for example, changes in name servers, changes in contacts and things like that.

Over the course of time, a number of providers have developed services around providing this type of information. How would that work with the recommended model that the EWG has come up with? That focuses on two things – data maintenance and data access. We are definitely recommending that the type of data needed to provide that service would be included in the RDS going forward. In the context of data access, let's remember what we said about private data and gated access.

There are bits of this information that we'd consider gated, and we're recommending that access to that data be provided only to people who have gone through the accreditation process and have credentials and permissible purposes that would give them access to that data. Next slide? Back to you Michele.

MICHELE NEYLON:

Thank you Scott. After going through all the FAQs and everything else, if you want to find out more about the RDS, our Report and everything else, there are a bunch of links you can look at where you can download the Report. If you're being eco-friendly we'd suggest that you don't print it, because it's incredibly long. You can read the FAQs, which are published online. We've also prepared several videos with Members of the EWG talking at cameras and trying to explain some of what we've done.

Now, next slide please. I'm going to hand this over now to Margie very briefly, who will talk a little bit about some of the next steps. Margie?

MARGIE MILAM:

Thank you Michele. Essentially, as you heard, the Final Report has been published. As this effort was requested by the Board, the Board is now considering how to use the EWG's Final Report as a foundation for the gNSO's PDP to develop the types of policies that you'd need to put together this new system. As you can imagine, with a 150-page document and all of the issues that are associated with it, it will be a very complex PDP. What the Board is trying to consider is how to collaborate with the gNSO to find a path forward to be able to manage the PDP so that it can be successful in looking at these recommendations.

In ICANN 51 in LA next month, there will be a session on Monday called "All things WHOIS". Among the topics that will be considered in that session will be how to run a PDP on the EWG recommendations for success. What we are interested in hearing from the community, especially at that session, is ideas on how to best structure that PDP so that it can be successful; so that all the issues that have been raised can be properly explored and that consensus policies can be developed from that.

That session will be open to the public on Monday and we'll be looking for feedback on the structure as well as the RDS; as it relates to the PDP. With that, I guess we'll open it up now to questions. Michele?

MICHELE NEYLON: Thanks Margie. If the operator could please unmute the lines? If anybody has questions, as previously stated, there are two ways you can ask them; either the chat function in the Adobe room, or you can raise your hand. If you are only dialed in over the phone, please just identify yourself and I'll put you in the queue. The first question we have is from Joly MacFie: "Who will the validators be?" I will put this one to Susan.

SUSAN KAWAGUCHI: Thank you Michele. The validators could be a variety of roles. They could be service operators that are completely independent from the registrar, or that registrar could act as the validator. It is a new role in the DNS system and we'd imagine that the validator service provider would also have contacts with ICANN, similar to what the registrars do today.

MICHELE NEYLON: Thank you Susan. Olivier, the outgoing Chair of ALAC. Good afternoon Olivier. You have the floor.

OLIVIER CRÉPIN-LEBLOND: Good afternoon Michele. Thank you. Just a couple of questions following up on this validation side of thing – as far as the costs of the validation service are concerned, would these be taken up then by ICANN?

MICHELE NEYLON: I'll speak to that briefly. Thanks Olivier. This of course is a question we've been asked by a lot of people. As you probably know, at present there are several domain extensions, which under their contract for a variety of reasons have extra levels of validation. For example, .travel, .xxx, recently launched this week, .organic, and there are others. All have an extra level of validation before the domain can go live. The costs of that validation are included in the registration cost.

If for example you look at the retail price of a domain name, then it's going to be in there somewhere. Does that answer your question Olivier?

OLIVIER CRÉPIN-LEBLOND: Yes. Can I follow up on the question of validation?

MICHELE NEYLON: As outgoing Chair of ALAC we'll give you a certain degree of latitude.

OLIVIER CRÉPIN-LEBLOND: I need to note that I'm only speaking here as an individual, not as outgoing Chair of ALAC. Just a question. Once the registration is complete, have you made provisions for the credentials to be verified regularly and so on? I can certainly see a number of ways you could get validated, and then you just change your data afterwards and that's it, you're validated anyway.

MICHELE NEYLON: Good question. Scott, do you want to speak to this one?

SCOTT HOLLENBECK: The only thing I'd like to add is that we had put out an RFI for information, to get an idea of what this could look like. Our findings were described in the Final Report. My own personal thought is that when you look at some of the people we talked to – law enforcement agencies, other types of associations – these are the entities that know something about their membership and the purposes for which they will need access. It seems just natural to me that they may evolve or eventually develop a validation role in this ecosystem.

MICHELE NEYLON: Okay. Carlton, do you want to speak to the question that Olivier raised?

CARLTON: Yes. I want to make a distinction between validation of data with accreditation. The validation of data, we'll look at RFI's, that look at how for example the ccTLDs validate their WHOIS data and commercial validators. We're talking about just verifying the data we get. The accreditation is a more extensive process where you're looking at the users of the WHOIS or RDS data, and ensuring that they're accredited for the purposes. There's a distinction being made there between validating the WHOIS data and accrediting the potential users of that data for the purposes that they are promoting they need access for.

MICHELE NEYLON: Thank you. I think the other thing, just speaking a bit more directly to Olivier's question, Olivier, you're talking about making sure that the data is current.

OLIVIER CRÉPIN-LEBLOND: Current and correct. Ongoing accuracy of the database.

MICHELE NEYLON: The basic premise we've discussed here is that if the validation and management of the contact data is being validated by the RDS then if you change it, it would have to be revalidated by that system. That's all handled over there. It's quite a bit paradigm shift from the current situation where the data is collected, stored and managed by multiple entities within the ecosystem. That wouldn't really be an issue.

I have two questions on the chat. The first one is from Luc: "Where and how would the RDS be hosted?" No, you didn't miss that, because we didn't actually state it. I'll go to Carlton because I think Scott has dropped off.

CARLTON SAMUELS: Thank you Michele. The thinking is that the hosting for the RDS would be in a jurisdiction that had a high privacy and data protection framework; that is the baseline that we thought would be necessary. It's also important to understand that we've not actually determined a place for that. We've simply, in the report, laid out some prerequisites for the hosting that we think would be necessary to make this work well. The

data protection and the privacy regime were two most important attributes to the host place.

MICHELE NEYLON: Thank you Carlton. Scott?

SCOTT HOLLENBECK: The only think I'd like to add is, as Carlton said, we aren't actually recommending anything specific at this point. I think the ultimate location and deployment of the service will be something that's subject to policy development and contracts and RFIs and what-not to be developed and shared and talked about in the future.

MICHELE NEYLON: Thank you. A follow up question we have here from Joly again. Could there be a mechanism that allows registrants to be contacted reliably, without necessarily revealing their data? I think I'll put that one to Stephanie.

STEPHANIE PERRIN: Let me be certain that I understand the question. Would there be a way of contacting people without their identity being disclosed? Even then there is a privacy proxy registration. We have discussed the parameters that are now being worked on in the Privacy Proxy Accreditation Working Group. We've discussed the recommendations for sending on serious matters to the registrant, so in other words, you could contact

them and even though you don't know who it is through the privacy proxy service provider... Am I capturing your question here?

CARLTON SAMUELS:

Can I add something to it? I think Stephanie caught that. There's a question of the privacy proxy and we're working through that, but there's one other way. If you notice we've added something to the contact ID, which is a unique number. We're presuming it would be recorded in the RDS record, and you could presumably use that ID to contact without actually knowing the name of the person that you wish to contact. That's one low level element that you could use to contact, and that is above and beyond the privacy proxy registration, and the [unclear 00:47:20] roles that are associated [unclear].

MICHELE NEYLON:

Thank you Carlton. Olivier, I see your hand so I assume you have another question.

OLIVIER CRÉPIN-LEBLOND:

Thank you very much. I have a question with regards to the data itself being there. As I understand it, the minimum data that will be available now to end users – I'm talking about standard users, not law enforcement agencies or anyone with any privilege whatsoever – but that minimum data that will be available will be less than the data that's available to any user on the current WHOIS system. Is that correct?

MICHELE NEYLON:

Thanks Olivier. I will address that in part. The answer I would say is yes and no, and I will qualify that. The concept I think a lot of people are having issues with is this concept of gating. Gating data does not mean that you are going to make people sign away their lives or get into complicated contracts or anything like that in order to access more data than a minimal set. The thing is also that some technologies that are implemented at present, we're simply making it clearer that these things exist, and we're actually highlighting them.

For example, if you were to do a look up on a .eu domain name, as an example, if you were to do a command line look up on that at present you would get back a very small set of data, but it would provide you with the information that a domain name has been registered, it would tell you which registrar the domain name is with, and it will give you the name servers, which at a technical level is more than enough. However, if you go to the Web-Based WHOIS, are run by the .eu registry, you can get back quite a bit more information as long as you "give up" certain amounts of your own information.

In other words, you go through a Captcha form so they're going to be able to log your IP address and various other bits of information. That is in many respects what we're talking about when we're talking about gating. It could be a simple matter than certain aspects of the data won't be open to the world the way they are now, but people might need to "jump through a couple of hoops" to access things. Scott, could you speak to this?

SCOTT HOLLENBECK: I don't know that I can add anything else, Michele. As you said, there's going to be a certain amount of technical data, primarily, that we're recommending is made generally available. The other bits will be subjected to the policies we develop around what is permissible, what is not, and how that all fits the different requirements that the community presents.

MICHELE NEYLON: Thank you. Is that okay? Does that address your question, Olivier?

OLIVIER CRÉPIN-LEBLOND: Yes. Thank you very much Michele. I do have another question afterwards, but I'll let others ask their questions.

MICHELE NEYLON: Julie Roth has a question on the chat: "Who is going to validate the accreditors and who is going to accredit the validators?" That's a horrible question. Sorry, it's a perfectly good question but it's got lots of Vs in there. Lanre?

LANRE AJAYI: Thanks Michele. I think it's the direct responsibility of ICANN to accredit the validators and the accreditors. I think there just needs to be actors that have to be accredited by ICANN. ICANN has the responsibility to determine who is qualified to be a validator and who is qualified to be the accreditor.

MICHELE NEYLON: Thank you Lanre. The other thing as well, just adding to this – and we’ve said this on a couple of points – a lot of the final details about how our proposals would work at an operational level and how they would be implemented are going to be subject to policy development processes. At a high level, we can say, “Obviously ICANN or a party selected by ICANN would have to do this,” but the actual criteria around that would have to be decided. Next in the queue I have Olivier again.

OLIVIER CRÉPIN-LEBLOND: Thank you. Last question from me for today, I think, before I go back to sleep, is with regards to IDN extensions. Has your group looked at any consequences of IDNs on RDS as far as the data is concerned and so on? WHOIS obviously, we’ve had plenty of work on that, but will that work carry over to the RDS?

MICHELE NEYLON: That’s a good question and I’ll answer it because it’s not a terribly complicated one really. Scott would have been the best person to answer it but unfortunately he had to leave. There’s been a lot of work around the alternative to the WHOIS, and in the number space with ARIN, RIPE and others, they’ve put in the RDAP and other things like that, which has full UTF-8 support and there are no issues there with IDNs.

One of the things that we also said in our report, and from our perspective this was a no-brainer, was that it has to work with IDNs. It

has to work, and there's no technical reason why it wouldn't. I don't know if there's anything else anyone wants to add to this?

CARLTON SAMUELS:

Let me add one little thing to it. There was extensive conversation about what the translation requirement would be; at one point it would be translated. Do you translate on delivery or do you translate on storage? That was a detail that we thought [unclear 00:54:25] implement, but the idea is that whoever requested the data, there would be some way of producing the data in a way that could be translated, so that they understand what they got back.

MICHELE NEYLON:

Thank you Carlton. Any further questions? We still have another 13 minutes. I can see Olivier is typing furiously: "Translation, transliteration and also what language does the frontend of the RDS have? What portion of the RDS system is multilingual?" Carlton?

CARLTON SAMUELS:

We thought about this a lot. One of the things that we thought is that it's easy enough to have a website where you have multiple languages, especially the six UN languages, but the thinking was that because there was [unclear 00:55:29] website you could have a scheme that could literally deliver the data in any language that you want. We're figuring out that by the time you get into implementing this, we'll have online translators and this will not be a problem. The ultimate objective is to have a translation when you need it, where you need it.

MICHELE NEYLON: Thank you Carlton. Any other questions? No?

CARLTON SAMUELS: I've just noted in the chat, but wanted to report, that the validators can also [unclear 00:56:18] language [unclear]. That's one way to deliver language support. You don't have to make it [unclear 00:56:27] synchronized RDS, but you could have local support from the validators.

MICHELE NEYLON: Thank you. I have Olivier again in the queue.

OLIVIER CRÉPIN-LEBLOND: Thank you. I heard we had another 13 minutes so I thought of more questions. Under what legislation will the overall RDS system run?

MICHELE NEYLON: Nice question. Thank you Olivier. Stephanie? Under which jurisdiction will the RDS itself run; the system as opposed to its parts, if you understand me. Under what jurisdiction will it operate?

STEPHANIE PERRIN: I don't want to make this more complex than it needs to be. Carlton indicated earlier that we were trying to house it in a jurisdiction with high data protection, however, you may be aware that there is litigation going on right now amongst the major corporations about in fact

whether data is accessible across boundaries, with or without court orders. The fact that it is ostensibly maintained in one jurisdiction does not necessarily mean that those rules are going to be applicable to manage access to the data. I think that's a general caveat on jurisdiction.

It's incredibly complex. We are aware of the jurisdictional study that is going on under Bertrand de la Chapelle, and we await with interest what he comes up with on that study. I'm not sure whether that effectively dodges the question or answers it.

CARLTON SAMUELS: It answers the question.

MICHELE NEYLON: Thank you. Another question on the chat from Olivier. He's asking who will own the data. I will throw this one over to Lanre.

LANRE AJAYI: These issues that are [unclear 00:59:03] but I think in my own opinion that the registrant owns its own data. I'm not [unclear] what are the [unclear] registrant's own data and [not] the RDS. That's my own opinion on this.

MICHELE NEYLON: Thanks Lanre. Susan, any thoughts on this?

SUSAN KAWAGUCHI: I would agree with Lanre that the registrant would own its data, but I think there's also something for the policy development. There are so many details to this whole system that the community needs to weigh in on.

MICHELE NEYLON: Thanks Susan. Just throwing in my own two cents, this is one where I think there's been a certain degree of contention in certain circles because some domain registries would try to argue that the domain registration data would be covered by database copyright law and things like that. They consider the database to be their copyright. That's obviously going to be in conflict with the right of the user to control their own data. Stephanie?

STEPHANIE PERRIN: Thank you. I've been well behaved, but this is a key issue and we should have perhaps given a little glossary in the back of the EWG Report on highly contentious issues. This is one, because as a group I don't think we ever reached agreement that ICANN was acting as a data controller. There are several data controllers in this model. The assignment of portions of the root, the assignment of all the technical parameters with a domain name – it's arguable that that is not the information of the registrant.

They have an interest in it, but so does everybody else. I think this is a huge policy issue that someone has got to take. In the next few weeks I hope we're going to see some clarification of which policy issues are going to be divided up. We had good questions yesterday from Chuck

Gomes on this whole issue of how on earth does the gNSO move forward with this.

MICHELE NEYLON:

Thanks Stephanie. Reading something in the chat from Joly MacFie he says there was a bit about no bulk usage in the spec. Speaking to that, one of the things that has to be aligned is the idea that data can't be abused. If you provide the data for one purpose that it's not being used for another... This is part of where the entire concept of this permissible purpose idea came from. There are lines that one should probably not cross. As Stephanie said, this entire thing around who "owns" the data is a contentious issue. It's not clear, and there are varying aspects to that.

Some people will state very clearly that it can be owned and others will say it can't be owned. I'm not sure if any of us are really qualified to make a judgment call on that. Any other questions? Speak now or forever hold your peace. That's not true, because you do get to share stuff with us and others in the LA Meeting during the Monday session, which is probably going to be held in the afternoon. Not seeing any other questions. Okay. Going once. Going twice. Okay. Thank you everybody.

The slides and other stuff will be made available online. If anybody has any questions or queries I'm sure you know how to contact most of us. For those of you who are coming to LA in person or remotely, don't forget there will be that session on Monday. Thank you all. Operator, you can stop the recording.

[END OF TRANSCRIPTION]