20140416_EWGWebinar_ID871

Margie Milam: Hello, everyone, this is Margie Milam and I'd like to welcome you to this webinar. This is the latest in a series of teleconferences for the expert working group that were produced to highlight the work of the group. The aim for this session is to be interactive, to have this be an interactive session with the expert working group, which is focused on identifying potential risk and benefits that might result if ICANN were to place the WHOIS system with a next generation system as suggested by the EWC.

Logistically, the way we're going to handle this webinar is that we will go through some slide presentations. That will take approximately 30 minutes of a basic outline and then there will be a Q&A. After the Q&A session, there will be five specific areas where we would like to get input from the audience with about 60 minutes.

Before we begin, I'd like to remind you of some housekeeping items. This webinar is being recorded, and if you have any objections, you may disconnect at this time. The session is being steamed through the Adobe Connect room, but if you intend to make voice comments rather than chat through the Adobe Connect, you need to join the Adigo Bridge. And if you are in the Adigo Bridge, please remember to mute your line if you're not speaking so that we can avoid any echoes. You can do so by pressing *6 and then to unmute, you press *7. And if you'd like to make comments or have questions during the session, use your hand raising option in the Adobe Connect room and that will put your name in the queue. And you can also put questions in the chat function so that the presenters can take note of them and answer any questions or comments.

And with that, I'd like to introduce our first speaker, Rod Rasmussen, the expert working group. Rod?

Rod Rasmussen: Thank you, Margie, and welcome to everybody on this Wednesday or Thursday, depending on where you are in the world. We appreciate you very much taking your time to take part in this webinar and your interest in the work we are doing, and we look forward to getting your comments, and questions, and your feedback, most importantly. The agenda, we're going to go over. We're going to (inaudible) some of the main goals of review, the -- what we're doing here with this working group and some of the key features of the RDS very quickly. And then we're going to do open Q&A, and then we're going to go into a feedback cycle around risks and benefits where we really want to get your input on the things that we're looking at from a risk benefit analysis perspective (inaudible).

The next slide, please. Okay. There we go. So just to review, the expert working group was formed a year and a half or so ago, or definitely a little over a year ago to really take a fresh start, clean slate, a linear euphemism, but really start from the ground up to take a look at domain registration, directory services, how that would work, or how it should

work, how it could work going forward into the future, into a much more robust and useful, and compliant with various laws and purposes, et cetera, around the world, kind of system.

So as mentioned, in this workshop we're going to get your questions about features as described and our latest state of update report and then go into the risk survey issues. Could I have the next slide, please. So as an overview, the RDS is, in the very basic form, is the ability -- provides the ability for various organizations out there to query a system to return this public verified and accurate information about various contacts that are associated with domain names. And also, for some users they've turned some gated data, perhaps some different authorization. And there's an example of what part of a (inaudible) right there. The URL for it, itself, is there at the bottom of the page and it is very accessible from the ICANN website as well.

Next slide, please. So at a very high level, the key features that we identified in our reporting up to this point as really to provide a purpose driven system so that access to data is validated by, or is at least a type of specific purpose that a (inaudible) might have. And they get access to the validated data around the contact for domain names and DNS -- associated DNS data. Some of those data elements will be provided publicly about authorization or any sort of other gating needed. However, other data that may be more sensitive and may be protected by the protection of et cetera to have to have some sort of purpose to be able to get access to that would be data so to accredited users who then identify themselves for the purpose of their access to the information and agree to be accountable for the information that they obtain through the system.

And the goal is to make that consistent with various data protection regimes throughout the world, to the extent possible. And we are also (inaudible) enhanced and kind of a high-level privacy option for registrants to be able to take advantage of. In general, the queries would come through a supervised web portal that provides obviously user interaction over the web and also RDAT type query access.

On the back end of that, it would be either an aggregated model where the data is collected together or some sort of federated model where data may be stored separately and brought together for presentation purposes.

So that is kind of the high-level overview of where we are with the -- and it's very high-level overview of where we are with the reporting. I'm sure there are questions. I'll move that to the next slide, if you would, please. And this is the -- your chance to questions that we haven't had a chance to answer yet or that you may (inaudible).

I'm going to turn it over to Michele to run that part of the session. Michele?

Michele Neylon: Thank you, Rob. Good evening, everybody. So if anybody has any questions or wants to make any comments, if you're on the Adobe Connect, I think most of you know how to use those. So it's wide open. You can ask us anything and we'll try our best to answer your queries. Well, I'm not seeing any hands, though I am seeing Mr. Bladel (ph) typing furiously. Okay. So a question from James Bladel. Who determined whether or not a purpose praxis is (ph) legitimate. I'll hand this one over to Rod, since I'm feeling evil.

Rod Rasmussen: So who determines -- I guess within the -- what we've done in the working group, we determined as a group what we thought would be potential legitimate uses for purposes to access data, whether that's in order to do some sort of a legal action like a UDRP process or some sort of technical issue where there's a problem with the domain name that needs fixing or some sort of need to handle abuse issues type of domain names, things like that. And there's a whole list of what we came up with as purposes for the document.

At the end of the day, though, it's going to be a policy development process that will determine how a system actually gets put in place. What we're doing with our working

group is providing suggested purposes that would -- and then providing a way to map that to various jurisdictions, et cetera, as far as how that would work within privacy law (inaudible) to provide either public or gated access depending on how that would work. So there's a fairly interesting matrix that you end up putting together. But at the end of the day, that's going to be codified by some sort of policy development. And then I would assume part of that policy development will also have the ability to create a process for determining new legitimate purposes, et cetera, that would be allowed as things change in the future.

Michele Neylon: Thanks, Rod. James, does that kind of answer your question? Thank you. So James has just put on the chat that yes, he's happy with that answer or he's happy that we've answered it. Anybody else got any questions for us? Come on, this is your time, the ultimate opportunity to ask us anything you want. Oh, Alan Greenberg, please, go ahead.

Alan Greenberg: Hi, can you back to the first slide or the previous slide? Okay. The aggregated or federated storage seems to be a --either the point at which this thing will break or the secret under which it will work. Are you planning -- are you actually going to any detail on the opportunities there? Or are you leaving that to the next group? Because it seems to be a rather critical part of it, especially in terms of gaming, access to data that people shouldn't have, and a variety of other sins or benefits.

Michele Neylon: Thanks, Alan. Who would like to take that one? Faisal, how about you?

Faisal Shah: Yes, I'll take it. I think that's right, Alan. I think that it's going to make it or break it, the aggregated or federated and that's on the back end. I mean we've been through. We've kind of gone into the risk and benefits and fleshed out as best we can where we think some of the gaps are in the federated and aggregated models. But in terms of the actual design itself, getting into how it sort of works, the nitty-gritty, we haven't gone down to that level. And I would presume that's implementation that's going to be left for another group.

Alan Greenberg: I have a follow on.

Michele Neylon: Go ahead.

Alan Greenberg: Yes, by aggregated I assume you mean one or a very small number of storage locations and federated, do you mean perhaps each registry keeps their own data or some model akin to that. Is that correct?

Faisal Shah: That's correct.

Alan Greenberg: Okay. Have you come up with any models for aggregated which seem to be viable? Because tossing it out as an option, I know in your first report you were implying if not suggesting an aggregated model and there were a lot of wholes shot in it. And I'm wondering is it really a viable model? Have you come up with any scenarios where it could be viable given the potential for problems with it? Otherwise, it seems to be a -- just confusing the issue by providing that option.

Faisal Shah: Yes, we looked at several different models and you'll see that in the status update report. One of the models was kind of this hybrid model, which was basically setting up regional storage centers, which was kind of a take between the aggregated and federated model. But I think as we started going through it, we started realizing that there were significant issues with that particular model. So we came off of it and went back to really recommending that there be two models, which is the aggregated or federated model. So Alan, if you go back to the status report, you'll see that we've kind of gone through several different models and some of which were recommended to us at some of the public forums that we were at. So we tried to (inaudible) as much as we could.

Alan Greenberg: Okay. I guess I'll read it in further detail. I'm still having a great amount of trouble how I can imagine a single storage anywhere that would not be subject to potential abuse.

Michele Neylon: Mr. Rasmussen, do you want to add something to Faisal's answer?

Rod Rasmussen: Yes, just a couple of points on the first that we actually had IBM do a study of various -- the two different major implementation models. So there was some actual thought put into how you could actually prototype this from a systems perspective. Not down to, like, real software do this and et cetera, but it was done to a level where it was looked at from a major systems components perspective for the two major model types we're talking about. So there's been some work done there and some really good reference material that IBM put together on how you might be able to configure those systems.

I think we have looked and you'll hopefully see that in our final output, at ways you could actually satisfy a lot of the issues around how an aggregated model would work vis-à-vis with data protection laws and transferring that data around. If the concern is abuse of data at any particular place, whether that's centralized or federated to just registries or something like that, those possibilities are always going to exist. It's a matter of how you instrument and protect those systems and then what level of risk you're willing to take. And that really gets it down to kind of the overall policy decision at the end of the day is what is more important, the risks you expose yourself to versus the benefits of the solution in one form or the other.

Michele Neylon: Okay. Thanks, Rod. I'm going to go back to James Bladel's query just to put on the chat there. One of the questions, since this effort is a "fresh look," did the EWG consider whether some types of data, for example, postal address, were no longer needed? Who'd like to take that one? I'll throw this at Fabricio.

Fabricio Vayra: Can you hear me?

Michele Neylon: Yes.

Fabricio Vayra: Very good. Thank you and thanks, Michele. Yes, it's a great question. So we actually have spent quite a bit of time talking about both what data elements are or are not needed. To give you an example, some of the questions have been could you substitute some data that's collected data today with, say, certain social media credentials because that's the best way of contacting you, right. We've talked about not only in the context of what is collective, but how that's represented. So obviously, one of the big complaints we have today is if a person goes in and registers a domain name, they often have to (inaudible) the same data three times over, not necessarily understanding what the other two, aside from their own personal contact information even mean to them.

So James, we have actually talked about if thing aren't necessary, maybe new things are necessary or better for contactability for a registrant at their choosing. And also, how that information, if collected, is even displayed for the right purposes. So hopefully that answers your question. And we, I think, believe we have in various places matrices on what is collected and what's optional to be gated and not gated, meaning now what's put out in public and what's not.

Michele Neylon: Thanks, Fabricio. James, is that okay or do you have a follow-up? Okay. Mr. Bladel is in a happy place. Does anybody else have any questions for us? You can ask us anything. I'm just, for the transcript, I'm noting that Olivier Crepin Leblond just commented that security would need to be tight. Carlton says that every configuration is subject to breach of one or another kind. Risk management is key in the balance of risks versus benefits as a driver. Rob is saying security needs to be tight at all levels, the attack services large with every registrar, registry having access in order to operate just like today. We don't really get away from that with either back end model, but we can better understand the risk profiles and exposures once you have a model established.

So no other questions? Okay. We've got plenty of time here for questions. I'm kind of leaving this open in case anybody wants to join in. Okay, then I'll hand things back over to Rod, then. Rod, back over to you.

Rod Rasmussen: I don't know that I'm next. Let me check the agenda.

Unidentified Participant: It goes to Carlton.

Rod Rasmussen: Yes, Carlton, I'm going to hand it to you.

Carlton Samuels: Hi, thank you, Rod. This is Carlton. I hope you can hear me. So we -- here's the thing, the EWG (inaudible) to provide a better informed recommendations and we think we know some things. We know we don't know some things. So (inaudible) survey is an attempt to crowd source a couple of things. One, we need to (inaudible) what we think we know and give us a chance to know what we don't know.

So it's a chance for you to tell us about risks and benefits that the RDS might have for you. You've seen what we have proposed. If you are in any way involved in domain name systems, you would (inaudible) participate in this survey, whether you provide or you use the registration data or so-called WHOIS data. Hopefully, at the end of this, we will get further and better information to refine our recommendations to reduce the risk and it will become input to a full risk assessment, which we contently did advise to ICANN before a (inaudible) system actually implemented.

So you see at the bottom there, we have a link to the risk survey. I hope it works. If it doesn't, call and ask, and we will sort it out for you. Next slide. So let's talk a little bit about the survey, purpose of the survey. So we're crowd sourcing, as I said. We're gathering input from anyone, anyone who may be impacted by the RDS, either in providing data or in using data from it. We intend to use this information for providing better recommendations from the preliminary analysis and the findings, and that will go into our final report.

And then if ICANN, through the usual development process, policy development process, intends to implement any of the what we recommend, then they would have to do a formal (inaudible). And we are pretty sure we will recommend a formal (inaudible). This will be a (inaudible) opportunity to analyze the risks that we identified from this original survey. They can look at ranking and prioritizing (inaudible) in a more professional manner than we probably would and they could do it (inaudible) themselves, looking at the impacts, the interactions between the various stakeholders and so on. And most importantly, they could then be informed as to what might be done to reduce the risks that are identified, or prevent risks that are not so well identified.

So it's the beginning of a process. We are, as I said, we are seeking to identify some risks. So once the survey comes back then we go through the next steps. Next slide. So we want to go a little bit deeper into the rationale for this risk survey that we are (inaudible) to produce. So we are going to explore some of the topics as we see them. We want to look at the risks (inaudible) that as you implemented either model or the new next generation RDS that we could be impacted in one way technically. The idea is that if it changes the way used or (inaudible) provided data, it may create some risks, new risks, and it might exaggerate some risks. There are legal and financial risks, naturally. For some of us, there are costs and to all of us there are legal considerations associated with the registration data. And we would know -- need to have a sense of what those might be from this survey.

Next one, operational changes. Well, naturally, once you use it to add data to it or retrieve data from it, speed, and accessibility, and availability are some issues around which you could estimate risk. We want to know about those. Security or privacy. This

is an -- this is (inaudible) really trying to grab you with the privacy issue. I want to disabuse everybody from thinking that we are only concerned about privacy issue in one jurisdiction. We are actually looking at privacy on the global level and we would wish to know or begin to have a better sense of what those issues might be in terms of security or privacy. And of course, going through all of this, we would get to a point where we would wish to know what could be applied to reduce risk and then increase the benefit from having this next generation RDS.

Next slide. So think about the risk and the benefit from the technical side. Start at the middle, tell us about you and there's -- on the right hand side, there are some questions that you would want to answer. And on the left hand side, there's some things that you anticipate might happen to you if you were to (inaudible) might need to change. And on the other hand, you might have registration data that might be easier to maintain and so on. If you go through the list of questions, this is just an indicative list of the questions that we would -- would pertain to the risk survey. There are lots of others that you might wish to conclude. We are encouraging you to include as many of them as we have not thought of. But the idea here is that we want you to tell us as many of the technical risks and the (inaudible) as you see them for one other implementation choice that we make in the RDS.

Next slide. Here again --

Margie Milam: Carlton, hi, it's Margie. I think the way we wanted to do this is to give everyone an opportunity to comment on each slide, each type of risk. And I think Michele wanted to add some specifics on this particular slide, the technical risk.

Carlton Samuels: I'm kind of (inaudible) to it. So. Should we go back to the technical risks and benefits?

Michele Neylon: Yes, let's go back to that slide. Carlton, please stand down. Okay, the -- as you know, there are dial-in options available for people and unlike during the preliminary part of this webinar, the lines are -- should now be open as well. So the thing here is that with the proposed changes, there's got to be some things that people might view as being very, very positive, some things that people might view as being incredibly negative. We thought about a few of them, which is what's on that slide. So a negative aspect is that you might no longer have anonymous public access to all registration data. The other side of it could be, well, as a registrant I'll be able to maintain my contact details more easily.

From other people who have access or need access to registration data might feel that with this system they're going to have better access to the data that they really need. And there's a bunch of different things that we've looked at from different aspects, both, but we are a group of people. We've taken input from various parties. So the questions we're asking you all is if you were users of WHOIS, technically speaking, what kind of impacts do you see in what we proposed, both positive and negative? And if there's anything you want to ask about the technical side of it, now's the time. My colleagues will be going through other aspects of this, as Carlton outlined at the beginning.

Carlton Samuels: Yes, thank you Michele. Maybe we had a little difference in understanding. I was told that we have six slides and we have to go through them in 10 minutes. So I'm afraid I may have misconstrued the instructions. My apologies.

Michele Neylon: Oh, don't worry about it. It's grand. I mean you want to do more work for me, I'm always happy to (inaudible), Carlton. Okay. So nobody has any comments or queries about this, on this slide? Okay, then. I will then hand it over to Faisal, who is going to talk about the legal and financial risks and benefits. Faisal, over to you.

Faisal Shah: Thank you, Michele. So as Michele stated, we all know that with the adoption of any new RDS system, there are going to be changes, positive and negative impact across a

number of areas as Michele said, and including legal and financial areas. So we're kind of focused on trying to get from you what risk and benefits you see in this particular area. For example, perhaps you think that there will be a risk that the RDS will be charging for certain types of services, ancillary services maybe for value add services. But on the other hand, perhaps you already paid for those services so it really doesn't matter. But maybe providing those services could have an impact on certain providers.

Perhaps you think that a new RDS will provide greater benefits than what we have today, potentially maybe an RDS that could accommodate diverse (inaudible) piracy law requirements as seen on this slide. Some other legal and financial risk benefits from this slide, the amount of registration data that's freely available might go down, might decrease. Potentially, could the RDS access logging notification components, potentially compromise active investigations. Now, we're not saying that this going to happen by any means. I think we're just trying to ferret out what are some of the risks and benefits of any RDS system today. And also, maybe from a risk standpoint, maybe you have to consent to centralized access or storage to registered domain name, and this obviously would come into play depending on what model is adopted.

Again, on the financial and legal benefits side, some other things to think about, proved quality of the registration data might reduce costly inefficiencies that are ongoing today. Also maybe the validator services might reduce validation expenses that are currently required. And more importantly, I think, is this is potentially something creating a whole RDS ecosystem where you might spark some kind of innovation and create some new business opportunities for people that (inaudible) today.

So let us know your thoughts here. It's open for people to comment on the risks and benefits that they see.

Margie Milam: If you'd like to make a statement, you can raise your hand and we can put your name in the queue. Okay. I guess (inaudible) to raise their hand. If you think that we haven't poached all of the legal or financial risks, certainly put some information in the chat, raise your hand, or participate in the survey. If not, I guess we can pass it onto Susan for the next item.

Susan Kawaguchi: Okay. This is Susan. Can everyone, can you hear me? Make sure I'm off mute. So operational risks and benefits. How can the change to the access to the registration data speed up your access or availability of the data in general. So the negatives, there may be, if there's a failure at the RDS, either at the aggregated or federated, you might have a delay in obtaining that data, being able to search for it and request it. You also -- there may be a few bottlenecks, your accreditation and the purpose you provide could slow down your ability to get that data.

Also, there could be a problem with synchronization. The registries will retain this data in their own database, but as they upload it and sync with RDS, however it's designed, then there could always be synchronization problems. But I think we have similar issues today anyway and that's what we're trying to overcome. So there may be more reliable high speed access to data. Everything is in the same access point. You don't need to go to a thousand different registrars or even five to ten different registrars to find most of the information.

Also, it should be -- the response time should be more uniform and predictable. You know what's available to you by your accreditation and the purpose. And so you will be able to predict what -- how quickly you can get that information. And then authenticated, real time authenticated access to gated data may be faster than today. Having accurate data in the registration data that you're looking for, the WHOIS right now, very inaccurate. So in the new record, you would have to sort through all the false data and sort of try to figure out the connection.

And possibility, depending on how this process works, there's revealed responses from accredited proxies may be faster. So I think with the change and with the vision that we're looking at today, it would -- there would obviously be some operational risks and risks to accessing the data. But there'd be so many more benefits.

So is there anybody else that has comments on risks or benefits?

Michele Neylon: Susan, there's a few comments in the chat, if you can see that.

Susan Kawaguchi: Let me see. I would agree, Alex. I know Alex Deacon, I note that these risks and benefits, operational or otherwise, can't be truly determined until architecture and even some implementation details are known. That's true. There's a lot of questions to what we're doing but because of the -- how we -- our mandate to think at the high level principle, getting into the weeds, and implementation is what we've tried to stay away from. Go ahead, Fabricio.

Fabricio Vayra: Yes, thanks, Susan and Alex, I saw that you agreed to Lisa's response, which is Lisa had put in that knowing which potential risks are important to everyone will help prioritizing them to complete design. In going through this, my approach, if I was outside this group, would be assume that we're dealing with two kind of frontrunner models, one being federated, one being aggregated. And answer from that standpoint. And obviously, if both are failed, there's a problem to both of them. Put that in the other category that we provide throughout the risk survey. But the risk survey is going to be really good in answering which kind of model maybe takes the front running on this. Because ultimately, as Lisa points out, if we know that the risks or those risks that are very important are noted very important to the majority of people, weight heavy on one model as opposed to another, it will actually help kind of decide.

Because as I see Alan writing here, and I think he was alluding to earlier, I mean there are obviously some very significant pros and cons to both models. And understand, yes, Alan, I know front running is a dirty word. I mean it in a context outside of ICANN but in the way that most people would see it in a business model. So from a business model perspective, front running a model, knowing which has more risks to the community or foreseeing risks to the community will help actually put forward a model.

So hopefully that helps answer things.

Susan Kawaguchi: Any other questions?

Michele Neylon: It's Michele. I'll make the comment, if you don't mind.

Susan Kawaguchi: Sure.

Michele Neylon: I mean just one of the things operationally speaking, as a registrar, both as a registrar providing who it services, it's a headache that you need to make sure that your WHOIS servers are up and responsive. And when you're trying to transfer domains to yourself, if the losing registrar server is having issues, that can be a problem. Whereas generally speaking, you don't see issues with registry WHOIS. So one can assume that this system would be as stable if not more stable than existing (inaudible) registries. So that operational problem would disappear. Thanks.

Susan Kawaguchi: Then it looks like I can't see any other questions. So we should move onto security or privacy risks and benefits.

Margie Milam: Now, Carlton comes back.

Carlton Samuels: Okay. This is Carlton again. So we want to have another look and see how the RDS could change or effect privacy of domain name registry data. We really need you to tell

us about you. Even if you think a risk (inaudible) risk or the benefits, the good things only apply to you, we want to know about it. So for example, you may believe that the registration data could be misused by the RDS operator. That would be classified as a risk. And later on, you might think that the registration data is more secure in a more uniform way and that's a benefit. That's a good thing.

If you think about them, you will come up with a list of them that you think are particular to you or (inaudible) on the risk side, the bad things side, on the benefits side, the good things side. We've just given you a list of questions we think you might wish to ask to stoke your thinking about what it is that we are looking for from you. Those are the impacts, I'm sure. If you think about it, you will come up with some on your own. Here's one that is (inaudible) to everybody, whether it's not if you (inaudible) state whether you are a natural person during your registration is a bad thing. But then again, if you wanted to have registered using secure, protected credentials, that might be a good thing. It all depends on you do the work.

Again, it's important for us to hear from you about what you perceive to be the risks and the bad things and what you perceive to be the benefits and the good things. And we'll open it up for questions now.

Michele Neylon: Go ahead, Alan.

Alan Greenberg: Thank you. One thing I don't think I've heard mentioned, the fact that the portal will be in charge of security policy implies that registries will be prohibited from making available the equivalent of their current WHOIS service. Am I reading that right?

Carlton Samuels: Anybody want to jump in there and answer that question?

Rod Rasmussen: This is Rod. Not necessarily. In fact, I think, I can't remember what the latest version of what our document says. Earlier, we were saying that you could have the registries published as well. I think that becomes more of a policy decision and it could even be an optional decision on the registries. But when you do that, you do -- you have the -- you lose that capability around gated access and all those other things. If you were to do such a thing, you would need to work on how you would actually transfer the rights, et cetera, that would be created using a centralized portal that that would create to let the registries take advantage of that system.

So it becomes far more complex to have the whole set of policies carry through and have the registries also be able to provide data. Now, in an alternate kind of thinking process there is they could provide things that would be normally available under policy that would be -- wouldn't require authorization, would be designated as public information anyways. So kind of almost if you could think of that as a different version of WHOIS in a way --

Alan Greenberg: The least common denominator information.

Rod Rasmussen: Right, right, yes. Exactly.

Carlton Samuels: Fabricio, I think you had something to respond?

Fabricio Vayra: Yes, I was just going to say, Alan, it's a great question and we've also heard it in the context of just registrars or WHOIS portals generally who are necessarily affiliated with registrars or registries. And Rod, no surprise, hit the nail on the head, which is that the perceived benefits I think from all sides on this are that as a community, we could decide or build systems that, say, in a privacy perspective could account for global privacy and security levels, right, appropriate to where a person resides. And once you start taking it out of that system, it becomes a lot harder to make sure that those privacy rules and regulations, filters, et cetera, are actually applied appropriately.

So I think you have to kind of weight the balance of the accessibility versus allowing one registry or one registrar, for example, just to go out and willy-nilly open up everything about WHOIS and kind of undo all the work and foundation building that you've built up, say, around privacy. The example would be if we built a rules engine, for example, or someone built a rules engine, we wouldn't do it, but if someone built a rules engine to go with an RDS that said that every registrant was afforded the utmost privacy according to their local laws. And then a registry went and decided to apply just kind of open WHOIS, you'd basically go back to the old regime where all that person's data would go forward despite the fact that that registrant may have said, I want nothing except the lowest common denominator information out there and everything else I wanted gated.

But I think it's an excellent question and one that I think needs to be flushed out because it's been asked now in the context of both registry and registrar, and just non-affiliated portals.

Carlton Samuels: Thank you, Fabricio. Faisal added one question and he thought that registry might get (inaudible) but only to provide non-gated data. So it's (inaudible) supporting the point you were making, Fabricio. Just one small thing that I might bring to the attention. If you notice that there is always the possibility that a registry may have (inaudible) requirements that are above and beyond both of the RDS for whatever the purpose internally, they would have to do that within their local law and jurisdiction or (inaudible) consideration.

But it could include something like some registries might need to have more than one piece of contact data. The RDS might require one piece. They might decide for whatever purpose. I can see that happening, for example, some of the branded (ph) registries (inaudible) how they go about making that -- those domain names available outside of the small group. So the good thing about this is that we are attempting to have some kind of global threshold for privacy and security. At the same time, there is some room available to make added extension either for privacy purposes or security purposes.

Michele Neylon: Carlton, if I may, just I know that Susan Prosser (ph) put something --

Carlton Samuels: Yes, Michele.

Michele Neylon: Susan Prosser from Domain Tools, this is something actually we discussed several times over the, I don't know, it seems like eons. So the question from Susan or comment, wouldn't the ability for registry/registrar to also publish data in conjunction with RDS create authoritative and accuracy issues? And this is something that we have spent quite a bit of time discussing. I think it also came up in our initial update to the community, possibly in Beijing, but somebody with better memory might remember.

And yes, the way we looked at this was that the RDS would be the ultimate accurate resource. I think it's in one of the previous slides that we threw up there this evening. We mentioned the potential for there to be sync issues. Like it could be a bit of a lag. So for example, if I were to change my email address with the system at 9 a.m. Irish time, the centralized system or federated system might not reflect that update for a period of time. Now, it could be a matter of a couple of a minutes or it could be a matter of a couple of hours. There could be that kind of sync issue.

So if you were having registries and registrars also publishing data then yes, there could be all sorts of interesting problems. And as others have mentioned, of course, or when it comes to matters of privacy, and all these things around accuracy and providing people with an incentive to provide good quality data, if you allow third parties to start publishing data that we were to consider to be privileged or gated then the entire thing falls apart. Thanks.

Carlton Samuels: Thank you, Michele. You've noted that Susan made a comment, further comment (inaudible) as you mentioned with the gated data elements.

Susan Kawaguchi: Yes, I mean my point was that the data is available if even if you are on unauthenticated, you haven't gone through the accreditation process, the very minimal dataset. If we haven't looked at that completely, but if a registrar or a registry provided that data, that small set, subset of data, and I'm not sure that would cause problems.

Carlton Samuels: Okay. Thank you, Susan. Alan, you have a hand up.

Alan Greenberg: Yes, I thought I heard someone else trying to talk.

Margie Milam: Was that Lanrie?

Lanre Ajayi: Yes, this is Lanrie. I just want to comment on that (inaudible) will not do a validation. Therefore, further validate and if the registries are not (inaudible) available, they are not (inaudible) go through validation and that will be a problem. So I don't really think they should be allowed to do that. I think the (inaudible) should be done by the (inaudible).

Carlton Samuels: Okay. Rod is saying that he needs to get off now. He has a hard stop and he's thanking everyone for showing up and thinks the questions are great. Alan, you can go now, sir, and then I'll hand it over.

Alan Greenberg: Thank you. A couple of things. On the authoritative, I'm not sure I can accept the concept that the portal is more authoritative than the registry when the data comes from the registry. So we perhaps need to think about that. What I put my hand up for, two separate questions. Number one, I presume your models will also be amenable to a registry, which had as a requirement and as something that the registrant must accept to register a domain name that all the information is public, for instance. If a registry says you can -- all the information is public then I presume they will not be prohibited from having a rule such as that, if that's applicable to whatever the model is for their TLD.

The question I wanted to ask is I think, but I'm not 100% sure that the only information that is really relevant to initiating a UDRP before the UDRP is actually initiated is the existence of the domain name and possibly the registration and ending date. Have you thought at all, though, to make sure that whatever restrictions you're going to put on are not going to inhibit the ability of a registrant to use the UDRP against other domain names?

Michele Neylon: I think Fabricio was going to respond.

Fabricio Vayra: I was going to respond to authoritative. I think I can take a stab at all three, Alan, if you like, or I can say it down, whichever. So on authoritative, I love the fact that you're asking this question because we've had some very lively debate over the past I guess now almost year and a half on this exact issue. And I think from where you're coming, you're absolutely right. Meaning the data that comes from the registry would be authoritative. Obviously, as they were the first receiver of that data from the registrants, right, registrar to, well, second, but registrar to registry. And then any data that, depending on federated or aggregated, to have that filtered up and communicated through the RDS.

The question we've had is really if you ask people to go through, and I think this links to your third question about filing UDRP somewhat, if you're asking people, though, to only use the RDS to actually gain access to that data, what's really authoritative because you end up creating this kind of infinite loop that because there's obviously going to be some sort of syncing delays, no matter how minute, you always run into this issue of I relied on the data through the RDS to file a lawsuit, or a UDRP, or send a cease and desist letter, or make a certain claim, et cetera. And the registry can always come back and say, oh, no, no, no, no, that wasn't actually accurate. The stuff I have on a separate server is actually

the accurate stuff. I passed on something different or it had been since updated before you sent your demand letter, UDRP file to your lawsuit, et cetera.

So I guess on the authoritative issue, I think you're right that -- and from the basis you're coming, that authoritative would have to necessarily come from the registry. But we also need to account for the fact that outside of that kind of ICANN process, the machinations of how the data flows from registry up to the RDS, the world, the public in general is going to rely on the RDS if the system goes through in either federated or aggregated as authoritative to them to do all outside of ICANN machination processes, right, communications with even defined cell domain names, things -- very simple things. They will consider that authoritative. So maybe it's a process of defining all this stuff.

Your third question was have we accounted for making sure that the information is accessible to go ahead and let people do UDRPs and things like that. I think we have. I mean it's definitely been part of our discussions. So you need to be -- obviously be able to continue doing things like UDRPs and contacting people. And the only question really becomes there, we've envisioned a world where you have gated and ungated. The majority of everything you find today at WHOIS would be gated.

So I would encourage you when going through the studies and making the risk assessment survey and any comments to point out where, since this is going to be purpose driven model, what would allow you -- make sure that your purpose is there to access data to file a UDRP, right. I think we've covered for it, but just make sure that that's there.

And I just lost your second question.

Alan Greenberg: The second question is more out of curiosity. If a registry had a model where all the data was public, would they be allowed to do that?

Fabricio Vayra: And I would throw that out too. I think that's really a question for the community and the PDP process because it almost comes back to this whole unraveling thing, which is do you want to -- and maybe there's no problem with this. Do you want to build a system where we say that we want to build -- from the get go, we've said there's a system now of accountability and checks and balances for everybody, both people entering the system, putting their data into those, holding the data, and those people accessing it. And does that -- does allowing people to write their own rules, despite the fact that they've made registrants aware that they've got different rules than kind of the general ecosystem, does that undermine everything?

And I think of it from many positions, but I think -- I constantly come back to, I'm sure you could build that. I'm just wondering if ultimately it rocks the foundation so much that it truly undermines a lot of the benefits, right, because people don't feel safe or feel like, wait a minute, did I use this registry now. It's that whole joke about the priest who gets two pieces of information and connects them publicly. From a privacy perspective, I'd hate just one registry to produce information that unravels the whole system for someone who went to great lengths to rely on a system to get privacy, for example.

Alan Greenberg: I guess I was thinking of something, and it may or may not apply, if you look at a TLD, which is restricted to health professionals or something. And the ability to find out who it is that's presenting the information that you're looking at is indeed part of that trust model.

Fabricio Vayra: And that's actually built into -- yes, and that's built into the models we have because we've -- yes, you have -- I think when going through the studies or putting in comments, I would focus on what's default gated, default public. And something that kind of rubs against -- up to what you're saying is we've discussed at great lengths, and I don't know what we've come to a resolution on which is this whole premise almost of when you have

a business versus an actual person, and could you or could you not self-select under the premise that, for example, a business who's gone out and gotten a business license would like to most likely default to and possibly should be required to present all of their information because they're doing business. The question then becomes how do you get at that self-selection or required selection.

But we've kind of gotten to that issue, but I would encourage you to put in some comments on that as well.

Susan Kawaguchi: This is Susan Kawaguchi. I'd just like to add onto that. We've definitely written some high level principles surrounding the registrant's ability to make all of their data in that registration data available to the public. And just from a personal point of view, as my role as Facebook's domain name manager, I would select that every time. I would want people to know and there may be critical business needs, like getting SSL (inaudible) to that would just make the process much easier if it's absolutely ungated. And to me, there's no benefit to a company -- to our company, at least, when we're using a domain name to have the information gated. We would want it all out there.

So but that would be registrant by registrant. But we've definitely added principals, which you'll see in the next -- in the final report that speaks to that.

Faisal Shah: Carlton, hearing no more questions, should I jump to the next slide, reducing risk, increasing benefits?

Carlton Samuels: Yes, sir. I think that would be a good idea. We've given them enough time (inaudible).

Faisal Shah: Okay, wonderful. So I'm going to go ahead and cover the next three slides, really focusing on the nitty-gritty of the risk assessment and the questions themselves and how this process will work. Hopefully, gear you up and better prepare you for when you do go through and do the study, the risk survey.

So slide 14, reducing risks, increasing benefits. As you go through and complete this online survey, it says here please consider these columns. If you were in Singapore and you heard me talk about this, I made the analogy that this was kind of like a funnel. When you read the survey, at first blush you'll look at this and say, wow, some of this is either redundant or either overlapping, or I'm not sure what they're getting at. What we try to do here is funnel through and you'll notice the questioning here. It's really focused on what's a potential impact, kind of what might impact you generally, and go ahead and select everything. And then you start to funnel down.

What of that larger check might -- and potentially what's a subset of that, that really most would impact you. And then from there, a further subset of those that would most impact you, what's actually likely to impact you. And then you'll note, we have this new to the RDS. So this is a risk that comes up only because of the proposal of the RDS. It doesn't exist today. And then we also put at the end of every one of these sections kind of an other that we want people to go through and submit other questions.

But really do think of it as a funnel, right. You start with a broad stroke of I think that these are all things that would impact me if they happened. Of those, what's most impactful to me? And of those, what's actually really likely to happen to me? And as you can see, if you look at it that way, it starts to really kind of pinpoint what is the most likely and most harmful risk.

Next slide, please. So next slide here, we have the risk assessment. This is a sample risk matrix that's often used with these types of surveys. This is just an example. It's not exactly what we'll use, but I think it's probably the simplest way of noting how a risk survey would be synthesized to be, to point out where the major risks are. And using one of the questions from the prior slide, the way this would work is if you had -- the question

was my registration data might be more vulnerable to external attack. Well, if everybody clicks this might impact me, but nobody then clicks on, it's most impactful to me and it's most likely to happen to me, obviously then it's unlikely and it turns green. Whereas if everybody had picked this might impact me, this is one of the two things that would be most impactful to me and I really do think it's likely to happen, then it shoots up the scale to likely and a major risk.

And then you can see here that things that rate high, red, would be intolerable risk level and they need immediate action. Things in the middle, yellow, would end up being tolerable risk, and that means that we need to try to do whatever we can to reduce practical within the system that you end up with. And then the bottom one, green, it's broadly acceptable but you need to monitor for further reduce or practical.

And obviously, going back to some of the prior questions, this would obviously help when you have a world as has been in our last update, we have a world where you have kind of two different models that seem to jump to the front of the pack. And once you synthesize a risk survey like this through a model like this, you start to be able to differentiate between the two a lot better.

Next slide. So we really are, and I hope this purposefully beats a dead horse here, right. We really want you to tell us what you think. I mean this really is all about the community. I think that we have some great expertise within the group and we've obviously gone at this for a long time with the best of intentions and tried to put hearts and souls into this project. But we're only as good as who's in the room. And we really welcome everything that you guys bring in.

So with the risk survey, obviously, we're trying to figure out what the risks are and more importantly, what your top risks are. So tell us, are your top risks unavoidable? Are they acceptable? Is there a way to shift or reduce those risks. And really consider do you -- are some of these risks acceptable because you're trading for something that's a benefit. Some of the things we've already heard back are concerns about having to accredit yourself to get into gated access. But the question -- a good example of this would -- are you okay with then accrediting yourself or getting a credential to access gated -- access if you know that that information you gain is always verified and accurate, as opposed to what you received today.

A question kind of flushed out with some of the questions Alan was asking earlier about an aggregated system, whether feasible or not, people really do worry about does aggregation lend itself to more fraud or tampering with data, et cetera, exposing data. And there, again, ask yourself the question, what is the real risk there as opposed to federated, but where there is a little bit more risk or more -- whatever the risk increase you think there is, is that outweighed by the benefit of streamlining data, applying let's say privacy rules, security rules more uniformly.

So with that, I think, are we pausing for quick questions before we go to the next steps, Margie?

Michele Neylon: I see Alan has his hand up.

Faisal Shah: Okay. Alan?

Alan Greenberg: Yes, thank you. Perhaps too late to change the survey now, but I really think it's an issue of perceived risks instead of just risks.

Faisal Shah: I think that's probably right and I'm hoping, and I'll let Lisa probably speak to this a bit more because she's really good at always (inaudible).

Alan Greenberg: The issue is, if you can't find a single jurisdiction in the world where everyone would -- which everyone would trust then an aggregated model is going to have real problems. And that's the kind of issue I'm talking about. Whether they're really trustworthy or not is moot. It's whether they're perceived as being trustworthy.

Faisal Shah: No, I think that's right and hopefully the funneling aspect of the questions, because it really -- so I took it, right, as one of the guinea pigs of it all and I found myself obviously taking it from the perspective of who I work for and who I represent, or the interest I represent. And that funneling effect of the questions really forces you to make some hard choices. I mean if you take it and be honest when you're going through as far as really struggling with it, right, I found myself doing that because I said, okay, well I really don't have to pick two. And about halfway through the survey, I could start seeing why this was funneled the way it was and hopefully it helps identify the true nature of risk versus kind of more perceived or I'm kind of worried about this, but I'm not entirely sure about it.

Because I think you'll get a lot of the perception in the first column, but as you start weeding down into the second and third column, it will really start identifying the real, real problems.

Michele Neylon: Olivier is in the queue.

Olivier Crepin Leblond: Thanks very much, Michele. Can you hear me?

Faisal Shah: Yes.

Olivier Crepin Leblond: Okay.

Michele Neylon: I'm tempted to say no.

Olivier Crepin Leblond: But you can. Okay. Olivier Crepin Leblond speaking. So thanks very much for this complete amount of work. It looks very impressive indeed. I have just a question and a comment. The first thing, and I might have missed that, but who is the owner of that database?

Faisal Shah: Can I put in on that?

Michele Neylon: You're going to have to. Go for it.

Faisal Shah: Okay. So I don't know that we've addressed this question exactly, but throughout the past year and a half, whenever we've discussed -- and obviously, this only goes to aggregated, because in the federated model, the system would only basically ping the registries to allow you a unified one stop shop at accessing all the data that's coming from different registry databases. But in the aggregated, who would own that, where we've come closest to discussing that is really under what agreement an RDS provider would have to live.

And so presumably within that agreement and based on I think community feedback through the PDP, there would be certain rules, right. So you build into the agreement that they have the data under license from, say, the registries, that they don't own it. However, they can't do anything or something like that. I mean I'm thinking off the top of my head, but I think that that would end up having to be almost like the IANNA agreement, right, who owned it and then how that was licensed out through agreements to ultimately the person running the IANNA, right, because they didn't own that data for a long time or the database and the functions.

So I think it would have to be dealt with under agreement and I think that we'd really want community feedback on that.

Olivier Crepin Leblond: Okay. Thank you. It's Olivier speaking again. So the reason why I'm asking this question is -- the reason why I'm asking this question is because the way that you planned it and so on, and the questions which you're asking here, very impressive indeed. But obviously, a lot of it will come down to how it's implemented and how things will roll out from that point onwards.

I don't know if any of you were around in the early '90s when the Department of Defense contract for the WHOIS services, or what was then the precursor to the WHOIS services was designed to go over to AT&T on one side, (inaudible) on the other, and I think it was General Atomics on the third side. The intent of the people who designed those things back in the day was all very positive and very good. And yet, some of the -- how databases turned out to be and so on, did not turn out how it was actually envisaged to be at the time.

So there's a historical side to it on the one hand, how things evolved, and at the same time, certainly, the ownership of that database, I recall the first amount of spam that I started receiving due to the fact that the database was (inaudible) with wildcards and so Canter and Siegel started sending their green card lottery spam. And immediately afterwards, while there was an uproar about this, at the same time, I remember receiving emails from what then became I think Network Solutions who started advertising their other services. And yet, all they had was the access to the database and to dotcoms. So there was initially, in the early '90s, never a thought that the database would be worth anything. And this is why I'm asking who is -- who would have the ownership of that database. That's the first thing.

The second thing is the jurisdiction under which that database would be held and I -- you have considered technical risks. You have considered legal risks, but have you considered political risks? And to expand on the political risks, let me give you an idea. You speak about law enforcement. Law enforcement is often seen as being just one type of stakeholder. But a response from law enforcement, let's say law enforcement in Russia would not be the same if the database was held in the U.S. as a response to law enforcement from a U.S. agency. And this is -- or a Cuban agency, or a Canadian one, or a French one. It's just the whole thing being the political risk of this -- those hold the knowledge, who hold the keys to the database will somehow be politically seen as bringing advantage to the country in which that database is "implemented."

And I hope I've been clear on that and I haven't mixed the issues a bit too much. But the great concern today is the optics of that database and the political optics to it, especially since we're now seeing that several countries in the world are seeing control of the internet as being a key issue.

Faisal Shah: So Olivier, I'm glad you brought that up and the reason being, I was addressing the pure ownership issue, but some of the issues you brought up, I think, would be addressed also by some of the things we've been most recently deliberating on, finding a mechanism that actually applies the privacy laws and data ownership laws to the jurisdiction of where that person who gave their personal data. So ultimately, if done properly, there shouldn't be a leg up to anybody who controls it. And in some ways, and I hate to use this term, but it's the only one that comes up, to some of the, I think, advantages of someone running this database may be perceived to have, they would ultimately be castrated in some ways because they wouldn't be allowed to transport data, move data, sell data, use data in any other way than, one, the registrant allowed them to. But two, as applied to the laws of their local jurisdiction.

So despite, you have two components running there. You have who owns the database and then also the person who gave their personal credentials and their local jurisdictions, which hopefully will ultimately curtail a lot of the examples that you gave and highly

restrict or govern how the data was ultimately used based on what the data subject allowed.

Olivier Crepin Leblond: May I follow-up?

Faisal Shah: Yes, please.

Olivier Crepin Leblond: Yes, thank you. So that's fine as far as the use of the data is concerned with regards to those local jurisdictions. What about law enforcement? Are you saying that law enforcement from Cuba would only be able to access data from Cuban registrations?

Faisal Shah: No. No, no, not at all. What we would be seeing is that there would be a filtering under which if Cuban authorities today were not allowed to get your information, say, from Europe or that they had a protocol that they had to deal with their local law enforcement to get that data, creating an RDS shouldn't change that paradigm. Meaning it might actually increase it because you're going to become more accurate right off the get go on what your local privacy regime is.

So my point is that creating this shouldn't allow you any further access than what is legally allowed today, and our change the process by which somebody would have to go through to obtain that data if they weren't allowed to, to do it today.

Olivier Crepin Leblond: Okay. So if Country X were to contact the database provider, whatever that company would be, and say, we need a copy of the complete database, we need it on that -- a local copy ourselves, the jurisdiction under which that database would be held would probably be a defining factor as to whether that would be possible or not.

Faisal Shah: Both the jurisdiction of where the data sits but also the jurisdiction of the data subject.

Olivier Crepin Leblond: Okay.

Faisal Shah: So it's not one faceted. It's multifaceted.

Olivier Crepin Leblond: Okay. Well, I'm hoping that would work. Okay. Thanks. I mean it's still very early on and I do appreciate that you're looking at this. So thank you very much.

Faisal Shah: No. Thank you.

Margie Milam: Alan has a question.

Alan Greenberg: Yes, thank you. Just to belabor the point that Olivier was making, and I think his reference, his allusion really was to what if I cannot trust the jurisdiction under which the data is stored, that the powers that be in that country do not necessarily honor their own laws or somebody else's. And that really becomes the crux of can we find a place for such -- can such a jurisdiction exist that is going to be perceived as trusted. That's my original question on the aggregated model when we started this whole talk.

Faisal Shah: The only thing I would say, Alan, I agree with you and what you're saying and I think that this should be up for discussion with the community because that might be one of the -- I mean if quite truly, we can't find any one or a handful of jurisdictions that people felt comfortable with, then maybe that's an undermining factor to, like you're saying, an undermining factor to an aggregated. Now, keep in mind, it's not just going to be a jurisdiction where that person is. I mean it could be the database might sit in Geneva, but the person running it is a, and pick whatever country you want, is an XYZ company located somewhere, which then also contracts with ICANN out of the U.S.

So in some respects, they may ultimately be subjected to some pretty punitive damages, or loss of contract, or what have you if they reveal the database. And so ultimately, what

you may be able to do is contractually, and with penalties amongst various jurisdiction, be able to put some hooks in to where despite where the database actually sits, you can trust in kind of a broad spectrum of different jurisdictions that would apply the proper pressure to incentivize someone to never reveal the data unless it was under the proper rules set up by the community.

Alan Greenberg: To be blunt, that would be easier to sell two years ago than it is now.

Faisal Shah: Yes, and I would just say, and just, Snowden keeps coming up everywhere, including in this chat. Let's just keep in mind that the Snowden event happened in not even a federated model. It happened in a completely holistic, privatized, disaggregated model. So what a lot of people who bring up Snowden argue for is exactly where the problem occurred. So I would just balance that out as well.

And I don't know if anyone is monitoring here, but Olivier also asked who would know if the spook agency was to request data. But so we've covered that as well, and I don't know if -- I mean you say it's a rhetorical question. Well, we have actually discussed this often and it goes kind of to the credentialing as it really goes to everyone, not just law enforcement, but an IP owner, the law enforcement IP shop, what have you. How do we know? And we're trying our best to figure out methods to make sure it's credentialed properly.

Michele Neylon: I think we're almost out of time now. So I think Margie, next steps, right?

Margie Milam: Sure. Okay. So try and get to the last slide. Okay. So we have some information on slide 16 that gives you information about the survey, where it is, the deadline for the survey is May 15. We've also provided links to the additional information, if you haven't had all your questions answered today. And the purpose is to get this all taken care of so that the expert working group can deliver its final report in June, right before the ICANN London meeting.

And so with that, this concludes the webinar. We thank you for your participation in this session. The slides, and the recording, and the transcript will be available on the announcement page shortly after the webinar. And again, please remember to participate in the survey. It's very important the expert working group hears about the risks and benefits that this model may have for you, and as I mentioned, the survey will close on May 15. There's also an email address that you can send information to the expert working group@input-2-ewg@icann.org.

Once again, thank you very much for your participation.