ICANN Transcription

Next-Gen RDS PDP WG

Tuesday 02 August 2016 at 1600 UTC

Note: The following is the output of transcribing from an audio recording of Next-Gen RDS PDP WG call on the Tuesday 02 August 2016 at 16:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. Attendance of the calls are posted on the agenda wiki page:

https://community.icann.org/x/uQ_bAw

The audio is also available at:

http://audio.icann.org/gnso/gnso-nextgen-rds-02aug16-en.mp3

Coordinator: The recordings are now started. You may now proceed.

Michelle : Great, thanks Zach. Good morning, good afternoon and good evening. Welcome to the GNSO NexGen RDS PDP Working Group call on the 2nd of August 2016 at 1600 UTC. In the interest of time today there will be no roll call as we have quite a few participants. Attendance will be taken via the Adobe Connect room. So if you're only on the audio bridge please let yourself be known now.

Great thank you. I'd also like to remind all participants please state your name before speaking for transcription purposes. Also keep your phones and microphones on you when not speaking to avoid any background noise. With this I'd like to turn the call over to Chuck Gomes.

Chuck Gomes: Thank you very much Michelle . This is Chuck and I want to welcome everyone to this call today. I do want to warn you that I am calling in from a small motorhome on a trip up to Northern California and Oregon Coast so if I have a few interruptions I ask your apologies. I will try to minimize them. But just want to warn you in case - when I'm not on mute, which is often for me, as chair you are - you understand what's going on.

So the agenda's up there. Certainly if there are any questions on the agenda we'll take those but before we do that are there any statement of interest updates? Please raise your hand if you have an update to your statement of interest. And of course as always remember to enter the, you know, to update your statement of interest online.

Okay not seeing any there let's go ahead and get started. The first thing we want to do is just give a brief progress update on the problem statement. And I see (Aiden) is on. (Aiden) can you give us an update of the problem statement since (James) is no longer a member of the working group? (Aiden) are you able to give us an update on the problem statement working group? Let's see is Alan…

Ayden Ferdeline: Hey can you hear me now?

Chuck Gomes: Yes, I hear you now. Thank you.

Ayden Ferdeline: Hi Chuck. Thanks this is Ayden Ferdeline. Just to update everyone we - the small group of us were involved in drafting this problem statement had a call last Friday to discuss next steps. And we're going to be regrouping this Friday. We're probably about a week and a half away from having a draft problem statement for everyone to review. But where we're at the moment is we've – we had two competing visions as to what we want the final statement to be. And we're just trying to bridge that gap and come to a common understanding.

So when we have our next call this Friday I think we're there. We're very close now so not much to share other than that. By this time next week we should have a draft published, a draft statement that we can share with the group that a more unified front if that makes sense.

Chuck Gomes: Thank you very much (Aiden). This is Chuck. Appreciate the work that the small team is doing on that. And if you do get 24 hours in advance of the working group call next Tuesday we'll talk about it in the meeting. Otherwise we'll talk about it with a full working group in the following week's meeting. Thanks again for the effort there.

The next thing under our progress updates is the triage possible requirements list. And I'm going to let Lisa give an update on that.

Lisa Phifer: Thanks Chuck, sorry just coming off mute there, took me a few moments. An update on the coding triage prelist possible requirements list. We have essentially put the further reworking of the possible requirements on the list on hold pending the definitions of the codings. As I began to try to apply the codings that Stephanie provided last week I realized that codings were probably based on the definition of the keywords themselves and that the individual possible requirements wouldn't necessarily map to the codes that Stephanie had suggested.

So now that we have those definitions I know that Stephanie circulated those to the working group mailing list yesterday for me. It was yesterday evening. Now that we have those in place the - I think we should all probably take a look at those definitions and see if we have any questions. But staff will try to go ahead and try to apply up the mappings into the triage list at least for the top three questions. We'll start there and see how works out and bring something back to the working group then to review.

Chuck Gomes: Thank you very much Lisa, Chuck again. And thanks to Stephanie for following through on providing the definitions on her in the categories she suggested and also thanks to (Susan) for providing the definitions for all of the categories that she had proposed. So we'll get an update again on that next week and then we'll have a chance of course if you take a look at the definitions that each of them submitted. If you have any questions or suggestions on any of those please do that on the list.

The main part of our meeting today is to discuss a few more example use cases. And remember that our goal is not to try and discuss every possible use case under the sun but rather to hopefully get a variety of example work use cases that will help us get a more comprehensive understanding as a whole group in terms of the various issues that we're going to need to keep in mind when were actually deliberating on possible requirements.

So with that said the first one we're going to discuss today is the one Number 9 as you can see in the agenda law enforcement compromised Web site at (Greg Mooney) submitted. And again let me caution everybody this is not the time to deliberate okay? This is the time to ask questions, to raise issues to look to share different points of view without debating whether which point of view is right or whether one's right and what's wrong -- whatever the case may be. But let's try and discuss these use cases honestly and openly and certainly without any criticism towards the person who prepared the use case. Our goal is not to make the use cases perfect but rather to discuss the issues that they raise then to add issues that we think of as we're talking about these. I see Shane Kerr you have your hand up. Go ahead.

Shane Kerr: Okay can you hear me? Hello?

Chuck Gomes: Yes I can. Sorry I was on mute.

Shane Kerr: Okay great, great. Sounds good, sounds good. Yes so before we start with the first use case here I noticed that several of the use cases almost seemed to me to be anti-use cases. So these are situations that are possible with current technology and maybe possible future technology which can result in bad things happening. I'm not sure what to make of that. Is that something that other people thought about? Do we have any thoughts about differentiating between those kinds of use cases?

I mean I think it's an interesting exercise to explore those possibilities because we can find possible problems and things like that but I'm not sure - I'm just not sure what to think about that. Maybe if anyone else has any opinions I be happy to hear them.

Chuck Gomes: Thanks Shane Kerr, good question. If anybody has some thoughts on that please raise your hand and we'll discuss that. I see Lisa has her hand up so we'll let her start.

Lisa Phifer: Thanks Chuck this is Lisa Phifer for the record. Yes that was actually an explicit goal of the use cases. If you look at the example use case wiki page and the description of what they are intended to be used for. They are intended to cover both uses that some people would like to see supported as well as uses that the system should be designed to actively deter. The reason for doing that of course is that for some of us in this working group there may be a gray area in between. Some people will support cases but others will not and it's good to get them all on the table. But the explicitness uses will be very helpful in designing security measures for the system and other precautions to actually limit access to data or prevent access to data that would - this group may determine should not be accessible to the system. So that would be the purpose of those use cases or misuse cases if you will.

Chuck Gomes: Thank you Lisa, Chuck again. And let's go to (Mark).

(Mark): Yes I - this is (Mark). I'd just like to make a tiny semantic suggestion. I'd like us to talk about cases that the policy should prevent as opposed to cases that the system should prevent. It's a minor point but I think the system is going to have to be built in a flexible way that accommodates a lot of these cases under near or circumstances.

You know, if you are this actor, if it is you are in this situation, if you are in a particular jurisdiction I think this situation - the system will need to be fairly flexible. And I'm not worried about that from an implementation point of view but right now since we're focusing on the policy that's what we're really deciding right now is, you know, the policy will determine what the system will ultimately do. And I know that's just a minor niche but I think it's good to focus on. I hope that makes…

Chuck Gomes: Thanks (Mark). Any other people that would like to respond to this? Certainly we don't want to just focus on the negative aspects so hopefully we'll have some balance in that regard. But as Lisa said the use cases can involve both what shouldn't be view - supported and what should. Okay not seeing other hands I'd like to ask (Greg) if he would just give us a not - I don't want you to raise the whole thing (Greg) but if you would just give us a brief overview of the use case you prepared to help get the discussion going on it? (Greg)?

(Greg Mooney): Thank you Chuck. Good morning, good afternoon good evening everyone. Can you all hear me?

Chuck Gomes: Yes. You're coming through loud and clear for me.

(Greg Mooney): Okay perfect. So just before the start I want to give you a little bit of context. I'm working for the European Police Office. It's called Europol. And I work the cyber division. So what I've done is I went to see the investigators entrusted in different teams and I said, "Okay we're working on this policy development process and the reform of the Whois. Could you please give me an example, concrete examples of one of the investigations you have been working on or you are still working on in which the Whois comes as a tool for you to do your investigation."

And so the first answer I received about two weeks ago was from the team which is working on child abuse Online. It's called Focal Point Twins. And so they said, Well that's interesting you're asking which is one of the cases that we've been working on recently in that case we've been using the Whois and Whois information publicly available information has been very helpful to reduce the range and the scope of possibilities in terms of investigative leads and was useful to pinpoint to a number of facts that are essential for the investigation to carry on.

So for those who haven't read the documents I mean it's – the very short document we found out and a number of investigators around Europe have found out that there is - there are a number of domains that they are in the clear with and that are distributing child abuse material. So if you go on the Web site -- and I still have a number of URLs so the Web site is still on -- then you will find a page with a number of pictures of young children that are likely lightly dressed. So it's not per se child pornography or child sexual abuse. But then if you start clicking in the link which is on the page then you get to another page where you have to sign up. And then for a monthly fee then you can have access to much more hard-core material which would in probably all jurisdictions fall under the title of child abuse material.

So what they've done to start with just their investigations they've gathered a number of domain names where the same modus operandi is applied and they found a number. I can't really specify. And then they started from there and they gathered three types of information. The GNS information linked to that - those domain names and they were using in particular domain tools that I suppose that a lot of you are using in your daily work to find the IP address which is associated to that domain.

And then they use the Whois data to try to identify and to illustrate those identifying domains. And when you crosscheck the three types or sets of information you find that there was one email address that was commonly used by the registrants to register the various domain names. So what the Whois data was used in that investigation and the start of that investigation which is still going on was to seek to prove and to show that there was one single organized brand that was that net - group that was running this business because this is a business of course.

So they've got no interest in hiding the Web site. They want the Web site to be there and they want clients to find it back. So that's also why they we're using these valued email address because they want that Web site to be posted with a host it is reliable. So the investigation is going on. I've asked recently whether they have issued in an (NLAP) request in order to get more information and they did. In particular they were interested in the bank accounts because that's also preventing (unintelligible) to trace back the (unintelligible) to try to gather as much information in that group as possible before their Web site is taken down. But they haven't received a request yet and the investigation is still going on. So I think I will stop here and I'm happy to answer your questions. Thank you.

Chuck Gomes: Thank you (Greg) for a very helpful introduction to this. And I'm now going to open it up - and this is Chuck speaking. I'm now going to open it up for questions or comments perspectives as we discuss this. So please raise your hand oh, if you'd like to talk. You can also of course put comments in the chat but let me open it up now and see if there are any questions for (Greg) are any comments on this particular use case?

I note Andrew's comment in the chat. And I don't know (Greg) if you want to respond to Andrew's common in the chat. What I understood you saying you actually are using lots of different information points but it might be helpful (Greg) if you could respond to Andrew's comment in the chat.

I know you weren't looking for a response Andrew but you raise a good point and I thought maybe it would be helpful if he commented on that because what I heard him saying is that they're really looking at different points of information. Email certainly wasn't the only one but in this particular case it appears to have been helpful to the investigators that were working it. Andrew go ahead.

Andrew Sullivan: Yes since I can talk faster than I can type. Thanks. The - so there are some things I think are really useful about this use case and I want to focus on them because they set up some possible future direction. What's actually I think like what actually is desirable here is to find the contact data of two registrants and find out whether they're the same and if not to find out what it is as such as I read this use case.

So the goal as I see it at least according to what I'm reading in this use case the goal is to identify that what you've got is a cluster of things that are all operated by the same people. And that's a little bit different. I mean the way that that's being done now is the way that Whois supports that. That is you query all of these things and get all the data back from Whois and then you see whether they're the same in some, you know, dimensions. And that tells you whether you've got the same thing.

But there's more than one way to do that right? I mean there are other systems that could permit that kind of a style of query without actually revealing the underlying data. And so I - that seems to me to be a valuable distinction that we could be drawing, you know, from this use case.

Chuck Gomes: Thanks Andrew. Rod go ahead.

Rod Rasmussen: Sorry I had too many buttons to push on my iPhone to get it to unmute. Just to – there's a couple of things to tease out of this as well, agree with Andrew on the primary use case there. It's really around correlation right, correlation. And then this in fact for building a case. You wouldn't necessarily be able to use this as direct evidence because it is easy enough to spoof somebody else's address. However it gives you if you have a series of things that you believe are interconnected and you can then tie them together through something like this type of data that gives you some probable enough information to issue (NLAP) warrants -- all those kinds of things that you need to get real evidence that can be then used in court right. So this becomes an important part in assembling a case.

I would also point out in this technique and again this child abuse material's was a case use here, this is a use for all sorts of abuse type of, you know, following the trail of the bread crumbs of abuse. I would also point that - point out that I think this use case also does something else in not just correlating things you know about but it'll also allows you to potentially go and find more things that you don't know about right? So if you have - if you start with a unique identifier like an email address and the email addresses are unique identifiers and may not be not – they're necessarily authenticated to a particular individual or organization but they are unique identifiers then you can then and we do this on a daily basis tracking botnets and the like is see when new domains are registered using that same telltale email address and you - then you throw that, go check that address and see if there's malware present. Typically there is and you add that to your security strategy. So that's - this use case also explores that.

The final point I wanted to bring up and is that you have this issue of an identifier like an email address which can be spoofed, anybody could go and add an email address to a Whois record or an RDS record or what have you. And certainly in a case like this you may be - your Web site may be tied or domain name more - to be more accurate, your domain name may be tied to some sort of nefarious activity. And if it's something like child abuse materials that could be very serious right?

So - and I believe I mentioned this in the list before one of the things that we talked about within the EWG was how could we provide some sort of mechanism for protecting yourself against that kind of spoofing? So this use case and an anti-use case example brings that – this of course as to why you might want to do that. So lots of stuff in there that ties up into lots of different areas. Thanks and now that was Rod Rasmussen for the record. Thanks.

Chuck Gomes: Thanks Rod. This is Chuck again, appreciate contribution. Anybody else like to jump in the discussion and hope everybody's watching the discussion in the chat as well. Any other questions or comments about this use case? Lisa go ahead.

Lisa Phifer: Thanks Chuck. This is Lisa Phifer for the record. I wanted to call your attention to the question in the chat that Maxim asked about whether this was a ccTLD or a gTLD and I'll let (Greg) answer that. And I also had a question. Reading the use case you talked about IT addresses being registered to individuals but I'm not clear on whether you're really talking about the IP address that would be the name server of the site that's hosting the material. And if other site that's hosting material are you actually talking about IT Whois rather than domain and Whois? Can you sort of connect the dots for me there? Thanks.

Chuck Gomes: (Greg) can you respond to those questions?

(Greg Mooney): Yes, thanks Lisa. Yes maybe just this for Maxim what was the question again?

Chuck Gomes: ccTLD…

Lisa Phifer: ccTLD…

((Crosstalk))

(Greg Mooney): ccTLD sorry, it's the gTLD. And then for Lisa yes it's the IT of the server which is hosting the Web site that's - so yes.

Chuck Gomes: Thanks. Thanks (Greg). Jim go ahead.

Jim Galvin: Yes thank you. I want to say - kind of restate with both Andrew and Rod have said and I'm looking at the discussion in the chat room here. And I apologize, this is Jim Galvin for the record here. You know, important thing to take out of this is what Andrew started by saying which is this use case more generally is about data correlation. That's what Rod called it and I like that.

You know, I mean in our experience in working with law enforcement and other folks on anti-abuse cases, you know, it's really about being able to see the data and match it up with other data. So things like email address and even IP addresses they are unique identifiers but they are unique identifiers in a technical sense. And that's the way to think about it. That's a unique identifier certainly because by design, you know, in their creation and in their intended use in an application on the Internet they are unique. And they get you to a certain kind of endpoint.

Now in context whether or not that's unique with respect to an organization or a person or what's on the other side of the technical endpoint that's a different thing. And I think that's where we often get confused and people forget that although I have an email address it doesn't mean it's a single person. As Andrew was pointing out in the beginning there could be multiple people behind that email address. And Rod said that too. There could be organizations. So the qualifier we put there is they are technical unique identifiers because that's the way they're designed. They're not necessarily applied in that way. They're not applied in a unique way because context matters there.

And the law enforcement use case here is all about being able to correlate data. You want to aggregate all of the various contact information registration data that you can get and that becomes a jumping off point for the next step in your investigation. It is rarely an endpoint this process except to the extent that, you know, the malicious actors here are, you know, not being very smart about what they do. Thank you.

Chuck Gomes: Thank you Jim. This is Chuck again. And note the good discussion in the chat with regard to Whois for numbers and Whois for names. Hopefully everybody's aware of that but if you're not that point was made while the chat and other points as well. So any other questions or comments with regard to this use case?

And Jim I'm assuming that's an old hand? If not speak up. Okay thanks. So I noticed that a lot of discussion about the word unique. I like the way Jim said it with regard to unique from a technical sense. That doesn't mean as somebody as (Cal) just pointed out that an email address is only associated with one domain name. I - hopefully everybody understands that. It could be associated with many domain names and that's not what is being said about unique care. Stephanie it's your turn.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. I just wanted to add under the section Privacy Implications while I absolutely agree that what was being said about the uniqueness of the technical unique identifiers they are considered to be (null) information in a data protection law case. So I think that that needs to be in the section under Privacy Implications. Yes they may or may not be unique in the sense of pertaining only to one individual but if they do pertain to one individual than they are personal information, just wanted to make that known. I think generally the privacy implications should always dissect the data as an office would in investigating a complaint but I was going to make similar comments on some of the other use cases. Thanks very much. Bye.

Chuck Gomes: Thank you Stephanie, Chuck again. Any other thoughts or questions on this use case?

(Susan): Chuck this is (Susan) and I'm off of Adobe Connect right this second but just two comments. I actually to Rod's point that sometimes people feel other Whois information users information, you know, I submitted a use case about that, the current one with somebody registering a domain name with all of Facebook contact information including the email address and only difference was with servers and with, you know, checkpoint. And then we found they were using it to harm Facebook users so - and it's a battle I'm dealing with, with a registrar right now.

But the other issue is Stephanie's point on this use case is the, you know, privacy concern and personal information if it's a commercial entity then that may not be personal information so it depends on what – who's the registrant is whether or not there are extended privacy considerations that we need to take into account. So I think we always have to go back to the registrant, see how they've declared themselves and then the privacy consideration should be attributed to that.

Chuck Gomes: Thank you (Susan) and thank you for jumping in since you're not in Adobe. I saw your hand earlier and you must have disappeared because you dropped off so I appreciate that. The – any other person would like to speak here? Lisa go ahead.

Lisa Phifer: Thanks Chuck. Just one other quick thing. I had put it in chat but I was wondering if (Greg) could provide any insight into whether for this kind of illegal purpose whether they are finding many of the common – those common email addresses actually belonging to privacy proxy providers rather than an individual that might be actually putting content on the site?

The reason that I ask is -- and I know you know this Chuck -- but there was a study commissioned on Whois privacy proxy abuses that looked at the various kinds of criminal activity and the correlation between those and use of privacy proxy services. But of course (Greg) has a real life example here and I'd be very interested whether they ran into that in his case?

Chuck Gomes: (Greg) this is Chuck. Feel free to respond.

(Greg Mooney): Hi. (Greg Mooney) for the record. Thanks Lisa. Yes also and we found cases where privacy and proxy services are being abused. But in that case it wasn't and that's why I put the small bullet points because you could think, okay, if you really want to hide your trace then you would probably use privacy and proxy services, but in that case they haven't. And we think that it's because the domain is hosted on the server which is in the jurisdiction which is not cooperating. And that's also why some of the investigators working the case are still waiting for and the judges as well waiting for the outcome of the – in that which will probably not come.

Chuck Gomes: Thank you (Greg). I'm trying to bounce in and out of mute as well so I was a little slow. So any other discussions? Let me complement (Greg) on the use case because it's generated excellent discussion that illustrates the kinds of things that we're going to have to keep in mind as we do our deliberations. So it's been very successful in that regard in my opinion so appreciate that. Any other thoughts?

And I won't try and repeat everything that's going on in the chat. There's a lot of good discussion in the chat as well and that's appreciated. Let me just pause just 30 seconds or so to see if there's anybody else who wants to speak. And not seeing any hands let's – oh here we go, Maxim go ahead.

Maxim Alzoba: Maxim Alzoba for the record. I think in this use case we need to enhance other elements that request because nobody knows which particular fields will contain some patterns that might help investigators. So I think that element should be broadened to the all fields of the RDS in question. Thanks.

Chuck Gomes: Thanks Maxim and again we're not trying to fix the use case descriptions themselves but rather to discuss them. So but that's a good point to make like Stephanie made with regard to the privacy implications. Anybody else? Okay then let's move on to another use case. The next one we have is Number 10, the dissident group using Internet to communicate. Ayden Ferdeline submitted that one and I'm going to – it's is being pulled up now as you can see. And I will call on (Aiden) to do what (Greg) did and give us a brief overview of this just to get the discussion going. (Aiden)?

Ayden Ferdeline: Sure, thank you for that Chuck. This is Ayden Ferdeline for the record. And so I do apologize if there's any background noise at the moment. I'm in a - not in the quietest place. But just (unintelligible).

Chuck Gomes: So we seem to have lost (Aiden) there along with the background noise. The - (Aiden) are you still on? Okay (Aiden)? That may be the case Greg Shatan. We don't know. And maybe a beer spilled on his laptop okay. While we can conjecture a lot of - so let's just – I'm just going to pause about 30 seconds. If (Aiden) doesn't - isn't able to rejoin us here what we'll do is we'll go to the next use case and come back to his later.

And let me say I hope we all appreciate the sense of humor that we're seeing in the chat right now. We're going to all need to have a good sense of humor as we do our job in this working group. So that's highly encouraged. So okay (Aiden) are you back?

Okay then what I'm going to do is we're going to move ahead and we'll come back to (Aiden)'s later to Number 14. And we could pull up Number 14 which is Whois queries for compliance purposes. And (Terry) I'm going to ask you if you would - thanks for submitting this one. If you can we'd appreciate you giving us the – an overview of this and then be prepared to respond to questions or comments on (unintelligible) comments that are made. (Terry) could you go ahead please?

(Terry): Yes. Can you all hear me?

Chuck Gomes: Yes there appears to be some background noise. I don't know if that's from you or whether somebody else needs to mute their phone. So if everybody else would please mute their phone until you want to speak that would be appreciated. Go ahead (Terry).

(Terry): Okay so the use case submitted involves what we investigate regarding transaction laundering which is an individual applying for a merchant account, establishes a Web site typically selling general goods as in the use case I submitted, Amish teacups, buy puppies online and then utilizes that domain name to transact, to do transactions for other types of goods which are not necessarily legal. As in this case this individual that set up the merchant account also had sites, prescription drug sites and the K2 bath salt online on Psychoactive high Web site to sell those goods but utilized the Amish teacup domain name to process the transaction.

So when we do these types of investigations to see if the Web site was in compliance at the request of banking institutions we find that one of the first things we always do is look at the Whois record for the domain name to pull out all the identifiers that we can. So that the email address in this case was what led us to finding the other domain names by doing reverse Whois on the email address. So it's important we can use any of those - any data elements listed in the Whois records we do reverse queries on to identify any other domain names. And this typically leads us to the owner of the Web site.

Somewhere in the records you find -- and it takes time obviously to analyze all of the data and pull all of the records out, historical Whois records whatever we need to pull out -- to drill down and find out as much as we can to make sure these folks are legitimate, running legitimate business and processing transactions for legitimate goods.

Chuck Gomes: Thank you very much (Terry). Now just a logistics issue. At least in my case I note that I'm not able to scroll so if everybody could be given scrolling capabilities so that they can – there we go. Thank you very much. Now let's open it up for questions or discussions on this use case. Any questions for (Terry) from anyone in the group please raise your hand. And of course again discussion in the chat is welcome as well. I think it's still going on from (Greg)'s use case so…

Lisa Phifer: Chuck this is Lisa Phifer. My PC has decided it needs to reboot so I'm on audio only at the moment. If I might ask a question to (Terry).

Chuck Gomes: Please do.

Lisa Phifer: I wanted to make a clear (Terry) the primary actor here is the merchant monitoring solution provider or is it an end user, any user of the Whois? That is could this be this case be narrowed just to that merchant monitoring solution provider or does it require public access? And then the second question that I have is if you're aware of any jurisdictions that actually require the ability to provide this kind of anti-fraud service? Thanks.

(Terry): Sure. Well in this case of – it's private industry accessing their data. I mean anybody that is looking up Whois records to find out a user of a domain name obviously the first thing they do is look at the Whois record for the domain name. But in, you know, in this aspect the merchant, you know, were private industry contracted to perform investigative services, you know, they say, "We need to know, you know, everything we can about this domain name. We want to make sure, you know, that these folks remain compliant with our regulations so give us the information." So that's the, you know, private industry needs to have access to Whois records for that purpose. What was your second question I'm sorry regarding jurisdiction?

Lisa Phifer: Again this is Lisa Phifer answering your question. My question was you mentioned that there are some regulatory bodies that, you know, get involved with anti-fraud protection like this. I was wondering if you knew of any jurisdictions that actually required the availability of this kind of service even though it's provided by private industry?

(Terry): No I do not.

Chuck Gomes: Thank you for responding (Terry). Andrew go ahead.

Andrew Sullivan: Thanks. So I want to come back actually to this question that Lisa started with because I'm not sure that actually the first answer really answer the question because the use case just like in the last one where we saw actually what the use case showed that there was a correlation that was the real goal. And so this use case is arguing no it's the raw data that is necessary and it's all fields because that's how you do the investigation right now.

So there are two things that the first is just a comment that essentially you're arguing from this is how we do it now so we have to continue to have that kind of access which I'm not sure is an argument that is sustainable. But more importantly it seemed to me that the fundamental question was whether it would be possible to have this be a limited service so that for instance if you were the kind of service that did this sort of performance monitoring then as part of your terms of service, you know, you could require somebody using a domain name under those services to consent to this kind of thing and then you would be authenticated to do the lookups on those names. And that would mean that you wouldn't necessarily have access to all of the public Whois but only authenticated access under certain circumstances. And I'm trying to understand which kind of use case would work here.

Chuck Gomes: Thanks Andrew. It sounds like some people are having trouble raising their hands so if anybody is having that problem speak out at a hopefully appropriate time. I know sometimes that's hard with so many people on the call but just do your best because I don't want people to get left out if they can't raise their hand. Marika please go ahead.

Marika Konings: Yes this is Marika. I just had my - I raised my hand and sort of object for using staff difficulty getting in the queue.

Chuck Gomes: Okay thanks.

Geoff Noakes: Yes Chuck this is Geoff Noakes with Symantec.

Chuck Gomes: Go ahead Geoff.

Geoff Noakes: So in our role as a certificate authority -- and this is true of all legitimate certificate authorities -- when we received a request to issue a digital certificate from either an entity like a company or an individual one of the very first places we turn to for information is Whois. And Whois ends up being sort of a treasure trove of information which we can use to correlate and relate to sources from other data providers, you know, are we talking to the person we think we are talking with? So I think that is sort of similar to what the use case that was talked about by Lisa earlier. Thank you.

Chuck Gomes: Thank you. Anyone else like to jump in on this? I see (Aiden)'s question in the chat what makes a certificate authority legitimate? How are they accredited or how does this work? I'm not sure we need to answer those questions right now.

Certainly if we decide somewhere down the road here to establish a requirement that relates to certificate authorities and ultimately any policy in that regard we would have to deal with the authentication issue. So it's certainly one that can't be avoided if we go that direction in the future so…

Geoff Noakes: This is Geoff Noakes at Symantec again. The likely authoritative place for that information for legitimate CAs would probably be a combination of the CA's recognized by the Certificate Authority browser forum and/or the root stores that are in the major browsers.

Chuck Gomes: Thanks Geoff this is Chuck again. Any other - anyone else like to jump in on this use case either asking questions or making comments or sharing different perspectives? That's all welcome right now? Jim you're up.

Jim Galvin: So this is Jim Galvin for the record. I just want to repeat I'm watching the chat room here again and going back to Andrew's comments earlier we haven't heard an answer to his question about, you know, this particular use case compares to the prior one. We had gotten to a place of talking about how in the prior one, you know, being able to correlate data was kind of the goal. In this case it appears that the goal is itself as a single set. And trying to understand if this is a situation where differentiated access would help us so authenticated access to get at all the data or is there some other critical characteristic that's being presented here in this use case? We appreciate some discussion or an answer towards that from (Terry) who, you know, presented the use case. Thanks.

Chuck Gomes: Before going - this is Chuck. Before going to Shane Kerr (Terry) would you - can you respond to that?

(Terry): Yes it does - it relates to users and purposes being one. You know, it's not just, you know, law enforcement that does investigations. Private industry also does investigative services, compliance services requiring access to Whois information that relates to gated access on what information we're able to obtain in the Whois record. It also relates to correlation because you are basically doing an investigation correlating all the data that is now available in Whois information. So it relates to all three of those things.

Chuck Gomes: Thank you (Terry). (Unintelligible) we're getting some background - there that's gone. Okay thank you. The background noise is gone. I don't know if it's - I hope it's not my line. So certainly Jim if you want to come back and follow-up further that - if that question - if you have more on that you can. Just jump back in the queue. Shane Kerr let's go to you now please. Shane Kerr? All we're hearing is background noise.

Shane Kerr: Okay. I guess my question is I think closely related to the one that I think (Terry) possibly just tried to answer. And I guess my question is what kind of flexibility are we looking at right now in the process in terms of modifying use cases? For example I could see an alternate version of this use case which instead of gated access required some sort of authentication token.

So for example in many countries we have the concept of a credit check which is when you go to buy something and you need to borrow money for it you authorize the person lending you money to do to look into some details about your background. And because they're authorized to do that they can get access to these details so you kind of pass the credential which is I think would kind of go towards resolving the underlying need of this use case but of course is a very different way to do it then gated access. So is that - should we - are we at the stage in the process where we should just kind of except the use cases as given or should someone maybe even me write a kind of alternate version of use case or what would we expect to do it in this case?

Chuck Gomes: So Shane Kerr keep in mind that our goal is not to develop use cases. This is just a tool to generate discussions so that we understand the breadth of the issues including competing issues. And…

Shane Kerr: Right.

Chuck Gomes: …the things you're talking about are all valid considerations for our work in the future. But one of…

Shane Kerr: Okay.

Chuck Gomes: …the thing we're not expecting will come out of this is some finalized use cases. So again our goal now is discussion which is happening. And even what you just shared gives some perspectives as about future ways to implement whatever policies we may develop in phase two.

Shane Kerr: Okay.

Chuck Gomes: Does that make sense?

Shane Kerr: That makes sense. And I think you've been very consistent about reminding me that…

Chuck Gomes: That's okay.

Shane Kerr: …we're not here to make use cases. No, no, no I think it's good. I think it's good. I appreciate that. So I think that pretty much covers it then. Great, thanks.

Chuck Gomes: Thanks for your understanding on that. And we're going to get to those issues you're bringing up. We have to and we have to cover conflicting points of view and conflicting suggestions and implementation methods and then hopefully reach some sort of agreement in terms of what kind of recommendations to make. So we will get there. Next up is (Vivek).

(Man): Hey good evening (unintelligible). I would like to - even it's quarter to 11:00 in the night here. I'm still driving. Pardon me for the background noise now. Jumping straight to the point here now Chuck thanks for the opportunity I think the idea here is to bring the attention back to the use cases, the discussions and the use cases arising again and again pointing to a definitive direction saying (unintelligible) all of us to understand that are we looking at validated Whois information so it could be utilized by different agencies be it the NEA, be it the banking organization, be it a credit authority, be it semantic. I think we've come back and I'm going to touch on (Susan)'s case with Facebook on the domain.

If for example if the Whois information is validated registrar registry then – if that's - and (Greg) is still on the call I hope. I'm still on the mobile side I know.

But it cuts down the entire investigation cycle. It creates a platform for anyone with (unintelligible) and (unintelligible) around ideas in his mind or our mind to at least creating a (unintelligible) that hey my Whois information is available. Now whether it's available on a controlled basis that's a different case to address the privacy issues. But then one thing's for sure that it's got to be validated. So how are we going to validate the Whois which was from and in my opinion the basis of the next generation Whois ideas across the platform? Yes that's me.

Chuck Gomes: Thank you. And again let me emphasize that (unintelligible)…

Man: Chuck we can barely hear you.

Chuck Gomes: Okay I'm not sure what's going on. Would everybody please mute their phones (unintelligible)? I – I can't (unintelligible). I'm hearing some noise? Can you hear me now? Okay that - can you hear me?

Man: Yes.

Chuck Gomes: Okay thank you. I appreciate the response. Okay so first of all understand that we have not yet decided that a new next-generation registration data services system is needed okay? That comes after we start looking at that after we deliberate on the first five questions. So we're not even - we haven't even decided that yet.

If we do decide that one is needed okay then and some already - believe that it is. I respect that. I'm probably one of those but that's irrelevant right now. And if we do do that then we're going to have to after we developed the requirements for such a system we're going to have to develop policy. And the third phase of our work is where we get into implementation. So if we end up recommending gated access for example then we're going to have to figure out and come up with recommendations as to how those who would be granted access are validated. That is a fact but we're long ways from that point right now and there – there's some very fundamental things that we have (unintelligible) to decide before we (unintelligible).

(Man): This is (untelligible) for the record. I think I agree but I would like to add to your point here that we also need to keep in mind that we're fast-moving to IPv6 technology accessing the Internet where every device that gets attached to it gets authenticated automatically so we do have a record for that system. So when we move on to IPv6 a lot of authentication issues will - are possibly maybe in the process of getting addressed.

Also every time we understand that there is a need for a process validation we need to understand as a group in terms of our recommendations that we need to be a little bit of futuristic because I don't think in the next ten years we're going to come back in this course again the entire futuristic RDS Whois, you know, about the NexGen because, you know, after 1990s we've come back here so it's almost at about 20 years that we're trying to discuss the Whois. So yes that's me.

Chuck Gomes: Thank you. And I really do hope that there are technical solutions like IPv6 that make our task earlier in the future if we end up for example recommending gated access. So thanks for that information. And hopefully the technology world will make our lives easier as a working group as we move forward.

Anyone else want to discuss this use case before we move to another one? And again I'm not ignoring the discussion in the chat. Hopefully everybody is watching that. Maxim please, your turn.

Maxim Alzoba: Thank you. Maxim Alzoba for the record. I think we should add different jurisdictions to the implications of this case because these same (legiscript) they have power to ask for things and even to ask for just traditional domains in some jurisdiction and totally have no power for even for investigation in others. It's for the other working case with them. Thanks.

Chuck Gomes: Thank you Maxim. And again I suspect that just about every use case jurisdictions are going to come into play when we get to actually especially implementing any policy recommendations that we make. They will be a critical issue and how they're handled will vary by jurisdictions. So anyone else want to jump in on this use case? Okay then let me find out (Aiden) are you able to talk now?

Ayden Ferdeline: I hope so. This is Ayden Ferdeline for the record. My apologies for the background noise. But the use case I want to present was where an entity say a distinct group launches a Web site with the intention of bringing important news and information to the public so registered the domain name in a foreign nation they don't want law enforcement or another third-party to be able to identify who's administering the Web site. And they don't want that personal data hidden because they are operating maliciously but because this information must be made known. They're publishing to be silent, their sources they contribute (unintelligible) to harm. And I won't give a hyperbole here. I don't want to say that the Whois protocol as it stands at the moment is personally trying to institutionalize the view.

But at the same time I wanted to say that this is not a purely hypothetical scenario because some registrants are facing real harm as we involve that personal identifiable information being retrievable by anyone for any reason. So even if you were to have an RDS which had gated access in respect to due process that's not necessarily a solution here because what constitutes a crime in one jurisdiction is not necessarily a crime in another. A (unintelligible) persecution in Saudi Arabia might and pass legal muster in another country. So this is why I suggest in this use case that no personally identifiable data elements should be collected in the RDS whatsoever.

Just to sort of some of in one sentence this misuse case is around how we can protect vulnerable voices with high institutional affiliations use domain names to communicate important information, how can we present them and protect them from being silent unnecessarily? And I'll leave that there. If there any questions I will do my best to address them. Thanks.

Chuck Gomes: Thank you (Aiden). And I appreciate you staying on mute until people ask you questions or you need to jump back in but let me open it up now. Now Maxim is that an old hand?

Maxim Alzoba: It was an old hand. Sorry.

Chuck Gomes: Okay thanks. Okay Andrew you're first.

Andrew Sullivan: Thank you. It's Andrew Sullivan here. And I think I have forgotten several times to say my name so apologies to ever has to cope with the transcript. So this is an interesting use case because it says no personally identifiable information should be stored in the RDS whatsoever. And there are a couple of difficulties with this.

The first one is I'm trying to understand what we mean by quote the RDS because that's been historically one of the problems here. And a few weeks ago I sent a fairly long message with a bunch of diagrams to the list to talk about this because the point there was exactly that the RDS just is the registration database. That's what the database behind the registration data services is in any - I mean it might not be the selfsame identical interest of the database. But if you're actually implementing this and you're, you know, like a person who's building the programming around this you're just going to use the same data store behind it.

So the data is there and it has to be collected. At least some of it has to be collected because we need it for registration right? I - we actually need the registration data in order to get people's money. So there's some tiny piece of RDS, the RDS that's going to have the data in it. And then the question is only how much and who has it and, you know, what are their obligations and so on?

The second thing is that there are some pieces of the RDS that there is a controversy over whether it's personally identifiable information. And the obvious example of this is IP addresses which some people seem to think are PII. I think that's wrong but there are apparently jurisdictions that believe that.

And since the IP address is sort of like the (Cin Qua Non) of even having an RDS at all, you know, of the host object - it seems that if you don't have that you don't actually need an RDS. We could just like if this use case followed all the way through to its logical conclusion we could say well we're not having an RDS. I'm trying to understand like what the utility is of the RDS if there - if literally this sentence no personally identifiable information should be stored in the RDS whatsoever. Thanks.

Chuck Gomes: Thanks…

Ayden Ferdeline: Hi Andrew.

Chuck Gomes: Go ahead.

Ayden Ferdeline: Sorry Chuck. This is (Aiden). Just to answer your question Andrew. I think it's important to separate the two concepts that you drew out there. So I think that there is registrar registrant contact information. And this is the billing information which should be stored by the registrar however they choose. That in the RDS itself I think they should only be storing the technical information that is required for a Web site to propagate into load so the domain name, the expiration date is status, the registrar and optionally the name service and the off code.

Chuck Gomes: Thank you for applying (Aiden). Before I jump in I have a couple thoughts but let me go to Stephanie first.

Stephanie Perrin: Thanks, Stephanie Perrin for the record. I think that this issue of exactly what are we talking about as an RDS is a really important one. My take on this in reading this case and the argument that (Aiden) making is similar to what we made or I made in the EWG that Whois traditionally we think of the publicly searchable or 43 – I'm not a technical person but wherever that data is housed it is available in a public registry. We are now talking about a more complex potential system where some data elements are held by the registrar, some data elements are still publicly available in a tiered model. And I think that we need to kind of take apart who's controlling the data. In data protection law in Europe they make a very useful distinction between a data controller and a data processor. And you've all seen that in the documents. ICANN is the data controller by setting the rules in the RAA and in policy for what data is collected, used and disclosed.

The processors would be the folks that have functional control over those data elements. So traditionally this in their registrars and their registries there may be new actors. But I think it's really important that we draw a line between what is publicly available in some kind of public system as the RDS and what is still collected for the purposes of the registrars running a business.

And then that leads us to the distinction between the EWG concept of folks having a secured protected credential where even the registrar in order to avoid a takedown shakedown from a hostile government for instance or a hostile religious group in countries where that would be the case so that the registrar cannot be shaken down to disclose the identity of the individuals at risk. I hope I'm being clear here but I think that very often when we talk when we use the expression RDS we're - we should be talking about higher ecosystem. And if we need the publicly available registry we'll call it that for lack of a better word, the replacement for Whois then we should be clear about that. Thanks.

Chuck Gomes: Thank you Stephanie. Greg Aaron you're up.

Greg Aaron: Thank you Chuck. Can you hear me?

Chuck Gomes: Yes.

Greg Aaron: Okay this is Greg Aaron. Thank you Chuck. A comment on (Aiden)'s case which was a party wishing to publish information that might invite investigational reprisal say from a government. (Aiden) asked the question - he asked a question or posed a problem which is how can such entities protect them - their identities while publishing that information using a domain name? And then his solution was don't have any information about the parties in the RDS, not have it and to not publish it.

What I'd like to point out and as I pointed out on the mailing list is that that is one solution to the stated problem but there are others as well. And so this is a use case where there are multiple solutions. Some of the solutions I mentioned include there can be use of proxy services and privacy services which may provide both anonymity and protection from parties who were trying to obtain the registrant's identity. This is also an example of if there are multiple solutions we can and should consider those balanced against various other factors. So my point is if we state problems we can then state various solutions to them and sometimes. Thanks.

Chuck Gomes: Sorry. It took me a while to get off mute on my iPhone. So thanks Greg and appreciate that. And this is the kind of discussion that these use cases are supposed to generate and hopefully giving all of us a view of the challenges that are in front of us but challenges that have alternative solutions like Greg just pointed out. So appreciate that. Anyone - okay we have another hand up. (Aiden) go ahead please.

Ayden Ferdeline: Thanks Chuck. This is Ayden Ferdeline for the record. I just wanted to respond to Greg's comment briefly. Thanks for your comment Greg. So I do want to push back a bit on your remark that privacy proxy services provide anonymity and protection. They might but they might not.

These services are often they're promises or assurance of due process. A privacy proxy service provider is not a court. There is no entitlement here to the registrants to a fair and public hearing within a reasonable time by an independent impartial confident tribunal as to wherever the data should be released or not. So yes maybe there are solutions but I don't think they're necessary one that all (unintelligible) groups will be able to rely upon. So I just wanted to put that comment back there.

Chuck Gomes: Thank you (Aiden). And before I go to Lisa and back to Greg keep and mind that there may be alternative solutions that fit different scenarios. Privacy proxy may work in some situations, maybe not in others but those are the kind of things that we're going to have to delve into in quite a lot of detail in the future. Greg did you want to respond directly to that or I see your hands down now. If you do go ahead.

Greg Aaron: Yes thanks Chuck. I mean that's an interesting statement from (Aiden). His expectation sounds like there would be some sort of a legal review which is what due process usually entails, a legal review through some sort of a court or legal entity. And again we would have to talk about at some point whether that actually happens or could happen. You know, most of the relationships on the Internet are not going through legal processes. They're governed by contracts. And services are provided by service providers who may have their own internal processes for making decisions. So again we have to examine some of the assumptions stated. Thank you.

Chuck Gomes: Thank you Greg. Let's go to Lisa.

Lisa Phifer: Thanks Chuck this is Lisa Phifer for the record. I just wanted to follow-up on some questions I put in chat. I'd like some clarification on what is the protected party in this particular misuse case? I see references to the registrant. I see references to the administrative contact and I also heard someone refer to the registrar as someone that needed to be protected. So I think it would be really helpful to tease out exactly who's data is at risk here and maybe even a little bit more about which data elements are commonly used in this kind of misuse. Thank you.

Chuck Gomes: Thanks Lisa. It sounds like there's a couple questions or statements that (Aiden) would like to respond to. (Aiden) you're up.

Ayden Ferdeline: Thank you Chuck this is Ayden Ferdeline for the record. I'll just address Greg's comment first. Yes actually that is what I would recently expect because if a privacy proxy service is simply giving data to whoever requested that's problematic. I think that there should be a legal review.

And to Lisa's question when I envision the scenario I think that the data of the registrant, the technical contact and the billing contact is (unintelligible). And so this is the information that these are the data elements that should not be collected in general. The only I guess identifiable data elements that we should be collecting is that of the registrar. And if they choose to maintain contact information for their customers behind - in whatever system they choose then that is their prerogative. Thank you.

Chuck Gomes: Thanks (Aiden). We're going to have to wrap this up so let's go to Alan and then Andrew.

Alan Greenberg: Thank you. Alan Greenberg speaking, just a couple of brief comments. (Aiden) implied before that privacy proxy services may or may not be sufficiently private. I think we have to understand that there is nothing that is going to be sufficiently private in some cases. Between coercion force of law and money you can find out almost anything if you really have enough desire.

You can keep it private who registered the domain name but your domain name is probably there so people can find your Web site which means there's an IP address that's traceable and somebody is running a machine. And again between the various ways you can get information out chances are if someone really wants to find out then putting something on a Web server is probably, you know, something that's going to be vulnerable and you have to accept that or not use that mechanism. Thank you.

Chuck Gomes: Thanks Alan good points. Andrew?

Andrew Sullivan: Thank you. It's Andrew Sullivan here. So I think I agree with Alan but I want to just because of the use case I want to once again come back to this question about, you know, the - how you don't collect the data by, you know, only the registrar having the (unintelligible). The point that I've tried to make a couple of times now is that the registrar databases are part of the backing store of the RDS. That's part of what the database behind all of this is.

And it's incoherent to claim that the registrar is not going to have the contact, the billing contact for the registration because of course that's the – that's how - that's what their business is. So there is no way they're not going to have that data.

So there really is only a question here of what data elements are going to expose to queries, not whether the data is going to be collected somewhere and be queriable because it's got to be queriable by the registrar because that's how they're going to get paid for the renewal.

So I just I really I think that we need to be very careful when we say things like this because I think it's confusing us about what the underlying system that we're interfaced to actually is. It's the totality of registration data that we're talking about. Thanks.

Chuck Gomes: Thanks Andrew. And I'm going to have to wrap this up but I understand Greg Noakes can't raise his hand so I'm going to call on him and then very briefly on Maxim and then we need to wrap this up so Greg you're up.

Geoff Noakes: Chuck this is Geoff Noakes with Symantec. My raised hand was raised earlier.

Chuck Gomes: Oh I said Greg. I'm sorry Geoff. Okay go ahead Geoff.

Geoff Noakes: My raised hand was answered earlier.

Chuck Gomes: Oh okay. Thank you. Very good and less - and Maxim did you have a quick remark? Go ahead but please be brief.

Maxim Alzoba: (Unintelligible) yes briefly in this particular use case we definitely should add legislation like jurisdictions as an issue because it's highly dependable on who is complaining on which dissident group. Thanks.

Chuck Gomes: Understand, thank you. All right and just in the last couple minutes here I want to – and Lisa you may need to help me on this but we will continue discussing use cases next week in our meeting okay. And our meeting will be at the same time next week on next Tuesday. The - I'd like all of you to think about are there any gaps in use cases keeping in mind that we're not trying to create this comprehensive list of use cases. That is not our goal.

But if there are any areas where you think it's a gap that we should fill and get a use case for I'd like to ask you to identify those gaps in the next few days this week so that we can attempt to get those filled. And anybody that's volunteered a use case if you can please get those done this week. We don't want to leave out any big gaps at this – understanding though that we don't have to have a use case for every variation in detail. That's not our goal. Our goal is to help us understand the requirements for our deliberations that are upcoming. So I'd like to ask everyone to do that.

So that'll be an action item for the whole group, see if there are any big holes. Again don't get down in the nitty gritty detail. There's every one of these use cases we could find other variations that have been covered. We don't need to go through all of those but if there are any significant gaps that need to be filled please communicate that on the list and we will do that. Lisa please jump in.

Lisa Phifer: Thanks Chuck sorry for the delay coming off mute. This is Lisa Phifer again for the record. I'd just like to suggest for those of you that are willing to try to do a gap assessment if you visit the wiki page where we have the example use cases there is a link there to the annex from the EWG report that was distributed about two weeks ago. So you can also find it in the media materials about two weeks ago. And it lists the examples that the EWG came up with.

Now I think this group has developed some additional examples that are very interesting as well. But if we're looking for gaps you might want to take a quick look at those use cases and think about whether they are things that you do in your everyday life with domain names because some of them are sort of the more, you know, typical everyday activities such as use cases associated with buying and selling business domain names. So I'll just give that is one example but there are several others there.

If you find something on that list that you think might be of interest to you and you want a copy of the EW use case just ask, be happy to send it to you. We've been hesitant to send you all 50 some use cases without introduction but anything on that list that you think is helpful to you to help fill a gap that material is available to you.

Chuck Gomes: Thank you Lisa and our time is up. Thanks for the great discussion. We've got - this is really highlighting a lot of the work that we've got to do in the future. We will continue this process next week. And just asking staff is there anything else that we need to cover before I adjourn the meeting? Okay well thanks everybody. Have a good rest of the week, meeting adjourned.

Michelle : Thank you Chuck. Again today's meeting has been adjourned. Operator, please stop the recording and disconnect all remaining lines. Have a great day everyone.

END