Transcription ICANN61 San Juan
GNSO: RDS PDP Working Group Meeting Part 2
Wednesday, 14 March 2018 at 17:00 AST

Note: 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.

The transcriptions of the calls are posted on the GNSO Master Calendar
page http://gnso.icann.org/en/group-activities/calendar

Chuck Gomes: Okay, thanks for coming back. I know I needed that break. I bet the rest of you did too. This is Chuck, and we're going to resume our RDS PDP working group now. And I'm going to turn it over to Marc to go the responses from Drafting Team 7. And I'll just let Marc take it from there. And again, we'll do the same thing. We'll let other drafting team members respond and then anybody in the room can respond. Go ahead Marc.

Marc Anderson: This is Marc Anderson representing Drafting Team 7, criminal activity (unintelligible) abuse mitigation. But I also note there's really a third item in there and that's reputation services. So those are really three main use cases that we looked at. I also need to caveat that. The members of this particular drafting team were particularly busy and weren't able to contribute as much as they would have liked. And so this is maybe not as fleshed out as it could have been. Fortunately, we have Rod Rasmussen here who will be able to contribute and help answer any questions.

But let's get right into it. Looking at criminal activity and DNS abuse mitigation, it's, you know, I just want to remind everybody. We talked about this when we presented at ICANN 60, but on this particular proposed purpose, it's important to remember that these take one of two different paths that aren't necessarily clear at the start. It's when you're looking at criminal investigation and DNS abuse, are you using the RDS information to investigate a criminal or to look up and contact a victim?

And so where, sort of, these use cases go depends up on what you're doing. Are you investigating criminal activity or abuse? Or looking at somebody who's a victim of criminal activity and DNS abuse? And so depending on which it is, you're going to take a different path which isn't always clear at the beginning.

Can you scroll down a little bit? Thank you. So looking at the first one, WHOIS associated with the domain name registration needs to be identified and/or contacted investigating criminal activity and DNS abuse. Looking at this one, again keeping in mind, you know, are you looking at a criminal or are you looking for a victim? You know, this is, you know, it's still not necessarily, you know, at this point you haven't necessarily diverged but you need to identify, you know, the person responsible for the domain name registration. And so, that's really the WHOIS the, you know sort of, the entity responsible for controlling the domain name registration. That, sort of, of particular important choice of words there, WHOIS controlling the domain name registration. Avoiding things like domain name owner there.

The objectives achieved, I'm just going to read this off. You know, prevention of criminal activity and DNS abuse, and mitigation of impacts from criminal activity and DNS abuse. This is, sort of, an acknowledgement that you can't always prevent all criminal activity. Sometimes your goal is simply to mitigate the impacts of this. And when it does occur, you want to use this data to help build a case for the prosecution of those responsible for the criminal activity.

Moving on. What might be expected? So in this one, there's sort of an interesting dynamic. You know, sort of the initial pass of this one would be that you - if you're investigating criminal activity and abuse, you would not want to contact the person responsible for that. And so, you know, that was maybe in the first draft of that. But then it was pointed out that well there may be cases where if there's a reseller or privacy proxy registration, there may be some contact that you would want to occur as you were trying to track down who was actually behind the domain registration.

You know, so while maybe you won't want to necessarily contact directly the entity controlling the domain registration, there may be some contact that needs to occur if there's a privacy proxy or registration. You may want to contact hat entity, the registrar or reseller to try and get more information about it. So when that is the case, you may be contacting those entities to try and get more information about WHOIS behind it. You know, trying to do investigation in to the entity ultimately behind the criminal investigation or the criminal activity or abuse that's occurring.

Can you scroll down to the next item? Okay so this one delves into the notification and so what we're talking about here, you know, previous one was around, you know, if there's a criminal activity or abuse occurring. Again, you're going for the perpetrator. Here, looking at notification, if you've identified a victim, you know, this is a, you know, this is the victim notification use case. And so, essentially the same answer who associated with the registration needs to be identified or contacted. You're looking for the controller or owner of the domain name registration. You want to contact the entity to notify them that abuse has occurred.

Next one. What is the objective? You know, here starting off to say the victim may not be even aware that there's an issue occurring. And I think some of the use cases we talked about where malware or maybe - may have been maliciously installed on a website, on that's hosted on that domain

name. You know, or, you know, or other activity that the owner of the domain name owner is not aware of. And so the objective here is notification in forming the domain name owner that some form of DNS abuse or criminal activity is occurring that's associated with that domain name registration.

And what might be expected, you know, obviously we're trying to, you know, in this particular use case, you're trying to rectify the situation. So what's expected in, you know, after you notify the person that they take whatever preventive or corrective action are necessary to resolve the criminal activity or abuse.

And the last one, I mentioned reputation. So, sort of, the third use case under criminal investigation DNS abuse is reputation services. And so the who associated with the domain name registration needs to be identified, contacted. You know, this isn't a contact use case, but an identification. The reputation services looking to identify WHOIS the domain name - WHOIS controlling the domain name registration to help provide a reputation score. And so here information about the registrant who created the domain name registration helps feed that reputation score. So identifying the person behind the registration is important there.

The objective essentially, I covered that already. But, you know, data about the domain name registration helps drive a reputation score. And so here the data, you know, what's - the objective is determining information about the controlling entity for that purpose, not necessarily for contacting these entities.

Under the third one what might be expected. Again, the, you know, the person using that data might not - or is unlikely to be contacting anybody here. But it was important to note that in our discussions, you know, if you're creating a domain name registration and you want to ensure a high score, you might - you would be motivated to provide more information and provide more accurate information. And so while there isn't a contact use case here

per se, what might be expected of that entity is that someone looking for a better reputation score is going to be motivated to provide more information and keep that information accurate and up to date in the WHOIS record.

So I think that covers the three use cases that we have for criminal investigation. Keeping in mind at the top that you don't necessarily know at the beginning if you're looking for a criminal or a victim using this data. So there's a little bit of a gray area at the beginning. But that covers the two main use cases. I like to look over to Rod Rasmussen and see if there's anything he would like to add to that.

Rod Rasmussen: Thank you. I'm sorry. I diverted attention because, yet another fire is burning. I've been - my attention's been diverted on. I did look through this document and reviewed it. It was, as I said, close enough to ship as we said back in the days when we had to get the alpha out the door. So good job in putting that together and my apologies for not being able to help put that - put that out. I'm here to help clarify any questions have on that.

Chuck Gomes: This is Chuck. Does any want - have any - anybody else from the - before we open it up, anybody else from the drafting team wants to add anything to what Marc shared before we open it up to general questions and comments and like that? Not seeing anyone, let's go. Let's open up wide.

Alan Woods (Alan Woods) for the record. This is actually a general general comment about this. This came up with I was presenting the last day which had a day. I don't know which day it was unfortunately. Question 3 and I know we went through and tried to figure out the questions. I know the answer to Question 3 make me scratch my head in bemusement and wonder just purely because I don't think we, you know, in part and parcel of this. I think it's quite confusing to ask the question what do we expect of this contact. Who are we to say what we expect of the contact at all? And I think Beth Bacon you mentioned this in the last one as well that even there, I'm kind of, I'm asking the question

of if he or she is motivated to obtain a higher reputation score, in every bad television program with a lawyer you would say, calls for speculation.

You know, I just don't see what it adds to the process. And every time I'm at the same point and I'm going what? So, you know, obviously we still have (unintelligible) there but I just I don't see the value in what we expect of that. We're just - the legitimate purpose does not necessarily mean the expectation of what that is. So I would just say that.

Chuck Gomes: There has to be value because Lisa Phifer came up with these questions. Sorry Lisa Phifer. Marika Konings go ahead.

Marika Konings: So this is Marika Konings. I'm just relaying some input that Greg Aaron provided on the mailing list as he'd not here with us. So he noted the questions and responses focus on context and notification. Who needs to be contacted and when. And under documented the value and use of identifying the domain name contacts. And the use of non-contact data. In the case of DNS abuse mitigation and reputational scoring, there are many legitimate reasons for processing RDS data elements that have nothing to do with contacting registrants and their designated contacts. In these and some use cases, contact outreach is irrelevant or undesirable.

For example on Page 1, Question 2, is missing a critical element. Please add to Page 1, Question 2, an objective achieved by identifying domain name contacts - contact and assessing noncontact domain data is to assign reputation which in brackets risk to domains. This can involve identifying trends and patterns, correlation with other data such as name servers and finding association with known bad actors.

Chuck Gomes: Lisa Phifer do you want to defend yourself after I blamed everything on you?

Lisa Phifer: Sure. And actually it's a good point Alan because I think different drafting teams looked at that third question in different ways. So the question, I think,

originally came from is there an obligation on the party WHOIS being contacted to respond? Which is a rather a different question that what was answered for reputation here. Which is, is there a benefit for that party to do something? And both are interesting questions in that they might help us understand the nature of the communication. You know, is this (unintelligible) contact that doesn't necessarily imply a response? Or is it a contact that normally would obligate the party to respond? The question about (unintelligible) goes directly to, you know, what's the benefit to the data subject and providing their data?

Alan Woods Just - I completely agree. And I know you're trying to get the extra dot on it and I really appreciate that. What I would only say that is when, and again I'm probably jumping ahead. So apologies. But if we are deciding what legitimate purposes - the legitimate purpose is devoid of the ultimate benefit to the data subject. There is a legitimate purpose or not. And whether or not that helps the data subject is actually irrelevant because we're asking to access data devoid of purpose freely or devoid of benefit.

So I still have a slight issue with it. But again, I appreciate that you wanted to ask the question.

Chuck Gomes: Kathy:

Kathy Kleiman: Kathy Kleiman, and I practice criminal activity on a regular basis. I put up pro-democracy websites. That's a violation of criminal law in China. So Marc, let me ask you a question and then I'll add some more about jurisdiction. I have to hand it to (Griffin). There was lots of qualification in there. Thing about legal actions and jurisdiction and applicable law. Did you guys talk about jurisdiction applicable law? What is legal and protected speech in one area, so the registrant would be protected may be a complete violation in another country. I was just wondering if I'm missing that kind of nuance in this somewhere.

Marc Anderson: Easy answer, no. But I'll give Rod Rasmussen a chance to jump in.

Rod Rasmussen: Sure the - any - this is addressing the entirety of the problem space and actually what actually happens in looking at things like would it have been identified (unintelligible) etc. The - whether or not anything is in particular jurisdictional law issue or not really is outside of the scope of what we felt we were answering here. This is - these were very much focused on the actual way that things work dealing with these issues and where - whether or not this tool, these tools are appropriate or not becomes a policy issue. So but within a local jurisdiction obviously. And so depending on where requests and responses are being made and expected from, there may or may not be answers. Anyway, just diving into beyond the obvious what we've written down here.

Obviously, when you have things that are illegal in one jurisdiction and legal in another and those very wildly across the map, you're going to have to have other parts of your policy regime that manifests themselves to address the issues where you're core purposes are around dealing with things that are universally accepted. So, you know, that's a long-winded answer to say we didn't really address these issues because we thought it was outside of the remit of what we were being asked.

Chuck Gomes: And Kathy, this is Chuck. Doesn't mean we won't have to deal with those when we deliberate, okay?

Rod Rasmussen: They have to be addressed.

Kathy Kleiman: Where - this is Kathy again. So where does the embodiment of this discussion then go into the document so that it is preserved for the future? And again, so when we look at abuse of activities, denial of service (unintelligible), harassment. You use probably more like a criminal activity and phishing may be more like an abusing activity. But where do we preserve this? Because the criminal examples here are very self-selected.

And don't include the wide range of hate speech and other things completely protected in one jurisdiction. Completely illegal in another.

Rod Rasmussen; This is a nonexhaustive list, right? This is - the whole purpose of this work party is to put these things together. I would encourage people adding that stuff.

Chuck Gomes: Hold on. Let's let Lisa Phifer respond to your question.

Lisa Phifer: So backing up a little bit. Before we did this exercise, when the drafting teams were organized in advance of the previous ICANN meeting, each of the drafting teams, you know, were charted with coming up with a draft definition expanding on the one-line definition they started with for each of these purposes. And as Rod Rasmussen said, there wasn't really an expectation that would be exhaustive. But certainly we will add to and refine the language that the drafting team produced as part of deliberation on each of these individual purposes. We haven't gotten to these set of purposes in our deliberations yet, but we have done that in the case of technical issue resolution and main name management. We have actually stared with text from the drafting team. Modified it and expanded it. So that's where it would occur in our outputs whether we, at this moment, capture as a footnote in the drafting team's output to make sure we get to it when we actually deliberate on this purpose. I think that's a good idea.

Chuck Gomes: Maxim.

Maxim Alzoba: Maxim Alzoba. Two items, first when we are talking about purposes, most probably we are going to use it in some kind of consent, etc. And in legal text, when your read: "The purpose of collection, criminal activity and/or DNA abuse mitigation," could we finally change it to like criminal activity prevention or something, so it sounds better? Because if we identify it as a purpose and later it's included as this in document, it would look really not nice, is the first thing. And I think we need to start differentiating between ability to contact

and verify the identity of some person. Because they are different. Not necessarily police wants to contact criminal, but definitely they want to identify him or her. And it would allow us to avoid issues on later stages. Thanks.

Chuck Gomes: That's certainly a possibility when we get to deliberation. But Marc, go ahead.

Marc Anderson: Thanks Maxim. This is Marc. I'm not sure I followed the first - your first point. I think on the second point we tried to capture that. So if we didn't, I'd be happy for any feedback on how to address that. On the first one, is there a suggestion for an edit or something you would like to see changed on there?

Maxim Alzoba: Maxim Alzoba for the record. On the first suggestion, it's the to rename the purpose. So later it would feed documents better. Like not for - the purpose is not - because in legal documents sometimes you see this slash symbol as and/or depends on the. So basically if you copy paste this into the consent and say that it is a purpose, reading that the purpose is a criminal activity, doesn't look nice. Thanks.

Marc Anderson: Thank you. This is Marc. I got you, right. Yeah, if we can incorporate that. I think it's a good point. That's a point that was raised previously and we didn't incorporate that in this draft. Do point taken. Thank you.

Chuck Gomes: Yes, Greg.

Greg Shatan: Thanks. Greg Shatan for the record. I don't know if in the title of this DT the word mitigation was meant to apply to both criminal activity and DNS abuse. If it was, then the word's already there. But, you know, English tends to rely on for native speakers on words that aren't' said. They're, kind of, assumed. And if you're not a native speaker, they don't get assumed. I think this may be one of those cases where we have to say it twice even though, you know, a monolingual person, I see it as applying to both or at least arguably to both.

Also, I think we have to avoid talking about these things solely in the context of GDPR. When I hear something being said about, you know, no benefit to the data subject, originally this was about putting together a registration directory system and not about figuring out how to comply with GDPR. Obviously, we have to do that. And it's going to come up and again and again. But sometimes I feel like we never talk about the actual nutsy boltsy type of questions that is - that we would be in here. We might have to ask ourselves every once in a while, if data privacy laws didn't exist, what would we be talking about? Because clearly that goes to - there are a lot of things that have to be engineered in here because of those laws. But that can't be the only thing that we're dealing with. We might actually forget to do something because we're so fixated on compliance that we're not actually building what we're supposed to build. Thanks.

Chuck Gomes: Thanks, Greg.

Marc Anderson: Thanks, Greg. This is Marc. You know, on your first one, your first point, I agree. And like I said that's come up previously. I think we have suggested language for how to address that. So apologies for not including that in this draft. On the second one, I'm not sure. Was that a general statement or is that feedback specific to this use case.

Greg Shatan: It was more specific to the comments I was hearing, but it is also more general. I don't think the use case itself. I think the use case itself actually did a really good job of focusing on the use case person and not on the privacy case about the use case. But the discussion always seems to come back to what's the privacy implications of this use case? And not anything about the actual use case and how it might be engineered for any other reason. Thanks.

Chuck Gomes: Thank you, Greg. Yes, Farzaneh.

Farzaneh Badii: Farzaneh Badii speaking. So in the legal action group, I also raised this point that criminal activity in some jurisdiction could be that you write something about some profit and it can be classified as blasphemous. And there is a death punishment in some countries for that. And we did - we included that in a background note just to remind us that it's not criminal activities, not always that when you say criminal activities. It's very subjective and it differs from jurisdiction to jurisdiction. And it will have human rights implications. So it is not the - we are not only getting child abuse materials down or stopping harassment, we also put a policy called activists and human rights activists in certain countries into danger and that could be criminal activity in their mind, these political activities that in the democratic country is not criminalized.

So we have to always remind ourselves of that. And I'm glad that we have that in our documents in legal action. But I don't know how we can put a background about this here. But in the legal action document, I think the first one, we had this as a background and we need to also add it here.

Chuck Gomes: Thank you. I know we've got dovetails. I mean I think that's complementary to what Kathy said and, you know, just expand on that a little bit. That really wasn't an aspect of criminal activity or abuse mitigation that we considered. We - I think as Kathy pointed out, when you identified, sort of, the specific types of criminal activity and abuse that wasn't one we mentioned. So I think this is great feedback. That's just not something we contemplated in our deliberations. So great feedback, thank you.

Farzaneh Badii: Just to follow up. Farzaneh Badii speaking. It is certainly - if you - if we can, well I am dreaming that one day we can say limited to technical. And not all the criminal activities around. You know, someone was saying they wanted to stop human trafficking by using WHOIS. Well let's not do that. There are other ways to do that, you know. It has to be limited. Let me just clarify. Not in this group, the other day it was.

Chuck Gomes: Go ahead. Thanks Farzaneh. Go ahead Rod Rasmussen.

Rod Rasmussen: Okay. I had a conversation with you the other day about this horrible term DNS abuse which I loathe because it's imprecise and an artificial construct that we've managed to fall into in ICANN. That's my personal opinion. That is not an (ASEC) position yet. So this all gets down to what is the appropriate tool and the appropriate place to look at dealing with the problem you have? And it just - when I say problem it can be somebody's problem that everybody agrees is a problem, a vast majority of people agree is a problem or a very small minority of people agree is a problem. All right? And so when we start looking at these things, we're talking about the tools and the methods that people use to deal with them.

In some cases of pick your very worst crime that we all agree with like child abuse things, right? Because everybody loves to go - hates that, right? That's my point. Is this the right tool to use in order to help with a case of trying to do something? It becomes pretty obvious if somebody's registered a domain about, you know, directly like I have 17-year-old girls for sale or something like that, right, dot whatever. You know, I'm not saying people do that. They're not usually that dumb, but sometimes they are actually. So in that case, you might want to find out everything you possibly can about that particular thing.

In other cases, somebody's put something on their Facebook page. And the WHOIS or some - let's not even say Facebook. Some website somewhere that somebody may have hacked into or they offer a free service for people to be able to come and post things. And some person doing this kind of activity has decided to add content to that place is using the WHOIS information appropriate in that place. Probably not unless, of course, there's no other information you have about how to get ahold of somebody so you can ask them can you give me information about that? In most cases, you don't need that. In some cases you do because it's just not - they don't put information on their website or what have you. And it's a useful tool. If you take that - if

you changed the accessibility to the information there, you make that tool less useful in that use case.

So these are the things we need to consider as we're going through here as we're talking about the point in time when a tool is the appropriate thing to use to get information to help in a particular situation. Now take that child abuse thing which we all agree is really bad and replace that with any other thing that's a crime somewhere whether that's, you know, speaking badly about the kind in Thailand. That's a, you know, a lot of - most people who got there don't even know that. And they could get in trouble for it, things like that. So around the world people - a lot of people don't agree with that. We'll put it that way, right? Is that something that if you were to register a domain in Thailand as a Thai person and publish in Thailand, well then you might have the ability to go do something? Again, it is the appropriate tool to use data around that?

Then you get into the jurisdictional issue stuff, right? Whether that - whether you can use the tool, right? Whether you have the ability and the right to use that tool. That's a stated purpose for accessing data for example. So if we can start thinking about this stuff more in the realm of is it the appropriate place to get information that may be used to either completely deal with an issue where there's a domain name registered for this purpose and this purpose only which clearly there's - that's a good - that's where the appropriate tool versus it's information. It helps me with either doing things of identification. It helps with mitigation. I let someone in whose domain has been affected by an outside party. Now they've got a problem. Is it looking for things to allow me to protect my networks? Is there a pattern of registration that are - that I can use this data from in order to solve this - help solve like spam problems, things like that? Can I do that on a systemic basis?

Those are all things that come into, it's the proper tool. It provides information that's actually valuable for accomplishing that purpose. So thus, that's why we put these things into here. And then it becomes a matter of who actually

gets access. We can separate the process and the tools from the who gets to use them argument, then I think that makes this a lot clearer. And I'm sorry for going on so long. But I'm just - I'm being distracted. So I figured I'd dump it all at once.

Chuck Gomes: Holly Raiche.

Holly Raiche: I guess my question goes back a bit further. But Rod Rasmussen thank you for, kind of, articulating the difficulty that we all have. I'll add a level of difficulty because it's a difficulty that I think. And that is if you look at basic privacy principles, you only collect the data you need. And you collect that data for a purpose because the consent is given. And now what we're doing is saying the data is there. Now is it okay to use it for whatever bloody purpose you like? And that's difficult. However, an analogy that I think works and makes me feel a little bit better and that is I know that if I provide certain information, it's pretty clear to me that the cops are going to come along and get it for their purposes and I think most of us have that expectation. But is that good enough in the case of a tourist walking into Thailand? Or somebody saying something - some - a person in China saying something really stupid like the guy really should have terms limited. Which is going to be pretty fatal.

So, you know, I mean expectations go a certain way for law enforcement, but how far? And I actually don't have answers. I just put a question on top of your question. Thanks.

Chuck Gomes: Go ahead David Cake:.

David Cake: Yeah, I think thought it's - I mean they're - the questions about appropriateness and things there are some that we answer within the question of purpose and privacy law and all of the stuff that we are discussion. There's other questions that we don't need to answer. It's really up to the, you know, the agency decided this tool is useful and appropriate. And they, you know, and they deal with that internally. There are other ones

that somewhere in the system we do have to deal with because, you know, have a solution because literally what is legal in one jurisdiction isn't legal in another. You - if you, you know, prosecution for blasphemy is the lore of the land in Saudi Aribia. It's a violation of the First Amendment in the US, and so on. So that we - we don't need to necessarily find what that solution is or provide that. You know, government literally has to provide that - agree on what that solution is. But we need to make sure that there is a mechanism by which they can enforce it.

And so there are whole different - this is not a simple question. It will never be a simple question of yes or not. There's always going to be multiple mechanisms and at least three different ways that we need to make that decision.

Chuck Gomes: That's David Cake:. Greg.

Greg Shatan: Thanks. Greg Shatan for the record. First to just clarify one thing that David Cake: said. Blasphemy is not criminalized in the United States. Making laws against blasphemy is unconstitutional.

David Cake: Exactly. Prosecuting people -

Greg Shatan: So just wanted to make sure, yeah. It hasn't gotten that bad yet. Anyway, the point - a lot of this can, kind of, be boiled down to this question more or less. What do we do when law enforcement is bad and criminal activity is good? That's, kind of, the question. That's a - the question is whether and how we make that judgement and when and why? And what happens when we get this to the GAC? All sorts of things there. And which part of the GAC? They may not agree with each other.

So it's kind of - that's what I see. It's actually a very simple question. I didn't -I tried to phrase it in as neutral a way as possible. I had a number of other ones that were, you know, pejorative or the opposite of that. But it's really,

what do we do when criminal activity is good? At least in the eye of some beholder. Especially when you have countries that are to us look extreme, at least me in - as a, you know, blue state, you know, progressive whatever. But if we had, you know, high government sitting in here. They'd say, of course. Of course it is. It's like, you know, inimical to our society that we do this.

So it gets to be a little hard to make value judgements about law enforcement. And I know, you know, off the pigs was something I probably said in 1968. It's gotten a little more complex that that since then. Thanks.

Chuck Gomes: That's, Greg. Now try to be a brief as possible so we can get to a few more people while we're on this one. Let's go to Rod Rasmussen and then we'll go to Michele Neylon.

Rod Rasmussen: Got two thoughts. One is if we can get back to, kind of, the original things there. One of the things is if you take a look at purposes for being able to do things like protect your network, because we're an internet - interconnected network system, right? So being able to reach out to people to deal with abuse that's coming across the wire is really important. And I would argue is fundamental to being able to provide the system, right?

Also being able to notify people that their domain name has been compromised in some way is fairly fundamental to the system. It may not be as direct as it's attacking other parts of the system. But it is part of the domain itself.

Woman: (Unintelligible).

Rod Rasmussen: Right, yeah. Exactly. So and that's what a lot of this stuff is. And when you take a look at things like reputation management that - or reputation services that actually is looking at protecting the system from being abused so much that you can't use it, right? So, kind of, fits into that purpose. That I would say

that this whole question about access to data for cross purposes when it's law enforcement or even just you don't agree with it, right? That becomes a risk management question, right? As to when and then has to be dealt with there. And if you decide risk is really high, you need to set high bars. If you decide the risk is really low, you set lower bars about what it is that you're trying to do. And this - most of this stuff comes from access. We keep talking about well this law says this and this law says that. Those are all access questions, right? If you're collecting it for law enforcement or network protection purposes that you agree on, then the other side of it becomes the access problem. I'll stop there.

Chuck Gomes: Thanks Rod Rasmussen. Michele Neylon.

Michele Neylon: 'Thanks. Michele Neylon for the record. I think we get into the weeds on some of this around, you know, what constitutes a crime and what doesn't. And I don't think it's particularly helpful to our cause. I mean ultimately, some of you will find this amusing. While one might think that Ireland is a first world country, we still actually have some rather amusing laws on the books. Whether the government actually bothers to enforce them or not is a totally different matter. So the entire blasphemy argument you just had amused me greatly. And probably amused Alan who's sitting to my right.

Generally speaking in the kind of day-to-day stuff that a lot of us the registrar and registry side deal with is, yes. We do get into requests for information coming from law enforcement. But it has to be complaint with the laws of our jurisdiction. So a lot of this kind of out there type of things aren't really that pertinent. And trying to fix the laws of the world in here is not going to help anybody. So I really would suggest that we don't go down that route. And if you're interested in jurisdictional stuff, Bertrand de la Chapelle and other people have been - are doing a lot of work around that. You may agree or disagree with them, but I don't think we're the people to fix this. And I wouldn't' recommend it.

Woman; (Unintelligible).

Michele Neylon: Microphone.

Chuck Gomes: Hold on. Let's do it. Let's do this orderly so everybody can hear. And keep it really brief because I'd like to wrap this one up and move onto the next one. Farzaneh, do you want to respond briefly and then we'll go to David Cake: and then I want to just make some final comments.

Farzaneh Badii: Farzaneh Badii speaking. We are also not here to rescue the world and prevent other criminal activity. This has to be limited to what ICANN does or the definition.

Chuck Gomes: David Cake:.

Michele Neylon: Sorry but hold on Farzaneh. That's entirely true because the data that gets collected is collected by contracted parties who have contracts between each other. The ICANN piece of that yeah, I agree. But I think there are going to be some areas of where it's like I will have data that ICANN doesn't need and that's fine, okay. I think she actually agrees with me for once. This is very strange.

Chuck Gomes: So okay, David Cake:.

David Cake: Yeah, I think that point of discussing that's relevant for us. We don't get to have any say in what is a crime or not and what is legal. That is quite rightfully the business of government. But if we make material that people that law enforcement agencies might want is no longer public. And then there has to be a process for them accessing it. And it has to take into account that there are laws that will decide that. But there needs to be a - all we need to really acknowledge there is a mechanism and, you know, it must be and think about what those mechanisms must allow. We don't need to decide what the mechanisms will be or how they will be used. There's a world of - it's kept

Bertrand very busy for a number of years. I'm sure it will continue to keep him and governments of the world very busy for a large number more. As long as we technically enable it.

Chuck Gomes: Holly Raiche real brief please.

Holly Raiche: Going back, Mr. (Rasmusan) got it perfectly. We have the excuse to collect the data. It is within ICANN's mission. It's about genuine abuse cases and that sort of information ties right in with ICANN's mission. We've done it.

Chuck Gomes: That's something we're going to have to deliberate on. So let me end this one by saying let's keep in mind. I think everybody know this, but let's keep in mind our choices aren't public access or no access, okay? I'm hoping that in the next few weeks we can get passed the different interpretations of ICANN's mission. And actually there have been some constructive comments about ICANN's mission today. And I recognize that. And really start focusing on how we can provide some access that's very controlled that deals with the bad issues that Kathy and Farzeneh and others have mentioned. While at the same time, allowing, assuming it's not inconsistent with ICANN's mission, maybe not purpose for collection, but dealing with some of these very real issues that probably we're all on the same page on. We don't want to happen.

So I just throw that out for everybody. It's not just - it's not a choice just between public or no access. And I want to challenge you to become creative in terms of how we can do this. And we'll try to work on that further in days to come. Let's move ahead to that last proposed purpose and the presentation there. if we can go to the other presentation by Drafting Team 5 on ICANN contractual enforcement. And we're going to go to Beth Bacon on that.

Beth Bacon: Beth Bacon for the record. So as we stated before, we did the other half of our presentation for Drafting Team 5 at the beginning of the session. And that was because in the previous iteration of our work we made delineations between what was, you know, what was regulatory. What and then what was

ICANN contractual enforcement. We felt they were two different beats. So this is very - the other - the previous was specific to regulatory bodies. And this is specific to ICANN's efforts with regard to contractual enforcement.

So this would be the information accessed to enable ICANN compliance, to monitor and enforce contracted parties' agreements with ICANN. So their use of the registration data. Question 1 as you can see, it's WHOIS associated with the domain name registration needs to be identified or contacted by contractual enforcement. And this is again, ICANN compliance. And there was some agreement that ICANN for some purposes needs to be able to identify WHOIS at the registrar and registry who knows about - who can, sorry, respond to questions about domain names.
There was a lot of question as we have on Bullet 2, this was - there was no agreement in the group. That we couldn't actually figure out why compliance would contact a registrant. There's no - they don't have a contract with the registrants. They probably would, I imagine they're data protection gentlemen. (Dan) would say don't query the WHOIS or the RDS for things you don't need to do. As the registries and registrars.

So we have that in there because it was proposed. But there was an agreement and I clearly was on the other side of that agreement. And then finally the - we moved down to what's the objective for reaching out to these entities. And again, some of this still would reflect that there's a second bullet talking about contacting a registrant. But if we all agree that you shouldn't be contacting the registrant, some of these would disappear as well. Just to - for uniformity.

So it's to provide notification of compliance issues and again, compliance issues are very clearly laid out in contracted party agreements. Ask clarifying questions, remediation, all of those actions taken. So the standard contractual compliance life cycle what would be expected of that entity. Registrars and Registries are expected to and required to respond to contractual compliance inquires and we would again through the life cycle of

that inquiry ask clarifying questions, provide some information, respond to the specific requests until that action was closed. So this one's pretty short and sweet.

Chuck Gomes: Thanks Beth Bacon. Now I want to call your attention. If you look that there are some blue text. One of the things that this drafting team did is reach out to ICANN compliance. And today, we have two people from compliance in the back of the room and relying on her colleague to talk. (Jennifer Scott), most of us know (Jennifer) have known her for a while from the compliance team. And at the table over here to my left over here is (Salim Mansak). Now they answered all our questions and they're answers are in the blue text there. But let's focus on this one about contacting the registrants. (Salim) if you could talk about that a little bit.

Salim Mansak: Thanks Chuck. This is (Salim Mansak) for the record (unintelligible). Let's start with that, you know, from Beth Bacon'command on that. ICANN contract compliance does not contact with registrant directly unless the complainant is also the registrant. So we see that complaints, for example, from transfer so that's more or less related with the registrant, registrants are also the complainants. So unless that happens, we didn't - ICANN contract compliance does not contact directly with the registrant.

Chuck Gomes: Talk a little bit about why you don't do that.

Salim Mansak: To talk a little bit about that is actually we as, again, as again mentioned, we don't have like the contractual obligation or registrants are not have - don't have a contractual relationship with ICANN compliance so that's why we prefer for registrars and the registry operators to contact with them on that matter.

Chuck Gomes: Marc?

Marc Anderson: Thanks. This is Marc. So a follow up question. You mentioned not directly unless the registrant contacts you. I'm wondering does this RDS play a role at all in validating that whoever contacted you is actually the registrant? And if not like what mechanism do you follow to validate that?

Salim Mansak: So for to contact with the registrants as I said, like we're not. But for that mechanism like we also have a validation method. We call like for the most current up to date WHOIS data to validate the registrant at the time of the complaint received by ICANN compliance. We do have that method to check, you know, through the WHOIS output. That's what we use actually.

Chuck Gomes: So I'm going to go to Lisa Phifer but just a clarification there. This is Chuck. So you may use RDS data to confirm the complaint is from the actual registrant. Is that right? I know maybe to identify them. Maybe not to contact them. I assume you get contact information when they file the complaint. Okay. Go ahead Lisa Phifer. No, that's -

Lisa Sifram: I have to questions. One is just a clarification. So you do look at registrant's data as part of compliance. But you don't use it to contact registrants unsolicited.

Man: Correct.

Lisa Sifram: And then my question is in the case where a complaint is filed that a domain name is using contact information of another registrant without authorization. How do you deal with that?

Salim Mansak: I think you're referring to the WHOIS accuracy complaints for that. Is that? So in case of - so we see actually different types of complaints on that matter. Like let me briefly talk about it. We may receive from one of the reporter, for example, (Salim Mansak) is me. But my contact (unintelligible) may be like, you know, used in other WHOIS contact data. So that may be type of a complaint that we may receive. So in - but these are, you know, kind of like,

you know, how we receive and how we also like, you know, validate the complaint. But also this is, I mean, this is basically how we use it.

Chuck Gomes: Thank you (Salim). Any other questions or comments of (Salim) or of this particular proposed purpose. Okay, so just to wrap this one up a little bit before we actually continue on this one and maybe and start deliberation. We have some time left, probably not enough to finish deliberation. But maybe we can get a good start. So it seems to me, and (Salim) this is probably to you, but it could be to anybody really. I think that you may have a perspective on this. If so if you - if the information that's public in the next generation RDS, is not sufficient for what you need to follow up with the registrant. We don't know yet whether that's going to be the case or not.

There might be non-public elements of the RDS that you may need access to. Now again, I'm - if my reasoning is wrong let me know. But if that's the case, that's something we'll have to deal with later when we see what is in, is public, to see whether there would be any registrant information that would have to be collected for that particular purpose. My personal guess is that might not be the case, but I'm just bringing that up. We can't really deal with that until we ultimately see what our recommendations are for public RDS data with regard to the RDS. And we could come back to you and ask whether that would - those are sufficient for how you would use it to maybe just identify. And Lisa Phifer made a good distinction there. And Question 1 really had two parts to it; identifying and contact. And they may not both be needed, but like that. Does that make sense?

Salim Mansak: Absolutely. Just to make it clear again. We, I mean ICANN compliance mission and vision is here like not to assume things. So, you know, before having anything in mind for before like, you know, the next gen RDS and also the GDPR, we are not in a position to assume, you know, what we will do in terms of have to use or have to validate the WHOIS data.

Chuck Gomes: Thank you very much. And thanks to both of you for being here. I hope you'll stay for our start of deliberation as well. Can we go back to the main slide deck please? And while we're doing that, if anybody else has a final comment on this one, or question, please feel free.

Okay, so we're down to Agenda Item 4. We made it to there. And by the way, some people have left. We don't have as many as Saturday, but this is what everybody's been wanting to do anyway is deliberate on this and the other. So we're going to - we're going to start and get a start here. Next slide please.

Okay now as we pointed out, Drafting Team 5 dealt with the ICANN contractual enforcement. If we had even more time, we were going to try and get to the domain name purchase/sell. We're not going to get there. We're going to try and start just the ICANN contractual enforcement. And look at the three questions. So here's what we're - we mean when we've been using the word deliberation. Discussing these three questions. Is these, and I'll add the proposed purpose into the question. Is ICANN contractual compliance a legitimate purpose for processing registration data? And let me remind everybody. When we say processing, that's a very broad definition intentionally. We're not yet getting - going to - at first, is there any type of processing that might be legitimate for this particular purpose. Do you want to jump in now?

Michele Neylon: Chuck it's Michele Neylon for the record. Yes, because I want to also leave in the next few minutes. So I'll do that now and, you know, I'll drop a bomb and walk away. So the one around contractual enforcement is an interesting one because we, as a registrar, we operate with multiple ccTLDs and obviously gTLDs. And there are contracts and there are terms to which we have to comply. So the contractual compliance function is not a matter of ICANN forcing a registrant to comply with anything. It's more to do with forcing the registrar or the registry to comply with a contractual obligation.

So this one is an interesting one to parse because in many respects the interaction as the gentleman from compliance already pointed out is between the contracted party and ICANN not between the registrant or some random third party and ICANN compliance. So is this a legitimate purpose for processing registration data? You probably could argue, well yes. But you haven't said by whom. And I think that's part of the bit that we'd need to pull out. As in, because the thing is this, Chuck. Contractual compliance doesn't deal directly with the registrant. Contractual compliance is dealing with the registrar and the registry.

So they have to make sure that we have fulfilled our obligations under the contract, but they don't have a direct relationship with the registrant. So they don't actually have - so they don't have a legitimate right to actually touch the registration data itself. Now that makes it, kind of, for an interesting problem. Because when - so ICANN is an American corporation. And because it's a not for profit, it can't actually sign up for privacy shield. So you can't transfer the personal information of your registrants to ICANN. I have no idea how you fix that, but that's a problem.

Chuck Gomes: Beth Bacon go head.

Beth Bacon: So I will - I just - my ears perked up. Let's pretend that one of the registries is a nonprofit corporation as well. So it's, I mean as we've tackled these, it's really different. And it's really difficult and let's keep in mind that not every solution is every entity involved has the same legal requirements. And by the way we have to rely upon model contractual clauses that are for the directive and once they update them, once we have a data protection board and they update them, then we need to replace them again. So get ready for that party.

Chuck Gomes: So by the way I think and I really can't speak from the drafting team here because we haven't discussed this. But based the feedback that we received from ICANN compliance, we probably would drop registrant from the list. And

that - we were waiting for that feedback, okay? And if any of you think I'm wrong on that from the team, just speak up, okay. But so let's put that one aside.

But a question I have for (Salim) and you probably you know I'd put you on the spot more. But do you need the RDS, any information in the RDS to manage compliance with registries and registrars? In this report, we suggested yeah, you need to be able to get registrant - a registry or registrar contact information. But my guess is you already have that. And this is coming back to what Kathy said in one of our other deliberations. If there's another source for the information, then you don't - if you don't need the RDS for that, then maybe this purpose goes away from the RDS perspective. So I'm, kind of, just for the - one of those things I said we'd have to get to, okay? Can you respond to that?

Salim Mansak: On behalf of compliance, I actually want to look at (Jen) for that, you know, to have her respond if I may.

Chuck Gomes: That's fine. There's a mic over there by Holly Raiche probably that's easily accessible. There's not one between me and Marc or I'd say here.

(Jennifer Scott): Hi, (Jennifer Scott) from contractual compliance. So I think the question is whether contractual compliance will use the information related to the registrar or registries contact information. And if there's another source if getting it from the WHOIS is a legitimate purpose.

Chuck Gomes: Let me clarify it a little bit more, I think. What I'm really asking is do you need the RDS to get contact information from - about registries and registrars? I'm guessing your probably don't.

(Jennifer Scott): Yeah, contact information is already available to us through our contractual obligations with contracted parties. But there might be other information that we need to see like their abuse contact information in order to validate that

they've got that requirement for abuse requirements met. But I'm not sure that that type of information, you know, will or will not be subject to this.

Chuck Gomes: Very good point. And I'll get to Marika Konings in a second. But - in the drafting team, we talked about this actually in terms of their being, you know, some of the ICANN contractual requirements relate directly to what is now WHOIS requirements, RDS requirements in the future. So to verify those, so you would need to not for contact purposes, but you may need the RDS for identifying that they've met the requirement. That's how - I'm sorry Marika Konings. Go ahead.

Marika Konings: Yeah, this is Marika Konings. That was exactly the point that I was going to make as because depending on what obligations are created for contracted parties, those will need to be, you know, verified. I'm thinking now we have, for example, have, you know, labeling and display. That may still be valid even if it's after, you know, behind the gate or tiered that requirement will still exist, and compliance will need to verify that, you know, contracted parties meet those obligations. So not a need to contact, but to look at what is being provided is consistent with what the requirements are I would think.

Chuck Gomes: So, and I hope I'm not - no, in fact, I'm going to turn it over to you guys. You can go in turn whichever order you want.

Michele Neylon: Oh, he's being gentlemanly, for once, exactly. Just Michele Neylon for the record. No, I mean the other ones, I mean the contractual compliance also conducts audits. And, you know, the way they conduct the audit has evolved and changed and, but it will change again probably in the future. But that can have - that can tie back to specific domains that they'll take a - I think the way you did it most recently is you did like a spot check X number of domains chosen at random. The last time it happened to us was hilarious because you managed to choose two domains all registered to me personally.

But it, you know, some is particular bits and pieces to do with those domains or aspects of their life cycle will be checked which could include display, etc. And there's also syntactical checks which goes down to, you know, is the - what was the one that a few of us got into? Had a bit of a problem with? I think it was telephone syntax at one point. I know it's a nonissue now, but it was something that would be in RDS WHOIS or whatever the hell. The one about the abuse contact that's an interesting one because depend - under the current paradigm for the abuse contact in a thick registry is something that's a problem for the registry operator to collect and manage. Whereas in the thin registry, it's a problem for the registrar to publish. So there's some interesting, kind of, things there. If you move to a system where everything is going through this hypothetically existing magical beast the unicorn over in the corner, then it'll probably look after all to of these things.

Alan Woods It's Alan Woods. One thing that we need to, of course, remember here as well is that ICANN is a data controller in this instance. And by reason of that designation alone, they have access to that data. We have a contract with ICANN which states that we must provide them with this data, so BRDA for instance. We provide them with that data, and they use it to enforce the contract (unintelligible), etc. And it's there already. So when we're actually bringing it down, do they have a legitimate purpose to access the behind the gate? One, they don't need to. So no, they do not have a legitimate interest in accessing that because it's not necessary. They already have that data; therefore we shouldn't be curating it.

Chuck Gomes: I'm going to differ with you. And see if I'm right on this. But isn't one of your requirements to display that in your - it is now. That may change, but if that - if you have a requirement, let's say in the future RDS that there's a requirement that you display the abuse contact publicly. They don't need - you've told them who the abuse contact is, but they have to verify that you're also not just giving it to them but displaying it as required in the agreement. We don't know whether that's going to be required or not. Did that make any sense? Beth Bacon go ahead.

Beth Bacon: So what I actually saw it. I think that what you're saying is that would actually be part - if we're talking about this, it's going to be the RDS data that is public. And then there's going to be the RDS behind the gate. And I think what we're talking about is compliance would not need the information behind the gate. And the abuse contact would be public. So quite frankly it's there and anyone can look at that if it's the public set of data. But we're talking about, you know, we have the - you have the contract with the contracted party. We have requirements with regards to responding to compliance and providing them with reports. So we are going to send in the data in that context. And then if they ask a question, we can provide more.

But if you need an abuse contact or something, I think it would be - that's a conversation of what is - what's the public set? So do we need the abuse contact in the public set or is that something that we could keep behind the gate? And that would help with this purpose. But if it's out front, I would say no. If it's behind, maybe. And I apologize, but I have to.

Chuck Gomes: Go head Michele Neylon.

Michele Neylon: Two words, data escrow. ICANN already, because ICANN is data controller for the data escrow, it already has all the data. So in may respects you could actually say well, you know, no. They don't need access, because they already have access. Now the data escrow is managed through a number of different agreements and terms and all that kind of thing, but they have access both for the registrar - to the registrar escrow and to the registry escrow. And then with the new TLDs, there'll be (ebaro), etc.

But again, this not a purpose that I get terribly passionate or excited about. I mean we can argue about it, because we're really good at arguing about stuff at ICANN. That's what we do even if there's no actual point in arguing.

Chuck Gomes: We do no arguing in this group.

Michele Neylon: I would have to beg to differ, Mr. Gomes.

Chuck Gomes: Your chance to disagree with me.

Michele Neylon: I just did. No, but joking aside, I mean I think the contractual obligations of something that we use to justify collection and processing of data. So when somebody - we would say to our clients, you know, you need to provide X, Y and Z. They go, why? We'll go well if you don't, we'll suspend the domain name. Oh why would you do that? Well, because I've got a contract that forces me to do this. So there's some interesting areas around it, but again I can't get excited about it. The jurisdiction one was a much more interesting conversation.

Chuck Gomes: Thanks Michele Neylon and you notice he's still here. He's enjoying this so much he hasn't left like he said. Griffin, please.

Griffin: Thank you. This is Griffin. This is in response to something that Beth Bacon just mentioned and she's not here anymore. But she said they may - hey, she just leave. So she said, you know, it may be necessary for a public data element that they still need to see it to determine whether that's there. But I think it could still apply to private elements or, you know, non-public elements as well because if there's a requirement that that element be included in the non-public data set, they may still need to check that that's being done if that's what is required.

Chuck Gomes: That's interesting, Griffin. This is Chuck. Yeah, I was thinking about that a little bit ago myself. Now, do they need access to the RDS in some way to verify that that's been provided? I guess that's a question we're going to have to figure out, but yeah. Good.

Alan Woods: So this, kind of - Sorry, Alan Woods. This kind of harps back to something that's been said a few times this week by (Yurin). He was talking about

whether or not in a certification sense, that ICANN themselves would need to be certified in order to get the data for the (unintelligible). And I mean the thing is and yes, I understand if it's in the public versus the non-public and I agree with Beth Bacon to that extent. But at the same time, they don't need to be certified to see that data that is in the non-public set because again, they are by their nature a controller and therefore have access to that data. They have a right to see that data without certification. So we don't have to go through that entire false process of certifying them. They just will have access to that data.

So again, and just to say what's going to happen here. And I think this will happen, continue to happen. When we're going through certain events of these deliberations. Is that we're not only looking at data minimization, we're also looking at purpose minimization in these things. And this is a prime example of purpose minimization. We don't need to over-egg the pudding in this. They have the data; therefore, it's not a legitimate purpose.

Chuck Gomes: Thanks, Alan. Lisa Phifer.

Lisa Phifer Thanks. Lisa Phifer for the record. I guess I'm a little lost in this because I understand the point being made that ICANN as the data controller has access to the data. But ICANN will need to demonstrate that it has a purpose, correct? So for example, ICANN will have to demonstrate that it has a purpose for escrowing data. And that will be a very specific reason to deal with failures and transfer of data in the case where a registrar is the accredited for example. But that’s very specific, narrow, limited use. And so then to take and say oh, but they can also use it for contractual compliance enforcement is a different purpose that still needs to be defined.

Michele Neylon: We will miss you Lisa Phifer you know that?

Chuck Gomes: (Unintelligible) please.

Vicky Sheckler: I'm not sure if I'm following Alan. But it seems to me if there is an RDS requirement and there are data elements supposed to be included within, I'm sorry. And their data elements are supposed to be included within the RDS, regardless of whether they're inside a gate or outside of the gate. And if that's part of the contractual obligation that ICANN at, you know, with its enforcement hat is supposed to check, they'll need to know if it's there or not regardless of whether they have it in escrow. Because it's a different purpose. And it's checking to see if the RDS obligation if there is one is being met.

Chuck Gomes: I'm not sure I got all of that. This is Chuck. But Lisa Phifer -

Michele Neylon: I speak fluent Vicky Sheckler sometimes. I can explain that one to you.

Chuck Gomes: So, but I want to - and I'll come back to Lisa Phifer and this may relate Vicky Sheckler to what you're saying. So help me out there. But so Alan said the answer to our question, the first one up there in red, was no. I think I heard you saying that no isn't the right answer. Did I understand you correctly? And explain to me - and you can too, do you agree - Vicky Sheckler do you agree with Lisa Phifer that the answer isn't necessarily no one is this a legitimate purpose for processing registration data?

Vicky Sheckler: I believe the answer to that is yes.

Chuck Gomes: Okay.

Vicky Sheckler: The reason I think it's yes is because we're talking about processing in the broad sense. I don't know if processing in this particular sense means you need to give ICANN the data distributed to them. I think it does mean they need to be able to access it to know that it's in the appropriate location.

Chuck Gomes: Yeah, okay. I get it. The - I needed some help there. So now like for example, the storing that they do is processing, right? Okay. Yeah, does that make sense Alan and Michele Neylon?

Michele Neylon: Yes, it does. I suppose as a checkbox compliance, yes. To be honest, why I'm going to waste time. I think this is non-contentious. I think we're just - we're teeing up the next things on this one. I think it's a good start. It's getting us warmed up, you know.

Alan Woods: And you can just refer to us as Ireland, Chuck. Because it's Ireland over here.

Chuck Gomes: I didn't call on you. So of course we can be very specific in the answer to this question. We use a very general term there processing. It's probably, this is the chair speaking probably out of hand, but we can be very specific in terms of the type of processing that's involved there. But we can get to that. Maxim.

Maxim Alzoba: Maxim Alzoba for the record. Just for - just small notice. First of all, we shouldn't assume that the current escrow contracts are going to be the same. And because of the trans-border transfers, for example, if the escrow provider is in the same jurisdiction, and trans-border doesn't occur with the storage, (unintelligible) will occur with the retrieval of information. And it might be forbidden for example. And it's the first thing.

The second thing is I'm not sure we need to just touch separate process here because escrow is separated from RDS. And to necessary you need personal data there. It could be -

Chuck Gomes: Say that again, please. I missed that last statement.

Maxim Alzoba: I mean that the escrow process is the storage of - offline storage of data (unintelligible) or somehow similar to offline. Because it's just snapshots of what's in the system's off-registrars effectively. Not necessary what's in RDS. And you can, for example, have situation where these storage of identity is separated from the technical storage of data. For example, for protection of the personal data. So we shouldn't assume that the current design will be in the future. So that it will not change in the future. Thanks.

Chuck Gomes: Good point. Now, watching the GDPR stuff, I've seen lots of stuff that looks like it, you know, that will seem to be a lot of people think that may be a legitimate purpose for backup and redundancy and stuff. But you're right. We can't assume that. We cannot assume that. Okay, I agree with you. Vicky Sheckler or not, I'm sorry. Kathy was next.

Kathy Kleiman: Is that a question we can as contractual compliance if they're here? Are there -

Chuck Gomes: Take advantage of it.

Kath Kleiman: And let me clear - rephrase what I think Maxim is saying which is that the public directory service or even the private directory service, public and non-public WHOIS may have nothing to do with what we're actually backing up for purposes of restoring by other registrars if a registrar or registry goes under.

Chuck Gomes: That sounds like a hard question and - but if you want to respond, however. Even if you have to go back and talk with your team or something, that's okay. But either one of you want to respond? Do you want to consult privately and then respond?

(Jennifer Scott): I think what you're asking is how the data escrow agents actually function. So I would probably have to defer to them on whether or not the registrars and how their interaction with the data escrow agent. If it's something that they're getting out of like their EPP system or if they're getting out of RDS, that I don't know. I'd have to defer to those experts.

Woman: Right, exactly. What data's going in?

Michele Neylon: So, Kathy. It's Michele Neylon. I might be able to answer the question. But what exactly are you asking? Because I didn't quite follow your question.

Kathy Klieman: And here I thought I was clarifying what Maxim said. But he was much clearer. Are we talking about two different systems? What goes into data escrow and what goes into an RDS? Are they - do they overlap?

Michele Neylon: No, they're - so the - so under the current data escrow specification, the - as a registrar I ship data to the escrow agent in a particular format. That format has absolutely nothing to do realistically with what I ship to the registries or what I display in public WHOIS. It's a very specific way of storing the data. So for example, as a gaining registrar of a failed accreditation, we would send two files by, I think it was - by ICANN via (environmentum) and then we had to try to reconstruct the registration data based on the files which, of course, made for some fun moments. Because some of those domains were no longer actually there. But anyway, that's another conversation. Yes, Kathy.

Kathy Kleiman: So can we just say this is out of scope for RDS - the RDS working group to talk about data escrow? That's just not in our scope.

Michele Neylon: Well no, it is in scope because it's a collection of processing of registration data. And the reason we're collecting and processing the registration data is because of RDS. So it is in scope.

Chuck Gomes: Let's think about that one, okay?

Michele Neylon: No, but I mean okay. The reason I'd say that is because if there was - if there's no obligation to collect data and process it and do anything with it, then there would be no data to escrow. Do you understand what I'm saying to you, Kathy? If I don't have any - if I don't collect any data, I can't escrow it. Can we all agree on that point please? If we disagree on that one, I'm really going to have a difficulty functioning. I'm going to stop breathing over here for a second. Come on. I mean look, come on. Even the IPC people are agreeing over there.

Okay, Kathy if I collect data - if I don't collect data, I can't escrow it. Can we agree on that? Okay, thank you. So the only reason that we collect a lot of this data at the moment in the way that we collect it and process it is because it's a contractual obligation which is tied back to the WHOIS specifications which is becoming the RDS, correct? And the only way that you can reproduce the data and move it across if the in cases of failure is if the data has been escrowed. So the two are interlinked.

Chuck Gomes: So hang on a second. Sorry about that. So we have Vicky Sheckler and Marc in the queue and Maxim. Let's let them jump in and see if they can help on this. And if we need to, we'll come back to you Michele Neylon, okay? And Vicky Sheckler you're next.

Vicky Sheckler: I think this is more than likely by ignorance, but I had assumed that part of the escrowing and the data is included in the escrow while it may overlap with what we're doing in RDS, it was not completely assumed within the RDS. And I think what I'm hearing you say Michele Neylon is that you're contemplating, and this could be my complete ignorance, that the RDS that we're trying to deal with is not the subset, but the entirety of the data that's collected. Is that what you're suggesting?

Michele Neylon: Well okay, at the moment, sorry, at the moment the way that the registration data is collected and processed, it's not centralized. So I collect and process and publish and do stuff with data. Then in thin registries, it's, sorry. I'm losing my voice which is I didn't do too badly. I mean we're on Wednesday already. It's not bad. The - it's decentralized. And then there's, you know, the registrar holds a certain set of data. The registry holds a set of data. The two sets of data should be the same, but sometimes aren't. And there's lapses and changes and yada, yada, yada. I mean this is the kind of stuff that you know, drive everybody nuts. But if you move to a paradigm where well, no we'd still be collecting the data. So the - it's the data that we're collecting that you're escrowing. It's not the data that's held by the registry that's being escrowed in that instance. So there is an escrow of the data at the registry.

So no, I think you're right and I'm right and we're all happy. I think.

Chuck Gomes: And that's, kind of, what I was thinking. That everything that's - the two are not a match what's in RDS and probably even less likely in the future. And what's escrowed. There's - there are elements that don't - they're not - it's not a one-to-one mapping is it?

Michele Neylon: No, it is theoretically a one-to-one mapping, but it might not be a one-to-one mapping. Because even if I - okay if you - how do I explain this? If I make an update to a domain name after the data has been escrowed for that 24-hour period, what's in the escrow is different to the data that I hold and is different to the data held by the registry. So and the thing is that can easily happen. Somebody changes a name server, or I don't know. The domain gets deleted. I mean suspended, any number of different things.

Chuck Gomes: Marc.

Marc Anderson: This is Marc. I think before I get to my point I'll maybe add a little fire or wood to this fire. So if you accept that, you know, collection is a subset of processing. It's a type of processing. You know, you can't have escrow without the collection of data. So there, you know, they're inexplicably linked. They're inseparately linked. So it's really, you know, it's a really impossible to completely separate out escrow from the RDS conversation. You know, so I think we're - we can't ignore it even though it may be a secondary topic for us.

But that's not really why I raised my hand. I wanted to get back to, sort of, the underlying questions we're looking at, you know, is this a legitimate purpose? And I went back to the definition and do you have the definition handy here?

Woman: (Unintelligible).

Marc Anderson: For contractual enforcement. So trying to get a, you know, back to the question at hand right. Our definition is information accessed to enable ICANN compliance to monitor and enforce contracted parties' agreements with ICANN. You know, so that's our definition of our proposed RDS purpose ICANN contractual enforcement. If you'll bear with me and go back to the other slide, I think this is an interesting question because it almost creates circular logic for us, right? So is this a legitimate purpose for processing the data?

It seems on the, you know, it seems to me it's very reasonable to expect that ICANN, you know, as one of the contracted parties has a role in enforcing their contracts. But you don't collect the data so that they can enforce their contract, right? And you know, and then they don't enforce the contracts, so we can collect the data. You know, so there's the possibility for circular logic and I think that's part of why, you know I think nobody in the room feels uncomfortable here. We're not, you know, we all - this feels like a legitimate purpose. But if you look at it the way it's phrased up here, it's really just sort of circular logic. And so I think we almost need a different route to approach this particular proposed purpose. I see people jumping out of their seats to attack this one. So hopefully they have some solutions.

Chuck Gomes: Thanks, Marc. And this is great. I hate to cut it off, but we're just about out of time and I want to be able to wrap it up. So if Maxim and Griffin and Holly Raiche if you could take no more than a minute each and then I'll wrap it up. We're going to continue this in our next meeting which will be a teleconference. I think it's the 27th, right? Week, the Tuesday after next week. Okay, and it will be at our regular time. But go ahead, Maxim.

Maxim Alzoba: Maxim Alzoba for the record. First, I think that escrow is part of the purpose. Not necessarily the part of RDS system. Okay, so that's why we need to mean - to mention it. The second, registry escrow is quite different from registrar escrow. For example, registrar escrow has real information which is

hidden behind privacy and proxy. And registry doesn't know if it's just set of symbols saying privacy proxy or the real privacy proxy. So the contents are different. And not necessarily registry will be able to know the registrant at all. Thanks.

Chuck Gomes: Griffin.

Griffin: Thanks. This is Griffin. I can keep it pretty brief. It's in response to Marc's point about sort of circularity here. I think the problem stems from our broad use of the term processing because you're thinking collection is the processing that you had in mind. And ICANN compliance may not - I mean the collection of the data may not be what's required for ICANN compliance purposes but accessing that data would be required. And that's a separate processing step.

Chuck Gomes: Thanks and Holly Raiche?

Holly Raiche: Pretty much exactly what I was going to say. The collection relates to the functions of registries. And registrar cooperation compliance is a different purpose which is to check on that. And that's a different part of the whole term of processing.

Chuck Gomes: So I need to do a quick wrap up here. So we end on time, I hope. First of all, a practical question. Can we isolate the recording for this meeting and the transcript for this meeting to just the ICANN compliance stuff that we've covered at the end of the day today? And the reason I'm asking that, if we can, it would make it easier to ask working group members to listen to that part, so we don't have to do an extensive review on our next meeting. Marika Konings.

Marika Konings: It is Marika Konings. I don't think for the transcript it will be any issue, but for the recording I'm not sure not easily possible.

Chuck Gomes: Well at least we could do - we could probably identify a time when that starts and do that. So an action item them would be to do that. So that we can ask before our next meeting which will be - Is the 27th the right date? Did I have that right, 27th of March? It's on a Tuesday. It'll be at our regular time. There may be a little adjustment because of the switch over to Daylight Savings Time for some jurisdictions. So let's make sure we're clear on that with everybody. Because I know in the US they've already gone to Daylight Savings time, right?

So that's an action item, I guess, for staff. What I'd like to just - for those that have been a part of this discussion and thanks. This was really, not only useful but it was fun. And there was good back and forth. This is what I hope we'll have more and more of in the future. We're going to have some tougher ones than this one. I know that. But we can still have some fun and grapple with the issues and come up with some solutions.

Think about and we're a little - this is a little bit premature, but I'd still like you to think about it. You don't - and if you come up with some ideas, jot them down. Think about how you might answer that question we're talking about. Is this a legitimate purpose for? And you're probably not going to - based on what I heard you're probably not going to use the term processing. You're probably going to be more specific.

If you come up with some ideas that might be nice before the next meeting. Because it might help us, okay? And go ahead Lisa Phifer.

Lisa Phifer: So I just have a couple of other actions too. Both for us to take note of what we have to do and to keep everyone informed of what will be done. So staff will take the notes from this session on and also Saturday's session for each purpose. And integrate that at the end of the drafting team answers for each purpose. And combine that with the original drafting team outputs for each purpose so that we'll have one document to look at for each purpose as a starting point as we get to it in deliberation.

In addition to that, we'll take a crack at trying to flesh out the summary table based on what we've covered both Saturday and today. As also as a way of getting our arms around all of the purposes not just each of those vertical, you know, slices of what a purpose might be. And those will be input to deliberation in the future.

Chuck Gomes: Thanks Lisa Phifer. And I want to give a special thanks to (Salim) and (Jennifer) for being here with us. And by the way, yes. By the way, and another action I guess is to send them the meeting information on the 27th. You would be welcome to join us on that one. We're talking about that and it would probably nice now. So think about that. And (Maggie) can decide whether, you know, that's good use of your time or her time or whatever. But you guys have been involved in this.

Woman: (Maggie) is sitting in the back.

Man: (Maggie)'s behind -

Chuck Gomes: Is (Maggie) here? Oh she showed up for us. Thanks (Maggie).

(Maggie): I've been here at the other session and this.

Chuck Gomes: Okay, I can't see very well back there. So thanks (Maggie). Anyway, we'll send - the staff will send out the meeting information on that Tuesday the 29th. It's not too bad for California time if you guys are all in California. Because that's where I am too, so it's been 9:00. I don't know if after Daylight Savings Time it's the same. We'll get that word out, okay? So hey, thanks to everyone. It's been a long meeting not as long as Saturday, but it was nice to end it on some deliberation which I know everybody's been wanting to get to anyway. And this is the kind of effective deliberation that I hope we can see a lot more of going forward. And again, this is an easier one. Okay, I get that.

So thanks a lot. I hope you all have safe trips home after these meetings and we will continue to plug away and try and make some good progress going forward. That said, the recording can stop and the meeting's adjourned.

END