**ICANN Transcription – Abu Dhabi**
**GNSO Next-Generation Registration Directory Services (RDS) to replace**
**WHOIS Policy Development Process Working Group Meeting Part 1**
**Saturday, 28 October 2017 08:30 GST**

Note: The following is the output of transcribing from an audio recording. 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

On page: https://gnso.icann.org/en/group-activities/calendar

Chuck Gomes:     Good morning, everyone. And for those that are dialing in remotely, hello to you as well. My name is Chuck Gomes, I'm the Chair of the RDS PDP Working Group. Good to see all of you here nice and early today. And we look forward to a productive meeting together.

The first thing I want to do is see if any of the working group members have an update to their statement of interest, just raise your hand if you do. Note we do have a mic out here in the front. Yes. Griffin, go ahead.

Griffin Barnett:   Thanks, Chuck. Griffin Barnett. So I changed firms recently so I'm at a new firm but otherwise my SOI is pretty much the same. Just wanted to call it.

Chuck Gomes:     Thanks. And have you updated that in the – on your SOI? Good. Thank you. Anyone else?

All right, let's take just a little bit of time to do some introductions, especially for those who are working group members, we won't take the time to do everybody in the audience that may be here observing or maybe you're a regular observer of the working group. But if the working group members would just probably you don't have to give much besides your name just so that people that haven't seen your face before can do that? And we only have three of these opportunities a year right now to – when we can work face to face, so let's take advantage of the time we have now.

I already introduced myself. And let me ask the vice chairs and the staff that are part of our leadership team to introduce themselves and then we'll go around the room. Let's start with Michele.

Michele Neylon:    Thanks, Chuck. Michele Neylon, I don't know – what else do you want me to say? That's it. Done. Perfect. Okay.

Chuck Gomes:    He's a vice chair, okay?

Michele Neylon:    Okay, yes, vice chair, yes.

Susan Kawaguchi:    Susan Kawaguchi, vice chair.

Lisa Phifer:    Lisa Phifer, ICANN staff.

Marika Konings:    Marika Konings, ICANN staff.

Chuck Gomes:    Okay…

((Crosstalk))

Chuck Gomes:    …let's start right over here with Maxim. We'll go down this row and that and if any of you are working group members and not at the tables, if there's a slot

at the table please come to the table, but would you go to the mic back there so you can quickly introduce yourself? Go ahead, Maxim.

Maxim Alzoba:     Maxim Alzoba, dotMoscow.

Alex Deacon:      Hi, I'm Alex Deacon with the MPAA.

Tapani Tarvainen: Tapani Tarvainen, NCSG.

Griffin Barnett:     Griffin Barnett, Winterfeldt IP Group, IPC.

Kris Seeburn:     So, Kris Seeburn.

Bastiaan Goslings:     Bastiaan Goslings, here in my personal capability. I work for the Amsterdam Internet Exchange and I'm a member of the ALAC.

Theo Geurts:      Theo Geurts, registrar.

Beth Bacon:       Beth Bacon, Public Interest Registry.

Vlad Dinculescu:  Vlad Dinculescu, registrar.

Sara Bockey:      Sara Bockey, Go Daddy.

Daniel Nanghaka: Daniel Nanghaka, AFRALO.

Kal Feher:        Kal Feher, Neustar.

Mark Svancarek:  Mark from Microsoft.

Rich Merdinger:   Rich Merdinger, Go Daddy.

Woman:           (Unintelligible) from IGF China.

Holly Raiche:      Holly Raiche, ALAC.

Rich Leaning:      Rich Leaning, RIPE NCC.

Farzaneh Badii:    Farzaneh Badii, Non Commercial Stakeholder Group.

Stephanie Perrin:  Stephanie Perrin, Non Commercial Stakeholder Group.

Marc Anderson:     Marc Anderson, VeriSign.

Roger Carney:      Roger Carney.

Chuck Gomes:       Thanks, all of you. And look, again, welcome to this session. The first thing that we're going to do is Michele is going to just do a brief discussion of the background of this PDP and I'll let him take over from there.

Michele Neylon:    Thanks, Chuck. Once upon a time there was an ICANN meeting without a discussion on Whois.

Susan Kawaguchi:   Really? I don't believe it.

Michele Neylon:    No, neither do I. okay, so for those of you who aren't familiar, we're just going to go through very quickly where this call came from. So years and years and years ago there was – what for years has been battles and arguments around Whois, we had the EWG and then back in 2015 you had the kick off of this particular working group.

                   So Board initiated a GNSO policy development process to define the purpose of collecting, maintaining and providing access to generic top level domain registration data and so forth. And we've got a timeline, we've broken it out – broken out the entire work of this PDP into multiple stages. And that's kind of

where we're – we're still in Phase 1. Chuck is our glorious leader and long may he continue to be so.

So we've been battling away on this since – when did we actually start? January 2016? Oh my God, yes, so I think we're – by the time we finish this I won't have any hair…

((Crosstalk))

Michele Neylon:     …I won't have any hair left. Next slide please. So our purpose – our job is to establish requirements for gTLD registration data and directory services. And you'll notice as well that a lot of these slides we don't explicitly say "Whois" because Whois is not – well Whois is a mish mash between the data and the methodology and the protocols which are currently used to display, store, process and do other things with that. Over the years the technical aspects of that have evolved and what we're moving towards now are replacements such as RDAP.

So we're looking at various aspects of it here, users and purposes, so we're asking who should have access to the registration data and more importantly, I suppose, why. Which elements themselves should we look at? Which elements should be collected and stored? And of course the big question, disclosed.

Privacy is obviously something we've discussed heavily, and we will probably continue to discuss. We've also been looking at the concept of gated access or differentiated access, in other words, the idea being that not everybody gets to access everything in the same way; depending on who you are you might or might not get to see different things. And of course another conversation that we are meant to be having in parallel is looking at, you know, how do you maintain the accuracy of the data within the system.

But the kind of fundamental question that we have to answer is, is a new policy framework and a next generation system needed to address all of those requirements? Or is everybody happy with the current one?

Next slide please.

And again another one because that's a very blank slide. Oh sorry.

Chuck Gomes: Susan.

Susan Kawaguchi: Okay. So at this meeting we're going to focus on the charter question, who should have access to gTLD registration data and what – and for what purposes? And I'm sure everyone's seen the WSGR memo, now the Hamilton memo and then somebody just handed me last night in the airport a memo from the EU Commissioners of some sort, have not read it really, first page is all I read.

And in all of these things we're seeing more and more it's becoming more apparent that the purpose of collecting, processing, accessing the data is key or core to what can be done with the data. So even though – we've known this all along, but it's become clearer and at least in my mind, that this is what we – this working group really needs to identify and work on.

And we've tried over the last year and a half to work on the purposes, but it's always, you know, we've gotten stuck and so we've tried to maneuver and move forward in some ways by maybe limiting the discussion to the, you know, thin Whois, the multiple – no, minimal public data set.

And so a few weeks ago after we received the WSGR memo, then we sort of reconvened the leadership team and decided that one of the issues we had in the working group is it's hard as a large group to have a fruitful discussion because things get lost in just in the amount of discussion and how many people are chiming in at once. Where in a small group it's a little easier to

stop and say wait, I don't quite understand that position, but let me hear more.

So we developed small teams and to identify key areas and we have six teams?

((Crosstalk))

Susan Kawaguchi:     …seven teams, sorry. I'm a little fuzzy, I've been sick all week. And so – and in these teams one of each of us from the leadership team sort of coordinated the discussion but definitely left it to the team – drafting team to decide what the purposes were, what the, you know, tasks that are supported by the purpose, the parties involved and the data that is often used to fulfill that purpose.

So we are going to have a presentation of the thinking and the draft purposes that each of these teams have come up with. And – but that doesn't mean that we've defined these in these small groups, and now it's set in stone. This is just hopefully helping the discussion in the larger group move forward a little easier.

And I know that the – I felt with the drafting team that I led or coordinated, it was an interesting discussion. We only had a couple of calls but I think we definitely came to some understandings and it was helpful to me at least to hear the other points of view. So hopefully this we can discuss once you've heard all of the presentations today and then we can enter into a full discussion of each of these purposes, which may take a while.

Chuck Gomes:    Next slide.

Susan Kawaguchi:     Is that me or you? So, you know, as I said, we're really seeing this becoming more apparent that the purpose is, you know, the key to the first element of the discussion that we need to have. And this is one of the ICANN

Board tasked the working group with answering the question of purpose resolved, the Board reaffirms its request for a Board initiated GNSO policy development process to define the purpose of collecting, maintaining and providing access to gTLD registration data and consider safeguards for protecting data. So it's definitely what we need to reach consensus on first.

Is there another slide?

Chuck Gomes:     Next slide. Okay. Go ahead.

Susan Kawaguchi:     So for what specific legitimate purposes should gTLD registration data elements in the minimum public data set be collected? So we started –we've talked about those that a lot. And we also in the working group decided that it was legitimate. In these small drafting teams we did not go – we did not take it that step. We purposefully did not take it the step of deciding, was this a legitimate use or is this just a use that's been happening?

And so that is for the full working group to decide. And we tried to not let the legitimate use hamper our thinking or determine, you know, determine our path. So domain name control is a legitimate purpose for minimum public data set collection. Technical issue resolution, domain name certification, domain name purchase or sale, academic public interest DNS research is a legitimate purpose, regulatory and contractual enforcement, criminal investigation and DNS abuse mitigation, legal actions and individual Internet use is a legitimate purpose for the minimum public data set.

So we started with all of those topics, grouped some of them into teams. And do we have another slide? No. And these are the topics that you'll hear the presentation on today.

Chuck Gomes:     So this is Chuck. And by the way, let me just from a logistical point of view, when you do speak, and we hope all of you will feel free to speak including those who are just observing and are visitors today, but so remember to state

your name when you do this for the recording and the transcript. And we'll try to do it up here as well.

These nine items are all items that the working group reached rough consensus on quite a while ago. So these are nine agreements that we've already come to in a preliminary manner. We can always come back and revisit any of these.

But each of these purposes – and they correspond to the nine purposes that the teams have just been working on – are – there's general agreement in the working group that they are legitimate as far as the minimum public data set is concerned. And the minimum public data set, just for those who don't know is what we've usually referred to as thin data in the past. Next slide please.

Okay, now what we're going to do now is we're going to divide the rest of our time this morning up to the break and after the break and five or six of the teams are going to share what they provided as their understanding of the purpose. Now our objective in this time we're going to have is to try and ensure that everyone in the working group, and of course guests as well, understand the purpose.

We're not going to deliberate yet on whether any of u think it's a legitimate purpose. We have to get there next. Whether we get to that on Wednesday or not for any of them, probably not great chances, but we will be then talking about legitimacy of the purposes after we ensure that everyone has a reasonably good understanding of the purpose. Whether you agree with it or not, we want to make sure you understand.

So one of the things you'll find me doing at the end of each of these team sessions will be asking you, "Is there anyone that doesn't understand, and if so, what is you don't understand about the purpose?" so that's going to be our metric, understanding.

And please, speak up if you don't understand because like Susan talked about a little bit, if we don't understand the purposes fairly well how do we decide whether it's a legitimate purpose for data beyond the minimum public data set?

Now, before we start the team sessions, and each of the team leaders will lead those sessions, I'd like to just open it up to see if there's anything that's been covered so far, including past work and we didn't spend very much time on that, where we're at or what's been shared so far, let me just pause and see if anyone has a question about what's been covered? Stephanie, you're first.

Stephanie Perrin: Thanks very much, Chuck. Stephanie Perrin for the record. I just wanted to clarify the concept of purpose here, because as I have pointed out in – not tedious detail in the working group, there is a big difference from a data protection perspective in stating the purpose of ICANN's collection, use and disclosure of the data as opposed to the various use cases that third parties might have for the data.

So for instance, ICANN definitely does not collect data for the purpose of academic research. They provide it when required for the purpose of academic research. That is a disclosure to third parties for those purposes, not a original purpose for collection. And I hate to get picky but it's really important from the perspective of defining the actual purpose of data processing at ICANN. Thanks.

Chuck Gomes: Thanks, Stephanie. This is Chuck again. And let me emphasize that our purpose today is to make sure we understand the purpose, okay? We're going to later, have to get into the level of detail that Stephanie is talking about, and when we make recommendations for final requirements, we're going to have to be very specific in that regard. But thanks for that input. Anyone else have a question? Milton.

Milton Mueller:      Yes, I think what Stephanie is asking for is not additional detail; what she's doing is raising the entire question of what you mean by purpose. And it seems like the working group has kind of gone off the rails in the sense that you've confused use cases with purposes. You've said this is a legitimate use. As an academic researcher I can say it's great when ICANN publishes data that I can collect for free and do things with. To say that that's the purpose of ICANN's Whois system is utterly crazy.

Whoever, you know, and that's just one of the nine. I would say about six or seven of those nine have the same problem.

And I think this is a very serious problem. And by the way, Chuck, you probably were there in 2006 when we had this same debate. Do you remember? And didn't we decide that the purpose was sort of contactability, some very basic simple thing like that? What happened?

Chuck Gomes:      So let me emphasize again, in fact I'll repeat it again, we're not making any conclusions about these purposes today. We're making sure that everyone understands the purposes. I don't know if I can say it any clearer. Can anybody else help me there? We're not saying that what you're saying or what Stephanie is saying is not critical in our future deliberations, we're saying that our objective today is to make sure everyone understands the purposes.

Milton Mueller:      I still think you're not understanding what I'm saying. It's – we're saying that some of those things are not purposes. So we understand them perfectly well. They're not purposes; they are use cases.

Chuck Gomes:      Fine. But we're not going to spend any more time discussing that right now. We will get there. Anybody else have a question? Holly, did you want to speak?

Holly Raiche:    My first question was – and I'm going to wait for the answer. I looked at Number 13 and thought I didn't really understand that, but I understand that each of those 13 categories that was on the previous slide will be discussed further, so that's fine. I think what Milton and you are doing are talking really across purposes. I think in a data protection sense when you look at why a particular individual or organization collects information, because that really is the foundation for saying that do you have to do with this? You know, is this a piece of information you need to do your function.

And that can be decided – that can be looked at as a purpose. And I think in the way that Milton is talking about it, you're asking the question, "Do you actually need this information?" Now I think what you're doing is using a different meaning of that term.

And I think that you've – the cross – and I hate to say cross purposes but what you're saying is how is something being used as a purpose as opposed to a justification for collection. And I think that's the difference, but I think what you're saying is you – we're now asking about how legitimately is the information used and the next question is then going to be is that a legitimate reason to actually collect the data in the first place?

So I mean, I think that although there's a lack of connection between the two, I think that's – and the sequence you're suggesting is looking at legitimately how is the information used and the next question you're then going to ask is, is that – is there a legitimate reason why that should be collected in the first place? So I'm prepared to go along with that sequence.

Chuck Gomes:    Thank you, Holly. And let me emphasize we're going to have to distinguish between use cases and purposes, and we're going to have to refine our language in that. I am not disagreeing with that at all. But one of the things we've discovered, and this isn't unique to this working group, that if we don't keep our focus fairly narrow each time we're doing something we go all over

the place and we get nothing done. I'm not disagreeing with Stephanie or Milton, I'm just saying we're just talking about understanding.

Now you're going to find when the teams share their – the information they came up with, there's going to be probably what you'd consider a mix of talking about use cases and purposes and they're not going to probably be terribly precise. We will have to be precise later on. Totally agree with that. But let's not go off there. We could spend three hours today just talking about that topic and we're not going to do that. Okay? We will get there.

All right, any other questions or comments? Okay, let's go to the next slide. Okay, this – oh we're going to skip that slide, that one's going to – go back there a minute just a second, just go back there a minute. So this was going to be our first one to discuss, that's going to be deferred until Wednesday for technical issue resolution. So just to let you know why we're moving on from that.

Next slide please.

Michele Neylon: Can I just throw myself on the sword, Chuck?

Chuck Gomes: Oh, I wasn't going to name you as the team leader that…

((Crosstalk))

Michele Neylon: It's okay, I'll quite happily fall on my sword. The reason we're skipping this is because I am a disaster and got completely side tracked with my day job and various other things and I didn't get a chance to pull this together in time so it's entirely my fault and Chuck and others may be rightly upset with me.

But I will say in my defense that in many respects the technical issue resolution is probably the least contentious usage of domain name data. So in some respects I don't feel too guilty.

Chuck Gomes:     Thanks, Michele. And I thought we had agreed that your day job comes second? Just kidding, for those that might…

((Crosstalk))

Michele Neylon:    My shareholders just don't share that view, Chuck, unfortunately.

Chuck Gomes:     Okay next slide. Susan, you're up. And keep in mind, we want your participation in this. If there's anything that Susan shares, and she's not going to be able to go through the full detail of everything in their presentation, in fact we asked the people who are going to share to keep it relatively brief, but it's critical if there's something you don't understand that you ask a question today so that when I come back – Susan's done and her team is done you can assure me that you have a pretty good understanding of this particular area. Susan.

Susan Kawaguchi:     This is Susan Kawaguchi for the record. And I coordinated the draft team for domain name control and then we'll also look at individual Internet users. And I just want to thank the team, I thought there was great participation so it was Maxim, Volker, Brian, Tapani, Alan, Daniel and Andrew. And we really had a pretty core group that dug in and sort of gave a lot of input so I really appreciate that.

                 And…

Chuck Gomes:     …don't have the ones that are here raise their hand.

Susan Kawaguchi:     Oh, yes, that's a good idea. So anybody on Drafting Team 2 that's in the room, do you want to put your hands up just so people will know? Maxim, just raise your hand just so we know. He doesn't want to be known. Okay, anyway, so it was a good group. And once again just to reiterate, these were, you know, each group – each drafting team was – we selected – the

leadership team selected one volunteer from each community and so we had perspectives from all over the community.

And that is really small but I've got that up on my laptop too. So this is domain name control. And you know, this is sort of the short version. Domain name registration, creation, management, modification, transfer and contact for operational issues, that's what we were looking at. And we really – Lisa put together a great template for us to work from. And to be honest, we used – we worked off of the EWG use cases to start.

And some of the tasks you see are lined out there, create registrant ID ,create domain name and DNS data for domain name, monitor domain name registration record, manage set of domain names to keep them under the same administrative control, transfer domain registration from one registrar to another or from one registrant to new registrant. Check registration database for status, existence of name when DNS does not work, and check information – contact information for ICANN policy compliance.

And so, you know, the users included the registrant, registrar, registry, ISP and other operational contacts. Domain name operational contact potential other users might be for a UDRP, WIPO, ICANN, court proceeding and enforcement actions. And in this area we tended to probably broaden the use case a little bit and move into some of the other topic areas that other teams also were working on, but we wanted to just call those things out here that it's just – it's domain name control may include some of those legal actions too. But I think another team will get into that further.

Reseller and registrant affiliates were important to be listed as users. New or gaining registrant, anyone attempting to interact with domain name for legal actions, ICANN Compliance staff and then law enforcement so these are all just users in the scope of the tasks.

And then there's a list of the data elements. And I'm not sure we need to go through each of those but you will see that it's almost the whole Whois record that we felt was needed to perform some of these tasks. So and the creation date became very important in our discussions too about fraud and like phishing for example.

And then if we move on down there's other uses for – can we just scroll all the way down to the individual Internet users? I think there's a second – there we go.

((Crosstalk))

Susan Kawaguchi:     Huh?

((Crosstalk))

Chuck Gomes:     That's getting into another purpose, that's not your topic.

Susan Kawaguchi:     That is…

Chuck Gomes:     Scroll back up, please?

Susan Kawaguchi:     Oh you want to discuss.

((Crosstalk))

Susan Kawaguchi:     Okay. Sorry. I was just going to flow through all this. Sorry about that. So I don't know if there's any questions or concerns or – and Maxim wanted to add something here.

Maxim Alzoba:     Maxim Alzoba for the record. Actually in the place we have users for the domain control, I think we need to add URS after UDRP because it's, yes, it's similar but different.

Susan Kawaguchi:     I think you did tell me that and I missed it in my notes. So we just want to. Any questions, concerns or opposition to these use cases?

Milton Mueller:     Can you just tell me in abstract terms what you mean by domain name control?

Susan Kawaguchi:     Just any…

Milton Mueller:     Control by whom? For what purpose I guess?

Susan Kawaguchi:     So if, you know, what we were working off of – and let me just bring that up real quick on my computer – were possible uses – and these were detailed by the EWG but domain name registration accounts and creation. So domain name control that you would need to provide all this contact information to create an account to register a domain.

A domain name control could also be domain name data modification and monitoring. So if – to control your domain name as a individual or a corporation, you need to monitor that information that is in the Whois record because sometimes it gets changed when it shouldn't when it's unauthorized to be changed.

Domain name portfolio management, domain name transfer initiation and then deletions, DNS updates, renewals and contact validation.

Michele Neylon:     Thanks, Michele for the record. Milton, I think part of the terminology, "domain name control" might sound terribly oblique, but in real terms it's looking after your own domain names, it's not controlling anybody else's domains, it's just looking after your own domains in many respects. So like in the case of say okay, Blacknight.com and that's our primary corporate domain name, if for some reason the name servers were to change on that or the expiry date

were to change, I would really, really want to know that and quickly. Does that help?

Milton Mueller: Yes, I think it's such a fundamental thing that it needs to be formulated properly and domain name control is kind of – like you say kind of an oblique label. So what you're concerned about is ensuring that the domain registration records are under the control of the authorized party, something like that, right?

Michele Neylon: Yes.

Susan Kawaguchi: Yes.

Milton Mueller: Okay. That's a good purpose.

Michele Neylon: Oh yes. Yes, we wouldn't let…

((Crosstalk))

Chuck Gomes: We're not determining whether they're good or not, but I agree with you.

Maxim Alzoba: Maxim Alzoba for the record. In users I think we need to add gaining registrar because it happens when a registrant want to move his domain from one registrar to another, yes, some reason.

Holly Raiche: Sorry, is that a purpose?

Michele Neylon: It's Michele. No, it's a user – could you please state your name for the record?

Holly Raiche: Holly Raiche, ALAC. Is that a purpose?

Michele Neylon: No, he said it was a user.

Holly Raiche: It's a user in a transfer so you would have a losing registrar and a gaining registrar.

Michele Neylon: I hate losing them but I sometimes gain. No, I mean, if you transfer a domain from Registrar A to Registrar B then there were two registrars, and then sometimes you have to undo the transfer and send it back to the original one.

Holly Raiche: Or…

Michele Neylon: Or…

Holly Raiche: …an unauthorized transfer to a new registrant too would be in that same.

Michele Neylon: Well, hold on now, you're complicating things.

Chuck Gomes: This is Chuck. Let me interject something here. Our purpose statements aren't going to be everything that's in these documents. To understand the proposed purpose we felt like it was critical to understand not just have a good definition of it, but to understand what tasks are involved if somebody is controlling a domain name, what users might be using that, what data elements might be involved.

Now just to - for those of you that haven't picked up on it, we're going to, you know, we're going to have to get down into the detail and we're going to have to figure out, okay, what data elements would be displayed for what users would have access to perform some of these tasks.

So all that will come and that gives you a little bit of idea how much work we have ahead of us. But again, our goal is understanding and it's hard to understand a proposed purpose if you don't understand these other elements.

Susan Kawaguchi:    All right, Susan for the record. Maxim.

Maxim Alzoba:    Maxim Alzoba for the record. I think it's in the users we have ICANN Compliance staff but it could be also ICANN audit, yes, because they need access of the information. And for Office of ICANN CTO, I'm not sure that we need to limit it to ICANN Compliance. So we need to understand maybe just ICANN staff, I'm not sure.

Susan Kawaguchi:    Okay.

Maxim Alzoba:    Thanks.

Susan Kawaguchi:    I'll make those changes. Holly.

Holly Raiche:    I'd rather keep it at ICANN Compliance but a small C so that people who are involved in checking and so forth they have, but ICANN staff can be loads of people who have nothing to do with the system who have something to do with very, very different tasks. So I'd rather keep it small but if you've got a small C then you take those sorts of people anybody who is involved in the sorts of tasks to make sure that the rules are being followed and just keep it as a small C. But I would not like it to be ICANN staff generally. Thanks.

Susan Kawaguchi:    How do you feel about that, Maxim?

Maxim Alzoba:    I'm not sure we can use short sentence to say that only the ICANN staff which has power to access information on behalf of organization or something, but we can keep it like ICANN staff, yes, ICANN Compliance, ICANN audit, ICANN CTO office, SSAC, you know, most probably they need to access something. But as many registries, for example, they give information to ICANN with the disclaimer no sharing with third parties, maybe does not harm.

Chuck Gomes:    Chuck again. So we're getting ahead of the game here. Okay? We will have
                to, if we decide that there should be access to certain data elements, we're
                going to have to define which data elements, we're going to define if for
                example there's gated access to some of this information, who would have
                that access. We haven't decided that yet; we're not deciding it today.

Susan Kawaguchi:    Okay any other comments? Lisa.

Lisa Phifer:    Thank you. Lisa Phifer for the record. So there is another team that is looking
                at regulatory and contractual compliance so how does that relate to this
                purpose? And I'm wondering if there's overlap if that discussion shouldn't
                take place in that purpose.

Michele Neylon:    Thanks. Michele for the record. I think actually that's a very good point. I
                mean, the – when we were working on this concept of breaking out into
                smaller groups, slicing and dicing a little to make it more manageable, one of
                the conversations we definitely had in the group I was meant to be
                coordinating, which I did a terrible job of, was that you had this kind of
                situation in our conversations where it was like oh hold on a second, you
                know, is this something that's better in that group over there? Because there
                aren't clear lines around some of these things.

                I mean, with some things you kind of go yes, you know, that bit of data over
                there if it's only could possibly exist would be used for what specific thing. But
                for other ones it's not a clear – there is not a clear line. I mean, you have
                different scenarios in trying to break things out into neat little boxes probably
                doesn't work as nicely as one might wish.

Susan Kawaguchi:    And just to add onto that, Susan Kawaguchi for the record. But and I did
                sort of when introducing this said we went a little broad on some of this. But I
                also felt it was important to note that and to, you know, track those tasks or
                users because then when we see that overlap with the other teams then we

know that we haven't missed anything so we have, you know, we definitely went a little broad on this.

((Crosstalk))

Chuck Gomes: Well we're not ready to move on yet. I have to get a measurement of everyone who's here including anyone who's online. Is there – in fact let me just, for the sake of those in the room, how many of you think you understand what domain name control is about? Would you raise your hand? Okay, there's a lot of hands that haven't gone up which means you don't understand, right? So we need you to ask questions in that regard, what is it you don't understand? Go ahead, Milton.

Milton Mueller: I think I understand so I want to read out my summary description and maybe you could even enter it into the record to make sure we agree. So by domain name control I think you mean collecting the information required to ensure that the domain name remains under the control of the registered user and that no unauthorized changes, transfers are made in the resource record.

Susan Kawaguchi: Sounds good to me. Can we capture that or not?

Chuck Gomes: It will be captured because we're – in the transcript. So thank you. Again, though, we need, you know, I'm concerned that a lot of you didn't raise your hand. The – because we really do, and it's especially critical for working group members to do that.

But we would like the rest of you to understand too. And Milton provided a nice concise definition there that we – and that may be what we use for that. So does anybody else have a question – oh I can't see Lisa, she's too close to me. Go ahead, Lisa.

Lisa Phifer: Thank you. Lisa Phifer for the record. So the definition that Milton just offered makes sense to me during the lifetime of the registration but the piece that it

seems like it might be missing is registering the domain name in the first place, which I understood domain name creation to be part of this purpose.

Chuck Gomes: Thank you. And we'll refine that. One of the things that it's real easy in the working group to get off on and spend all of our time refining languages in meetings, and we found that that's not the best place to make the language perfect. We can work on that offline, but a good point there.

So any other questions – yes, Maxim.

Maxim Alzoba: Maxim Alzoba for the record. Actually it's small note coming out of the work of Security Framework Group where we have interaction of registries, registrars and law enforcement, GAC, Public Safety Working Group, and always law enforcement is local law enforcement.

For example, if local for ICANN, law enforcements request something, it's law enforcement action for ICANN. And if registries stated, yes, which is resident of some particular country has a request from the local law enforcement it's law enforcement.

And when the same registry has a request from the law enforcement of third country, at the best it's pure third party for them. If knowing to governmental, I'd say, special agreements, are in place, for example Great Britain and United States have some special agreement with cross recognition of law enforcement requests. In absence of such agreements between countries, if you have a request from a list of some, yes, unknown small country, for you as a registry or for you as ICANN, or for you as registrar, it's at the best third party; at the worst it could be worse.

So we might need to add in commas, local, to law enforcement. And it's important. Thanks.

Susan Kawaguchi:      So I think we did have that discussion to a certain point but I didn't capture that so we can add the local law enforcement for those reasons. Yes, and so Lisa's point is – Susan Kawaguchi for the record. But a good point, I think that the law – the drafting team that covered the law enforcement may have more detail on that and we may have gone a little too broad for our domain name control for that. Okay.

Chuck Gomes:      Okay, I'm glad to see some others going to the mic. Go ahead.

Owen DeLong:      Owen DeLong, Akamai for the record. Local may be a little too narrow as well because for example, in the United States where I am from, local would cover the city police in the city you're operating in but it might not cover the state police or the county sheriff's office or the Federal Bureau of Investigation, and it would certainly exclude for example any cooperation with Interpol that may be subject to treaty and other such things.

Chuck Gomes:      Thank you.

Monika Ermert:      Hi. Monika Ermert, a journalist. I'm new to this discussion and you have to – sorry? Okay, sorry. It's better now? Okay, Monika Ermert, journalist. I'm new to this discussion, you have to explain something to me, why for domain control for transfers is law enforcement a party at all or third parties? Why are they a party to change control? Which I would understand as domain control.

Susan Kawaguchi:      Unfortunately we didn't catch all of that.

Monika Ermert:      You didn't catch it? This is about domain name control, so like – things like change control. So why are third parties like police, local or to local, be a party at all?

Susan Kawaguchi:      So once again, we did go a little board, but let's – let Maxim answer this.

Maxim Alzoba:     First note about local, it means the relevant to the jurisdiction when the party is situated and it's relevant for registry for example, it's relevant for registrar and relevant for ICANN because if California sheriff office comes with – to ICANN with some, yes, form properly made paper most probably ICANN should read it and do something they want if it's in the bodice of the law.

And about domain name control, it's a thing called domain name seizures, for example, some domains – not seizure – the process where the court says you have to give these domain to this law enforcement body and as law abiding company you have to give it to them. That's it. We just follow law.

Susan Kawaguchi:     Can we let Monika respond though?

Monika Ermert:     Yes, and just a follow up question, isn't then still the company or the individual user who is compelled by law enforcement, a court, or whatsoever doing the change in – initializing the change?

Michele Neylon:     No. Sorry, Monika, it's Michele for the record. I'll give you a clear example. We are a registrar, we are based in Ireland. We sometimes get a – get court documents from the United States. I cannot act on a court order issued by the court of wherever in, you know, in Texas or something like that, I can't do that.

So we will ask – we will respond and say, you know, we're an Irish company, we're not subject to US law. You can domesticate this or whatever. And so what sometimes will happen is instead of them domesticating the court order to the Irish courts, they will kind of go, okay, we won't bother with this, we'll just go straight to the registry. So they sidestep the registrar completely, go straight to the registry. They're not actually sending – they're not trying to act on the registrant, they're acting on the domain itself.

I mean, but you may not like this but that's what they – that's the reality, I mean, this is what we see. Or more recently in the case of what was

happening with dotCat, we received a request from Spanish law enforcement to do something with the dotCat domain name, we told them well, no, you need to go through the – go through the correct channels, (unintelligible) that from the Irish police we'll be able to act. So instead of doing that they just took a court order directly to the registry. So, yes, that's what we're dealing with.

Susan Kawaguchi:     Stephanie.

Stephanie Perrin:  Stephanie Perrin for the record. And I understand that this – these groupings are somewhat loose and flexible and there will be further discussion on it, but I think part of the problem here is the use of the word "control." If we talked about domain name management and drew a bright line between domain name management per se that is normal, and then these unusual circumstances which of course I'm informed by the anti abuse community that they aren't that unusual, but if you kept that in the legal category then the interventions of what I would call those representing applicable law, using the word "applicable" as opposed to "local," that would be a lot clearer.

Because obviously there's a lot of routine domain name management that doesn't fall into the getting your court order from the local constabulary, right? And that would make those of us who are uncomfortable with this analytical frame a lot more comfortable because there's a bright line there. Thanks.

Susan Kawaguchi:     And we – Susan Kawaguchi for the record. And we could do that and I think we have in other cases, you know, the EWG definitely did that. And we can go back to that. But I also felt it was interesting in the conversation the discussions that we had as a small team that we include some of this and having managed corporate domain names for over 20 years, you know, for big entities, the reality is that you're contacted through your day to day admin email address which I was host master at eBay.com and you know, domain@fb.com, I was that first line of defense for our company and in

responding so those came to me. There was very few other people that even paid attention to those.

So from a domain management perspective, that was something that was on my checklist to do, okay this goes to this department, I won't handle this, you know, request, from a law enforcement, but I'll make sure that somebody responds to this. So it is a management responsibility. But we could take that and put it into okay, all things law enforcement over here.

Stephanie Perrin: That's where you draw the bright line because your management and then you send it over to law enforcement and that's exactly, you know, I'm not trying to get rid of the function, it's where do you draw the line, yes.

Susan Kawaguchi: And if you don't do that, you end up in big trouble.

Stephanie Perrin: Right.

Susan Kawaguchi: You lose your domain name sometimes.

Chuck Gomes: So I think Stephanie, you hit the nail on the head with regard to the word "control." I think that's probably what's led us a little bit into other areas in this discussion instead of just understanding and the two of you seem to be agreeing that maybe management is a better word than control. And we'll work on that, we don't have to finalize that today.

Any other questions or comments about domain name management? And again, we took these terms from the Expert Working Group report and this is no criticism of them at all because they did some great work, but so we can refine the word so it doesn't lead people down the wrong path.

Lisa Phifer: I just – this is Lisa Phifer. But I just wanted to read into the record the comment from someone participating remotely. Claudio says, "How about

using domain name administration, which actually pairs with the fact that this is the administrative contact."

Maxim Alzoba: Maxim Alzoba for the record. I have suggestion, could we call to domain name management and change or change of control? Because it's change of control when the third party…

((Crosstalk))

Chuck Gomes: I think those may be a little bit too restrictive because we've already talked about things besides those two things, so I think we're going to draw this one to a close.

This is Chuck speaking. Because we want to get to others today. One last chance, anybody want to say I still don't understand what this particular proposed purpose is about?

Okay, let's go onto the next team and you don't necessarily have to go – well yes, if we can have the slide for the next team that would be good and then we'll actually bring up their – the document that they delivered to the working group.

And I apologize that some of the documents didn't get out with much lead time so that everyone could review them in advance, that was our original intent, unfortunately we didn't fully succeed. So the next…

((Crosstalk))

Chuck Gomes: What?

((Crosstalk))

Chuck Gomes: Okay. So the next – yes, Griffin.

Griffin Barnett: Yes, thanks Chuck. Just quickly, there was a section from the last group I think called individual Internet use, did we want to cover that at all?

Chuck Gomes: No, we haven't covered that yet.

Griffin Barnett: Okay so that's coming later or…?

Chuck Gomes: We're not covering them in the order – in their numerical order, okay? We tried to cover them and we have some rationale for the way we grouped them…

Griffin Barnett: Okay, I just thought it was part of the same group as the previous…

((Crosstalk))

Susan Kawaguchi: …worked on them.

Chuck Gomes: Yes, we're not doing them by team but rather by – and in fact for the sake of breaking things up we decided to split up the two purpose – there were two of our seven teams covered two purposes – proposed purposes, okay? So that they didn't go all at once, we're breaking them up, so.

Okay so now David, unfortunately, could not be with us. Is David online? I know Alex is going to do it but just for the sake of knowing, I don't know if he's online or not. But we'll let Alex – Alex a member of this team, Alex, you want to take over?

Alex Deacon: Sure, Chuck. This is Alex Deacon. So we were tasked with the domain name certification piece, and this is essentially the certificate authority use case, if you will. Are we going to put up the doc or – oh sure, yes. So it was myself, David, Kal, Carlton, Jeremy and Arsene, we were tasked to come up with this.

Based on my past experience in this industry I kind of took the lead and put together this document. And we had a nice discussion about it. And the result is this doc. I'm not going to read this but maybe I'll just touch kind of upon the – what I think are the interesting parts of each of these sections. So really the role of a certificate authority – of a CA – is to bind an identity of some kind to a key, a cryptographic key in the form of what's called a certificate.

So in the case of TLS, or what used to be called SSL, this identity is typically a fully qualified domain name. And so what the certificate authority does in this case is validate that the domain name is in fact associated with the person requesting the certificate.

And there's a lot of ways to do this and we're not going to get into a discussion  or a debate about the different levels of validation and the different means of which that validation takes place. But I think it's just important to know that there is – there are different ways to do this and there's quite a few ways to do this.

In the task section we talk about the different types of validation, domain name validation, organization validation and extended validation. These are different levels of verification and authentication. The domain name validated certificate, this regime, if you will, doesn't use the Whois system.

The organizational validation and the extended validation certificates do. So you'll see when we kind of continued through this exercise that we focused on those two use cases because they do in fact use the Whois system and that's kind of what we're focused on here.

And so if you scroll down just a little bit, for this type of validation, Whois is used to confirm that the enrolling organization is listed as a registrant in the Whois system and there's lots of ways to do this, it could be automated or it

could happen manually, email can be sent, phone calls can be made, I suppose faxes can occur also.

How CAs do this validation and verification are defined in a document specific to the CA world called the CA Browser Forum Best Practices and so I've put a list in here. And then I just copied for I guess ease of reading, Section 3.2.2.4, that kind of describes exactly how Whois can be used and can be used to do this verification.

Again, I won't read this ,but if you look at Section 3.2.2.4.1 and dot 2 and I even think the next one, dot 3, it kind of describes how these various Whois fields can be used for the purpose of performing a validation and the verification of an identity for a requested certificate.

And dot 3 you'll see phone. Keep on going, there's other ways. I only included in this copy and paste the – again, the text associated with fields that leverage Whois. So who uses this use case, the users of this use case are employees of a certificate authority or automated systems run by certificate authorities.

This is how the validation takes place. And then here's the data, what we did is you'll see this is very high level, it's been about five, six, maybe seven years since I've actually been directly involved in this – in the CA world so I've reached out to some colleagues who are still in that world and have asked them to specify exactly what fields their systems leverage.

But if you look through the various documents at a high level, and I know this is perhaps overly broad, but they do use all of this information, registrant, tech contact, and admin contact and they use basically all of that information to perform their verification and validation. So that's it.

Chuck Gomes: This is Chuck. Thanks, Alex. And thanks to all the team members that contributed this. And the – as everyone can see, today, Whois data or RDS

data is used by certificate authorities and what we want to do today is make sure that everyone understands this particular proposed purpose. Are there any questions for Alex or any of the team members? Yes, go ahead.

Kal Feher: Kal Feher for the record. I was on that team. I'm not sure if one of my emails made it to the mailing list or not, but one of the things I wanted to clarify was that the RDS is actually not used at all for any of the identity validation. If you read the CAB Forum policies clearly, the baseline requirements require you to use the RDS amongst other options, for proving domain control only. Everything above that so for example an organizational validated or extended validated certificate they always explicitly use alternative sources for validation.

So none of the things that are listed there are actually required to get a certificate. You could actually have no information at all in RDS, and successfully get all the way up to an EV certificate based on those requirements. If it's there there's certainly – that's a valid use of the data. But it's not strictly required.

Now that's not to say that today certificate authorities don't use it as a convenience, but if we're being very pedantic and we're restricting ourselves only to what's absolutely required, you could get all of the – you could get all the way up to an EV without any – with a fully private Whois.

Alex Deacon: Thanks, Kal. This is Alex. So, yes, I don't disagree with that. I think what I hope to do is, again, by reaching out to folks that are actually doing this today and using – building the systems and validating and verifying certificates to get a better concrete understanding of exactly what they're doing, I agree that they do leverage lots of other third party databases to do this, but I think understanding what's done today is important.

Michele Neylon: This is Michele. I mean, just following up on this, I mean, we – in my #dayjob, you know, we sell SSL certificates. The dotIE ccTLD is anything but verbose,

I mean, you will look you will see, you know, the organization or the individual to whom the domain is registered and that's about it. No contact details appear in the public Whois at all.

And yes, we have EV certs, our clients have EV certs, but a lot of the certs now are just domain validated so it's based on the existence of either of a TXT record or a sub domain or something like that.

And of course to add to the fun and games then you have certain people out there who are quite happily giving away SSL certs without any validation whatsoever but that's another conversation.

Chuck Gomes:     Milton, go ahead.

Milton Mueller:     Yes, I think this is a good example of how we have mixed up or confused use cases with purposes. So let me just ask you this question, you've described how you as – Whois sometimes used by certificate authorities, but is there any information that needs to be collected by ICANN to support certification of a domain that is not already collected under the rubric of domain name management or control?

Alex Deacon:     This is Alex. I think the answer to that is I don't think so, but again it's been several years since I've been in that business. I think the data is collected, and I think to your point earlier around contactability, that's the important part is when a request comes in how can a CA contact the registrant to do its validation? Right? Michele…

((Crosstalk))

Michele Neylon:     Sorry, this is Michele, just going to disagree with you slightly. Because what the CAs are doing is working off a list – there's like a list of about 10 contacts if they can't get the one in Whois, which they'll use to reach it. So it's actually, I mean, your question is valid, I mean, what we're looking at is use cases as

opposed to purposes and, you know, to the – the thing that they're doing is just sending those emails.

Alex Deacon:        That's right. And sending those emails to contacts not only listed in Whois but other ones also when that fails or doesn't work. Okay.

Chuck Gomes:        Okay, this is Chuck. Kal, go ahead.

Kal Feher:          One of the things that might have clarified that conversation we did discuss on the call but I think we ultimately decided not to add this to the report, having – splitting it between collection and consumption. There's not much reason to collect this information for the purposes of certificate but if it's there there's certainly a valid reason to consume it.

                    So if you look at the guidelines Whois data can be used for contact, it is one of the optional choices for a CA to validate domain control, but there are other alternative ones that don't require it.

                    So if the data is there then CAs should be entitled to review it. But whether it's strictly required for collection, that's not strictly required I guess, yes.

Chuck Gomes:        This is Chuck. And of course we're going to have to decide later whether we think access should be given even if it collected. So keep in mind we're not going to go there today, but that's going to be a very critical decision for the working group to make with regard to access, okay? But again, this is I hope this is very helpful in terms of understanding what this particular proposed purpose is, and it may just be a use case, but we'll deal with that, okay?

                    Susan, did you want to jump in?

Susan Kawaguchi:    Yes, I just have a question, and because of managing domain names for Facebook I was definitely a part of the process to validate. So, you know, whatever cert company we used, we had an account with them, we had –

provided them all kinds of information and – but each and every time we requested a cert, they would then come back to the admin email address and say please validate that you made this request.

And so without that email address and without being able to independently validate how would that – any cert authority know that the request for a cert for Facebook.com was a legitimate request and they weren't issuing a cert to, you know, third party for criminal use.

Alex Deacon: Yes, this is Alex. So I think that's the key part of the binding, right, this is, you know, the – and a central, I guess I would say part of binding the FQDN and the cert to the organization that owns the cert. And the way they do that is via the registration records and using email addresses to ensuring that they're actually getting to the organization that's listed as the registrant and to someone else that's pretending to be there. That's right.

Kal Feher: Just to add to that, it's probably the easiest for a consumer if you send them an email that they need to respond to. But there are alternatives available to CAs whether or not those – all CAs support that, that's a different discussion. But certainly a change to your domain name or a text record or a Website change which are obviously easier or more difficult depending on the type of organization. So there's no suggestion that emailing to a Whois contact is a bad idea, it's just that it's one of the options, not all of the options.

Chuck Gomes: Great discussion. So let me ask the measurement question, is there anybody that still doesn't understand what this particular proposed purpose is about and how they – in our environment today how Whois is used by certificate authorities and their staff? Milton.

Milton Mueller: Yes, I don't understand it as a purpose. I think it's been very well established here that it is a use that doesn't even require any new data to be collected so that we could actually knock it off the list and not lose anything.

Chuck Gomes:    And we'll decide that later. But that's an option. That's an option, as long as everybody understands what we're talking about. And that's been a nice thing that's come out of this actually give us some information and the work that the team did is very helpful, I think in – and will be helpful in the future as we make key decisions. Alex, go ahead.

Alex Deacon:    Yes, this is Alex. And just to respond to Milton, you know, we were tasked to describe the use so – which is what we did. And then we'll have further conversations about purpose and so on later.

Chuck Gomes:    Lisa.

Lisa Phifer:    So this is Lisa Phifer. I understood you said earlier you thought information that was already in the record was used by this case and not necessarily collected, additional information was collected.

                But if there were additional information collected for this purpose, if there were, then this purpose would be information collected for the purpose of allowing the registrant to have a certificate issued to them?

Alex Deacon:    Yes, I mean, I guess if we're thinking about what new information could be collected, and I haven't thought about this, you could envision, you know, a certificate authority contact which may or may not be the same as the admin contact or the registrant directly, right? You could envision, I'm not saying we should do this, but you could envision that that could be collected and used for the specific use. Yes.

Chuck Gomes:    Thank you. This is Chuck again. Now how many of you think you have a fairly good understanding of this particular – and I'll use the word "use" – of this information, would you raise your hands? Okay. Does anybody have any other questions on this one? Okay, thanks for the good discussion on this. And again, thanks, Alex and David and the whole team, Kal, all of you for

doing a very good job in a short window of time. So let's bring back up the main slides and go to the next one.

Okay, looks like drafting team 6 is up. And I was the coordinator for this one. And you can see the names of the participants on the team. And it was a great team, I really compliment and thank the participants. Let's see how many of them are in the room. So those of you who are here, raise your hand and leave them up for a little bit so we're going to turn it over to – is Griffin the only – oh here we go, okay good.

So Paul, and Roger, Vicky – Vicky was real key participant in this, she helped us a lot but she couldn't be here in person. She may be online. And Farzaneh – where's – Farzaneh stepped out it looks like. So hopefully she'll be back because she had some input after the document was finalized.

And I'd like her to share that directly if she will. And then Juan also – everybody participated in the group so it was a good broad participation. But I'm going to turn it over to Griffin to go over this one. So could we bring up the document?

And by the way, while they're doing that, all of the documents are on the working group wiki site and so you can read them in full detail on your own and even pull them up now if you want. But they're all there. So, Griffin, it's all yours.

Griffin Barnett: Thanks, Chuck. And yes, I agree, we had a good group, a lot of active participation from everyone. I just want to preface this by saying, you know, there's probably some overlap here, like we've seen in some of the other groups, between this purpose or use and potentially some of the others, but we were kind of drafting sort of in a vacuum, so we didn't necessarily have the benefit of seeing kind of what the other drafting teams were working on.

So okay so to quickly define sort of what legal actions use or purpose of RDS, so again, includes assisting certain parties or legal representatives or agents to investigate, enforce civil and criminal laws, protect recognized legal rights, address online abuse or contractual compliance matters or assist parties defending their interests in connection with these kinds of legal actions.

And, you know, we had tried to create sort of a illustrative list of examples of what each of these kind of subsets of this purpose would include. You know, and it includes sort of all stages of a legal action related process, so that would include sort of initial investigation, trying to contact the parties involved and then, you know, pursing, you know, sort of formal legal action, again in a civil or potentially a criminal context.

And as far as the tasks, again, you know, this kind of includes identifying registrant contact information for potential legal action, includes things like reverse Whois or Whowas type queries to look at, you know, who might have owned a domain name in the past or to collect information about additional domain names that might be owned by, you know, particular registrant.

And also to identify other registration authorities who might be necessary to contact in a legal action type context, so registrar, registry, hosting provider, things like that.

So, you know, again we try to identify the various individuals or entities that might be involved in this purpose so that might include people who were the victim of a harm. So for example I think in our minds in this respect was things like, you know, some third party registered a domain name fraudulently using another person's, you know, name or identity and so this would be a way of finding out more about that issue for the person who was harmed there.

Again, this would include people like intellectual property owners to investigate and enforce IP rights or infringing activity as alleged or is thought to be occurring. This might include operational security, anti abuse, domain reputational professionals who were investigating or responding to potential DNS abuse as well as escalating those types of abuse cases to potentially civil or criminal law enforcement agents.

Non law enforcement agent governmental agencies who have, you know, responsibilities for enforcing civil violations of law so that would include things potentially like, you know, in certain cases like tax evasion or consumer protection type issues.

And then again we have actual governmental law enforcement agents, prosecutors, other governmental actors who investigate and enforce potential criminal activity. You know, and again that would be things like cybercrimes, money laundering, really any type of criminal investigation where you know, you're just collecting information and this might be a resource.

And again, as I mentioned at the beginning, this would also potentially include, you know, the – on the flip side of the investigative aspect, the actual party who's the owner of the domain name who might need to defend against a claim.

I won't go into too much detail on the data involved here. Again, it covers a lot of the different data elements that might be necessary to serve this purpose. And then we have an annex to our document here that also provides a little bit more detail on, you know, each of the envisioned tasks and kind of describing in more detail what each of those kind of means. And again, like in other groups, we kind of started with the EWG report a - our initial kind of basis and then tried to flesh things out from there.

So I'll stop there.

Chuck Gomes:     Thank you very much, Griffin. And again, thanks to each of the team
                 members that most of them participated in all three meetings that we held,
                 teleconference calls, over two week – less than a two week period, and then
                 lots of work on email and lots of drafting, so the team really did a great job.
                 So let me open it up for questions about this particular – again it's a proposed
                 purpose, legal actions. Okay. And see what questions you have in terms of –
                 to help you understand what this proposed purpose is.

                 Michele and then Milton will go next.

Michele Neylon:  Thanks. Michele for the record. I think just to save us from having our heads
                 explode, rather than using the term "purpose" can we just look to say "use
                 case" for now because we say purpose…

Chuck Gomes:     I think that's a good idea.

Michele Neylon:  …my head's going to explode.

Chuck Gomes:     I should be doing that as well. I did it a couple times earlier but it's good, it's a
                 good point that came out here that will help us I think in the future. Milton, go
                 ahead.

Milton Mueller:  Yes, but that totally spoils my next question, so Griffin…

Michele Neylon:  I like to preempt you, Milton.

Milton Mueller:  If indeed the purpose of legal action is to facilitate legal action, or the purpose
                 of Whois is to facilitate – you're an American citizen, right? So do you think
                 you should put your social security number in when you register a domain?
                 Wouldn't that facilitate legal action?

Griffin Barnett: I mean, potentially but that's not a data element that we looked at.

Milton Mueller:     What's that?

Griffin Barnett:     That's not a data element that we considered, I mean, it's not part of the current RDS system so we didn't…

Milton Mueller:     But why not? If the purpose is to facilitate law enforcement…

((Crosstalk))

Chuck Gomes:     Okay. Let me jump – this is Chuck so let me jump in here. Again, we're not at the stage of deciding whether this is a legitimate purpose. And what the question you asked, Milton, goes to the question is it a legitimate purpose? We will get there, we're going to have to debate that. And we will. Let's make sure we understand the purpose today – use case, sorry. I'll do it – I'll probably make that mistake again, because we've been working with using that term for a long time and I understand the distinction. So all right, any other questions about – anyone that doesn't understand this particular proposed use case for RDS data? Check in. Don't see any hands up, any questions.

Okay, Maxim, go ahead.

Maxim Alzoba:     Maxim Alzoba for the record. Actually the use case is well – I well understand this use case, but there are things which might be not so simple like, yes, security investigation companies, cyber security investigation companies, formerly if they do not have local recognition with the, yes, country agencies of sorts, for example Company A is allowed by police of some particular country to run an investigation or to assist them, then they have local recognition.

And if they go to some other country, you're a third party. And they don't have like exempts from data protection laws of this country. So most probably this use case is not going to be I'd say valid in all – in all situations. So I agree

with the, yes, law enforcement may receive – yes, obtain an access to data elements, because they act under some law and, yes, they have valid reason or maybe court order which demands to disclose some particular information, yes, court order which demands it from registry or registrant, it's similar to local law enforcement.

But if the recognition of cyber security company is not in the place at some country, actually these provisions are in Registrar Accreditation Agreement, if you read things say in that only the companies which have recognition in this particular country. And the requests from those companies are valid. Thanks.

Chuck Gomes:     Thank you, Maxim. Any other questions, comments, input on this particular use case? Okay, let's see – raise hands if you think you have a reasonable understanding of what this particular use case is about. Not too many hands that time, sure there are no more questions?

((Crosstalk))

Chuck Gomes:     What's that, Milton? I didn't hear that.

((Crosstalk))

Chuck Gomes:     Yes, okay, well you'll be happy to hear then that it's just about time for our morning break. And hopefully it's set up outside. I look – I can't see past the people sitting on that side whether there's still stuff in here, but there is I think up towards registration out in the big hallway is refreshments and coffee and so forth, so take advantage of that. Let's try and be back here by 10:30 and we'll resume discussion of these use cases. Thank you.

END