

**ICANN Transcription – Abu Dhabi
GNSO- Next-Generation Registration Directory Services (RDS) to replace WHOIS
Policy Development Process Working Group Meeting
Wednesday, 01 November 2017 16:00 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, but should not be treated as an authoritative record.

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

Chuck Gomes: Okay, we're going to start now. The recording is already going so we don't need to do anything in that regard. My name is Chuck Gomes, if you don't know me, and I'm the Chair of this working group, the RDS PDP Working Group. Again, if there are any working group members behind me, there's still some seats available at the table; I would encourage you to sit at the table if you're willing.

The – is the agenda in Adobe? I don't see it in Adobe.

Lisa Phifer: It is. It's in the bottom right section.

Chuck Gomes: Okay. So let's go ahead and get going. The first thing we want to ask, as always, is there any working group member that has updated their statement of interest and you want to alert the team to that? Okay, not seeing any hands in Adobe or otherwise, we'll assume not. The – and you are controlling the slides? So I can just – so ahead and move to the next slide. We're going

to do a very brief, a really brief up to date of what we did Saturday because today's session is a continuation of our face to face meeting on Saturday here in Abu Dhabi and for those dialing in.

Let me welcome not only the members who are here and online but observers to the working group and guests today. And this meeting is open to anyone to participate. We don't have an – a standing mic so what we'll ask you to do is find a space at the table with a mic if you'd like to participate and you're not at the table already.

So very quickly, let me – well certainly introduce Lisa as part of our leadership team and from ICANN, those that have been in the working group know what the great support we get from Lisa. Now Marika also from ICANN staff, Michele and Susan, our two vice chairs that are here, David could not be here, will be in – I don't know if he's online but Marika, Michele, and Susan will be late because they're in the administrative session for the new Council that was just seated, or probably has already been seated in that meeting. They will come here as soon as that meeting is over.

The first thing I want to do, go ahead and go to – do we have a separate slide for 1? I think we do. As many times as I looked that I should know. So as far as introductions, are there any working group members here that were not in the meeting on Saturday? I'd like you to just introduce yourself if you weren't there on Saturday. If you did it on Saturday I'm not going to ask you to do it again. Any – please, use the mic and remember, any time you speak for the recording and the transcript please give your name.

Tomslin Samme-Nlar: All right, my name is Tomslin Samme-Nlar, I'm from Cameroon. And I just am a pretty new member of the working group.

Chuck Gomes: Welcome, Tomslin. We're glad to have you.

Tomslin Samme-Nlar: Thank you.

Chuck Gomes: And encourage you, even though you're new, feel free to jump in to ask questions. We're not going to back up a lot and cover old ground but we'll be as helpful as we can. And some of that we can do offline too.

Werner, go ahead.

Werner Staub: Yes, Werner Staub from Core Association and wasn't here on Saturday either.

Chuck Gomes: Thank you, Werner. Anybody else that didn't introduce themselves? Okay.

Erica Varlese: I'm Erica Varlese from dotBlog and I wasn't here Saturday but here now.

Chuck Gomes: Thank you, Erica.

David Peale: David Peale from DNS Africa, also wasn't here on Saturday.

Chuck Gomes: Great. Anyone else? Any other working group members? We're not going to do the whole room because – yes, please.

Alan Woods: Alan Woods from Donuts Registry.

Chuck Gomes: Thanks, Alan. Okay, any others? It looks like the Council finished its administrative meeting. Welcome, Susan. All right, now the slide that's up right now, I'm just going to talk about one thing on it. You can read it all however you like, but I want you to look at the last balloon. It's right now we're targeting March of next year to start working on our first initial report. We're going to do two initial reports in Phase 1, okay, and we had originally targeted right now for that; we didn't succeed at doing that. So we're now targeting that for March.

Let's go to the next slide please. Okay, and again, I'm going to spend very little time on this. In Phase 1, which is developing requirements for an RDS system, there – the first five of 11 questions are in those top five boxes. And then of course after we develop requirements for those five areas, we have to answer the fundamental question whether a new system is needed for RDS or whether the existing one can be adjusted to do that.

Today, all we're going to focus on is that top left blue box, users and purposes, and in particular purposes. Okay? And I'll qualify that more later but that's where we're at now. Now the working group has done some work on registration data elements, on privacy. We haven't done anything in data accuracy yet. And we've done a little bit on gated access. But we'll be doing more work on all of those areas, but today's focus is on purposes. Let's go to the next slide.

Okay, and the next slide after that. So agenda Item 3 is the goals for this meeting. And we covered this on Saturday, I'll let you look through it, I'm not going to read through the whole thing. I want to call attention to the second main bullet. Our goal in this session, as it was on Saturday, is to improve our understanding of each of nine purposes that were proposed in the Expert Working Group report. And we'll see a little bit more of those. We covered five of those on Saturday, all of them, there seemed to be good understanding except for one and we can talk about that a little bit later.

And so today we're going to look at the other four and get a – before that get a very brief update on – from a couple of the teams that have continued their work based on what happened on Saturday. Next slide please.

Okay, so the – did I say that wrong? Did we cover only four on Saturday? How come there's five here.

Lisa Phifer: Four teams.

Chuck Gomes: Oh that's right, okay. Four team – yes, so we formed seven teams, okay, to do this work. Two of the teams had two of the purposes and these are the purposes that are going to be covered today, so domain name control, Drafting Team 2; domain name certification, Team 3; legal actions, Team 6 and then the last two, regulatory or contractual enforcement and individual Internet use will be Teams 5 and Teams 2.

Go and go to the next slide.

Lisa Phifer: These were the ones covered Saturday.

Chuck Gomes: Oh I'm sorry. If I'd read the title, I would have got that. You won't believe that I actually have looked at this presentation a half a dozen times so maybe that's my problem. So these are the – that's why I was confused on my first point.

So these are the five we covered Saturday. Now, based on just an informal assessment of the people that were in the meeting on Saturday, there seemed to be pretty good understanding of the – of the purpose documents that four out of five of these covered. The one that was a little less level of understanding was regulatory or contractual enforcement and you'll hear what's happened on that as well as legal actions in just a moment.

Next slide.

Lisa Phifer: Did you want to ask (unintelligible).

Chuck Gomes: Oh, I can do that, sure. But let me go ahead and ask if any of the teams want to give a two to three minute update and see if you have any questions of the people in the room. And while you're thinking about that, let's get an update on legal actions and on regulatory or contractual enforcement. So let's start with legal actions. And Griffin is going to give us an update there. And a lot of activity has been happening since Saturday.

Griffin Barnett: Yes, thanks, Chuck. This is Griffin Barnett for the record. Yes, so since Saturday on the legal actions purpose basically all we did was we met informally as the drafting team on I guess Sunday morning was it, Monday morning, anyway, one of the days right after the working group met on Saturday.

And we basically agreed to make two specific changes to our drafting team document. The first was to amend and streamline the purpose definitions so we basically took a lengthier definition that was a few sentences long and included some illustrative examples of various aspects of the purpose and basically condensed it down into kind of a streamlined single sentence format. And we took out some of the illustrative examples so it was a little bit more high level.

And then in the body of the document we had an Annex A that described the purpose and various tasks associated with the purpose in a bit more detail, and what we did there was we basically added one additional illustrative example that had kind of unintentionally been omitted in the first draft. And that example was related to suppressing political speech and things of that nature. That was an example that was suggested by one of the drafting team members, so those are the two changes that we made after discussions on – in our informal meeting after Saturday.

Chuck Gomes: Better use the mic. This is Chuck. Now, does anybody else from that team – Team 6 – want to add anything? Or does anybody have a question? Now you're all going to see the final documents probably the end of next week. We'll talk about that towards the end of the meeting. But anyone? Okay, all right, very good. Thank you very much, Griffin.

Let's go to Team 5 and is (Chris) here?

((Crosstalk))

Chuck Gomes: Oh you've got to come up to a mic. Come right up here. You can use this one. So (Chris) is going to just give a two or three minute update in terms of what's been happening – and again, a lot of has been happening on this particular team. Go ahead, (Chris).

(Chris): Thanks, Chuck. From what we had as meeting on Saturday, obviously we've taken note of the various recommendations that has gone around. One of the things that we – when we were looking at the document that we decided that – to break regulatory and contractual enforcement in two different documents. When we were looking at the regulatory part, it actually there was some overlap into legal actions, which we thought at some point in time we might have to collaborate closely because it has that impact. And so we've also done this more or less the same thing, we streamlined most of, yes, the description, so that people can understand it, so it's like two line so people should be able to do that.

We also looked at the various aspects that was in the document so it's completely streamlined. I'm pretty sure it will be more reasonable for people to actually read those documents. And obviously the whole exercise behind it is for everybody to be on the same line on the same page. We're nearly there, we just need the other team members to just formalize whatever is needed, and I think by the 10th of November, was it, to actually push for, whatever, well there will be a date, we'll get the document out and we actually hope that, you know, other team members and members of the working group would actually have a look at the documents and obviously give us the go-ahead whether there's anything there, any questions that needs to be looked at.

And as I said, regulatory comes very close to the legal actions. Me and Chuck had actually had a look at that and we think that's something that we need to be working closely and that might make more sense to a lot of people actually because the regulatory has an impact on law enforcement so that's how we're looking at it. And the second part when we're talking contractual

enforcement obviously we're talking about the ICANN, the registrars, the registries, and obviously the registrants. So they don't actually match there, that's the – or actually we moved it, we made it two documents. It might end being three, we don't know. But this is the – what we've been doing so far.

Chuck Gomes: Thanks, (Chris). Anybody else from Drafting Team 6 – excuse me – Drafting Team 5 – want to add anything or ask any questions? While you're thinking about that, and by the way this is Chuck speaking, I've got to remember to identify myself as well. The whole working group will get a chance to see these final documents, and we'll do another assessment to make sure there's good understanding. The goal being understanding at this stage.

We're not talking at all about whether any of us think these are legitimate purposes, let's make sure we understand that we're all on the same page like (Chris) said. And that's what this exercise is about.

Now let me open it up to the other three purposes to see if there are any updates. And I notice that David Cake, who's the coordinator, and one of our vice chairs, is online. So, David, if you have any update; if you don't that's fine, don't worry about it, it wasn't necessarily expected. And Susan, the same thing, on the two you cover, do you have any updates? Okay. And again that's okay, that's not a criticism.

I was pushing the two teams I was coordinating mainly because I'm going to be out of the loop starting the end of next week so we're – I'm trying to not dump too much on my colleagues on the leadership team. So we got a little head start. And then I think that covers the teams.

So all right, let's go to the next slide please. So now we're going to continue – and this is Agenda Item 4, with the purposes that we didn't cover last time. And we're going to change the order again here so go ahead – go to the next slide. Now we're going to skip one mainly because Rod has limited time so – and he has joined us earlier than we expected and that's absolutely no

problem, in fact the timing is quite good, real easy to adjust. So Rod's going to give an overview of the criminal investigation, DNS abuse mitigation purpose. And I'll turn it over to you, Rod.

Rod Rasmussen: Great. Thank you, Chuck. This is Rod Rasmussen. We had some slides...

((Crosstalk))

Rod Rasmussen: Excuse me?

Lisa Phifer: (Unintelligible).

Rod Rasmussen: Oh, okay. I frankly don't remember who all is on my team. Oh there they are, Richard Leaning, Marc Anderson, Kiran Malancharuvil, hopefully I got that right, Ayden Ferdline, myself and Raoul Plommer. And I'm not sure who all is in the room.

Chuck Gomes: Yes, let's find out who's in the room. If you're one of those people raise your hand. Okay, anybody behind me? We still have a couple seats at the table for any working group member so please move up if you can. Rod, back to you.

Rod Rasmussen: Okay. So, yes, if you could put the slides up that I tossed over? We're doing this all in real time, it came in like an hour ago.

Chuck Gomes: While they're doing that, let me say I think anybody that's been to an ICANN meeting know this is a terrible time to have to keep working on other stuff, because we're all booked solid and so forth. So if you haven't been to an ICANN meeting you may think that there's lack of preparation, it's just that everybody is so busy this week that it's really hard, so no problem at all on that, Rod. Go ahead.

Rod Rasmussen: Okay, so we just for logistics purposes we turned in our first draft I believe round four, five, six days ago, something like, I don't remember when exactly

we turned it in for the group to be able to look at the first draft, and then we made some edits actually live up until today and I think and much credit to Marika for formatting a bunch of stuff to give a little more – a lot more presentable than the drafters had – mainly me – drafter – I'll take full responsibility for any illegibility or questions within that bit.

And we had a couple of meetings and got feedback on the documents and the purposes and various things that we had put in there. So I think this is fairly well representative at least to flesh out as much as we could. And you could write a probably 100-page paper on this easily. I think ours is 15 so. So if we could – we have a slide deck, that's much easier to digest.

So these are lifted from – directly from the document to try and get some definition around the various categories of things that could fall into the rather broad topics base that we're talking about. So everything from looking at criminal investigations to the various types of abuse prevention, incident response, which is real time and over time, and then network protections and things like that. So a wide range of things from kind of what you would think of, you know, criminal investigation, cops and robbers, you know, hackers, people need to find them too, just mundane things that happen all the time in that highly automated fashion.

Chuck, you have a question?

Chuck Gomes: Are you – this is Chuck – are you comfortable with questions being asked as we go?

Rod Rasmussen: Sure. What I was going to say if – this is kind of sets the tone for it...

Chuck Gomes: You let me know when you're comfortable with that...

Rod Rasmussen: Okay.

Chuck Gomes: And then let me add one more thing. So the way this is going to be run is our goal, remember, is to ensure understanding and at the end of this session I'm going to ask does – is there anybody that doesn't understand or do you have other questions. So what we'd like to happen as soon as Rod is ready for this, and he can judge that better than me, we're going to – we want everyone, if there's something you don't understand ask questions and that will not only help you, it'll help everybody in the room in terms of understanding this proposed purpose, okay? Back to you.

Rod Rasmussen: Thanks, Chuck, for that. And this is Rod Rasmussen again. And this was actually – I found this to be useful in our group as well because we had a couple of pretty deep subject matter experts and a lot of people who – this was a learning experience for them and it was actually really good to have people ask questions about what do you mean by this and the like, so that's – from that perspective it was quite nice to have some people who hadn't been exposed to try and do it.

That said, it still may be opaque to some. So and let me give you an idea of this presentation here so there's appropriate place we can pause for questions. What I've done here is tried to give you a broad overview to give you an idea what we're talking about and then a framework within that to kind of – to frame your thinking about how – who, how, why there are.

And then, and drilled into specific use case areas that we've put in the document that is not comprehensive so it's not every particular think that you could do, but what it was supposed to be was illustrative of the various types of things so that would tease out the data elements at least that you would be looking for and reasons for them. There's a lot of overlap in the type of thing that you might be investigating or responding to and the way you respond to it and the way you need to access data to do so that are very repetitive but they may be for a different type of abuse, right?

So for example if I'm looking up something for phishing versus something for malware, it's pretty much – well pretty much the same steps in the process. So those have been kind of lumped together.

And we listed here, you know, again, non comprehensive, different types of activities that might be in here, everything from, you know, kind of run of the mill spam up to, you know, very serious crimes can be put in these categories. We can go to the – well before I go here, any question on just the broad area that I've got defined here because there will be more specifics coming, I just want to make sure we're – okay.

So let me move onto the next slide please, the one that says Users there. Thank you. So this is again, a non comprehensive listing of typical actors and that will be making queries to – we're assuming there's data in the system for this. And this was actually an important point in these investigatory types of things. This is not something where people are putting data into the system for say ownership of a domain or something like that where you – you as the actor would be a registrant, this is people needing to get a hold of data for some reason, is pretty much an exclusive construct for this type of use case.

But, you know, as you might imagine, various types of law enforcement, cyber security professionals, breaking up IT administrators separate from cyber security personnel because a lot of people in IT have to deal with all kinds of stuff coming at them, and they don't know what's going on and not trained in cyber security but they do know they need to – they've got some network or some domain that's broken and they need – and is doing something that looks like an attack and it may very well be an attack because for example in the DDoS, denial – the distributed denial of service attack, and so they're not necessarily your – if you think of the – kind of the anti-hacker types, you know, that's not what we're talking about, it's just somebody have to protect their own networks.

And then not just people but things, automated processing systems. And frankly that's what we all rely on far more than people are computers and servers and things like that, the firewalls and all those kinds of devices rely – do most of the protection that we have from spam, from denial of service attacks, all these things that otherwise would grind the Internet to a halt. So and then, you know, kind of the catch all, there's other people who are looking into abuse from academic researchers to individuals trying to figure who's spamming them, things like that that may end up looking up information around a domain name in order to do that.

Okay, any question on the users?

Chuck Gomes: While we're waiting for that, does anyone need more clarification on any of these categories? You pretty clear on what those are? Beth.

Beth Bacon: I apologize if you've said this and I missed it. So in your definition you say avoiding abuse or combating abuse and there's abuse issues, I'm sorry, am I not – I sound really loud in my head, I apologize, I'm a little sick. You say abuse issues and then in your definition you say combating abuse, how are you defining abuse in this?

Rod Rasmussen: Yes, there was within the definition there's a whole bunch of different types and there was examples and it can be anything from spam and you know, if you want to – yes, there you go, there's a whole bunch of different things there on that second paragraph. And that's not a comprehensive list, it was not intended to be – I could probably fill up a you know, 30 pages of PowerPoint with various types of activities that we might be talking about, but the idea was to get something that covered the spectrum and also the types of things that might be different and how you pursue them, that was kind of the objective here.

At least that's the objective we did because in two weeks there wasn't the time to list everything. And even on the EWG we didn't list everything, there's just – even with all the time we took on things.

Okay, could I go on two slides now? Tasks, so – and I want to emphasize that first point, it's even got an exclamation point, it depends on the circumstances what you do. I think there's a lot of perception that people who are doing anti abuse or law enforcement are accessing the Whois to find out who a registrant is so they can do something to them. And that is one of the things but it's actually I would say the minority case in this particular area mainly because of automation and other things that don't – you don't even care about that stuff. So it really is dependent upon the use case. So I just want to emphasize that.

But some of the things you may do is contact a domain owner or many, many cases just the entities that are responsible or a domain, whether that's, you know, from the technical side of it, or what have you. And there are different things that you may want to do. You might want to fix a problem that is on, you know, their Website has been compromised and has malware on it and it is affecting you, you want to let them know about that. You may want to talk to them about do they have logs of access to their domain or the website or their email, things like that, that might help in an investigation.

And of course you want, as I mentioned, notify them of compromises, but problems can be all sorts of different kinds of problems that end up being on the abusive side. Another thing you might want to do is expand – take a starting point, if you will, and expand that based on used this infrastructure or this person or entity is tied to this domain name, what else are they tied to?

And so often this is an infrastructure kind of thing where you're looking at name servers and what else might be tied to it, or how things are registered, could be things a reseller or a registrar, things like that where you're actually trying to expand and understand, okay, I've got these domains that are

involved with say this botnet, oftentimes there's many, many more and you want to understand what that looks like so you can – you can call that evidence gathering but it's also understanding the scope of the problem because you may not be a criminal investigator, you may be trying to add things to a block list and want to get that information which kind of gets me to the next one is identifying infrastructure itself.

So if I have a domain name that I believe is registered as a command and control server for example, for a botnet, I will take a look at things like the name server and how it's registered and the like, that might include contact data and the like that people reuse. And again, that could be real data or it could be fake data, what matters is the same data. And I can take a look at that and say, okay, I've identified that these things are being used and then I can do associations on that to figure out what, you know, what I need to block or react to or notify on.

And that gets to the next point which is I put these into endpoint systems, network protection systems and the like to – so think of your antivirus product, your anti spam product that may be on your laptop versus there's anti spam software that's sitting in an ISP to network firewalls at your corporate headquarters, things like that. This kind of information gets put into that, so the action from understanding the data you've taken in around an incident or incident that you've expanded may not end up in a notification, it may very well just end up as a protection mechanism for curtailing abuse that's hitting your network or your customers or what have you.

Then one of the things that does happen is requests for suspensions of domain names or transfers or things like that in some cases, but somebody has registered a domain name to do something evil so it's (evil) is one of the purposes from before, and – but that's the exclusive thing that that domain is for, right, this is very important is the – to know the difference and which is why one of the first things you do is actually determine whether it's malicious or not right?

And if you determine that that domain name is the only reason it's therefore then you would make a suspension request. So those are the kinds – and again, non comprehensive, list of types of actions that you may take based on gathering data around your investigation or your anti abuse thing. And I'll stop for questions here before I go onto the kind of – the forward stuff...

((Crosstalk))

Chuck Gomes: So this is Chuck. Now here's your opportunity, if there's any of these tasks – now keep in mind what we're talking about is using what we know today as Whois data, in the future it'll be called the RDS data, we're using that term already. But any of these that you don't understand as possible tasks for us in registration data with regard to this particular purpose? Okay, go ahead, Rod.

Rod Rasmussen: Cool, and by the way, after you take a look at the paper, I pulled these out of it, it's not – it's not in the PowerPoint, not every word in the paper is in the PowerPoint. I did do that, I mean, I hope you appreciate that. But if you think there's something missing because again, this has been put together in just a couple of weeks, that would be great feedback to get.

If we could move to the next slide? So one of the things I think it's important to understand about the kinds of actors and a way to kind of put a framework around various types of use cases and purposes is to understand kind of the flow, the process flow, and the kinds of actors you have. So the first category of actors here are individual people or small teams, where you think of your cop or your cyber crime investigator, what have you, has got something that is – they've reverse engineered malware or they've gotten an abuse complaint, what have you, so they're going to turn to start investigating and they'll do a look up of information, right, so they'll hit the RDS, Whois, whatever we're going to call it. I will call it RDS.

And they're going to get information about that particular domain name or small set of domain names. And that's something that happens over and over and over again. There's hundreds of thousands of people in the world that do that on a daily basis, probably around that scale. And they – so let's say there's millions of requests per day, tens of millions of requests for day, for this kind of thing.

Let me give you a scaling. They will typically do deep dives, right, on this, that information will be fairly rich because they may be looking for something in particular. The other side of this is the automated processes, and in this case there may be, you know, tens of millions, hundreds of millions, billions of requests for lightweight data, right, so a lot of the Whois information or RDS information that you would make decisions around would be things like let's say the registrar or the domain registration date so if it's something that was freshly registered you may treat something differently in say anti spam flow than something that's been registered for 10 years, things like that.

But if you think about that as these automated processes that need a little bit of data to help make decisions around real time protection mechanisms, that's a totally different thought and use case than I'm going to grab as much information as I can because I've got this criminal case I'm trying to do, right, so there's this – there's shallow and wide and deep and narrow, okay. That's – and I think that's a useful framing, now you guys may not think it's useful at all, but I think it's actually a useful way of trying to help understand the – just the wide variety of different kinds of uses we're talking about in this category.

So I'll stop here for questions on that kind of framework if anybody has any questions on that.

Chuck Gomes: Chuck again. And let me encourage members of the team to jump in in these pause times as well. I didn't say this at the beginning, I think we said it on Saturday, but these teams were intentionally structured to include people who were novices to the purpose and those who were experts so that they would

kind of mimic what we wanted to happen in the full working group where those who don't understand will ask questions and those who are the experts and have been involved in this can help us all understand. So time for questions on the categories of actors or anybody from the team want to jump in. Okay. All right.

((Crosstalk))

Chuck Gomes: Yes, oh sure.

Lisa Phifer: Lisa Phifer for the record. Rod, one of the things that we talked about on Saturday's session, which I know you weren't able to attend, was trying to determine when we have more than one purpose sort of lumped into the same purpose. And I'm wondering because you have very different kinds of users potentially needing different volumes of data if you think this might be two purposes?

Rod Rasmussen: Far more than two purposes probably. I put this here as a way of potentially – if you're thinking about putting together a matrix of purposes, of naturally dividing them up this way just from a thinking process and a description process. Because if you can categorize those together I think you can – you know, the example I gave before, phishing versus malware, do we you know, and I don't know what the legal side of that would look like. But, I mean, you're basically doing the same kind of thing so if you can label that as cyber crime or something like that and have that same flow, then potentially you could bundle purposes and because it's just a matter of semantics and language.

However, if you can't, then you need categories to put those into so that's why I wanted to propose this a framework for dividing these kinds of purposes up.

Chuck Gomes: This is Chuck. Thanks, Rod. And one of the things – and those that were there Saturday know that each of the teams are just going to have little bit more work to do in the next week and a half. But that you might want to focus on as a team is would it be beneficial in term – keep in mind what the working group is going to do in the next few weeks once we have a good understanding of all the things, we're going to start talking about which ones are legitimate.

So think about how would it make it easiest for the working group to deliberate on these things? And feel free to come back with a breakup, what came out of the discussion on regulatory and contractual enforcement it – a really good output of the discussion on Saturday was those should be separated, it would be useful. And so that has no happened, the team has gone back and as (Chris) shared, we're even thinking that maybe the regulatory would fit in the contractual actions. So feel free as a team to come back with any recommendations in the regard that you think would help the whole working group as we proceed beyond understanding and start deliberating on whether it's a legitimate purpose and so forth. Okay?

((Crosstalk))

Rod Rasmussen: Thanks, Chuck. This is Rod again. Okay, so one of the...

Chuck Gomes: Hold on, Rod.

Rod Rasmussen: Oh sorry.

Chuck Gomes: We've got more discussion this time. Michele, go ahead.

Michele Neylon: Thanks. Michele for the record. One of the things that came out of our conversations at the last meeting which was several months ago, or was that Wednesday, or Thursday of last week, I honestly don't know, it was at some point in the last few days – I'm on ICANN time, I have no idea – we started off

referring to these two purposes and as somebody pointed out, that's wrong, they're not purposes. They might be your purposes, but they're not the purposes of what's going on here; these are use cases really that we're talking about.

Now eventually they might evolve to a point and condense down to something where we can sort of say okay, this is a list of purposes but we're not quite there yet, we're still- we want to kind of look at evolving further. So just – it's just more in terms of the terminology. Now of course Rod and I can have a healthy disagreement about this now, or we can schedule that for later.

Rod Rasmussen: I'll schedule it over beers, Michele.

Chuck Gomes: So Chuck intervening again. I think ultimately to comply, for example, with GDPR, and this is much bigger than that, we're going to have be very explicit on what a purpose is versus a use case. But the use cases can be very helpful in helping us understand, so please, there's no criticism about talking about use cases. And Michele didn't mean it that way either.

Michele Neylon: You're trying to interpret my words?

Chuck Gomes: But I did it right, didn't I?

Michele Neylon: Maybe, we'll see.

Chuck Gomes: He doesn't like to admit to that. So we do have some fun in this working group if you can believe that, okay? So go ahead, Rod.

Rod Rasmussen: Sure. And I will note that throughout the document we used "use case" extensively so and I did see that as well. And I think one of the ideas here was to subdivide purposes and would have exemplary use cases. And we'll worry about getting the semantics and the wording right. But the main thing

was what are people doing? Right, and that's what matters, and why and who and how.

The other thing I will – which is – the way the document is laid out is this framework here is actually there's two sections, one on auto – one on manual, one on automation and then within that there's some sub actions so it's actually already organized this way so it made it really easy to cut and paste on the presentation.

Can we get the next slide? All right, okay so these are categories of types of actions. And there's really three things you – that come as the things you always are doing or are part of the process here. And the first one there is using this information to determine if – the nature of the domain registration itself. Is it malicious or is it just a compromise, right?

And you use all kinds of information, not just RDS data, that's all kinds of touch points you have in order to figure out whether or not something is – has been put there, put in the system, registered to do some sort of harm that we've identified as these types of different abuses and crimes. So that's one of the things you access the RDS data for is to take a look at things like when was it registered, was it registered by somebody we've been tracing as having serial registrations, was it registered at a registrar that has a really bad reputation for registering. There are all these factors that go in trying to determine that.

Next thing is then based on information that you may have from figuring this out, you may do a notification. And notification could be to somebody whose Website has been compromised or their email has been hijacked, hey, your domain had its Website hijacked, right, or compromised or what have you. So – or to the technical contact that's responsible for that domain, might want to let them know that. Or if they've got a problem with their DNS to their DNS provider.

Or, if you find that it's malicious you may want to notify the registrar itself that, hey, you've got a bad guy has registered the thing and, by the way, that credit card that they sent to you probably is not – it's probably stole and will be a charge back, things like that.

And then I mentioned this before, and I don't want to dig into it again because I explained it fairly earlier, which is taking a starting point and trying to understand the scope and scale of a particular attack, campaign, etcetera. So if you think of those cool charts that you see in the movies where you take your hands and you spider around into all the points draw together and stuff like that, well there's software that actually is like that and you can – except for the whole hand thing, but actually I've seen some in the FBI, they've got some cools stuff like that.

But you can actually do this kind of stuff and researchers do this all the time is they use these tools to link things and figure things out and cluster and all that stuff. So that's all really useful stuff. So those are kind of the broad categories, and there's lots of specific different kind of steps you do in here with different types of data but these – this is kind of a categorization, again, this is to help frame how you deal with use cases and the like. And I think would be helpful for as you were mentioning earlier, Chuck is to try and understand different ways of bundling together, rolling them up and/or saying well, this fits in and this may not, right. So and I'll pause here for any other feedback on that.

Chuck Gomes: Thank you very much. Thanks to the whole team, okay, for the work you've put into this. And the full document has been – it's a long way, by the way, compared...

((Crosstalk))

Rod Rasmussen: Wasn't quite done yet, Chuck.

Chuck Gomes: It was – was it 13 pages?

Rod Rasmussen: The – well no I wasn't quite done with the presentation yet.

Chuck Gomes: Oh okay, I'll let you finish.

Rod Rasmussen: Okay.

Chuck Gomes: But...

Rod Rasmussen: If I' out of time I could stop, that's fine.

((Crosstalk))

Chuck Gomes: But I want people to understand he is – and he's made this clear, that this isn't the full document, okay. But you all as working group members have it, so please take the time to look at that, that's important and they put a lot of work into this. Go ahead and continue.

Rod Rasmussen: If I could have the next slide because I do – I'm sensitive for time. There was – Michele, did you have a question?

Michele Neylon: I was just trying to – going to correct my learned friend, you keep – you referred to registrar a number of times where realistically speaking it's not the registrar you're looking for at all, it's the hosting provider.

Rod Rasmussen: Yes, if I have a compromised Website, I'd contact the hosting provider or a technical contact or some sort or what have you.

Michele Neylon: Yes, no...

((Crosstalk))

Rod Rasmussen: I wasn't – yes.

Michele Neylon: It's just, no, because the thing is in this environment people have an awful habit of going oh, it's a problem with the domain, contact the registrant or the registrar. That's ridiculous and it's got to stop. The hosting providers – and this is not aimed at you, Rod, it might be aimed at Dick though, the hosting providers are not being pulled into this and they should be because a lot of them are not responsive. So what's ending up happening is that we're seeing a lot of these discussions around abuse mitigation, which is landing stuff at the registrar door. So in the case of a company such as our ourselves, we are both the hosting provider and a registrar, while we...

((Crosstalk))

Michele Neylon: Oh shut up. Last time I'm buying a coffee or a beer or any other liquid, besides to pour it on you.

Chuck Gomes: So do I need to get Herb involved here?

Michele Neylon: No, it's fine. We're big enough and ugly enough to sort this out between us. No, but, I mean, the thing is this, I mean, often you find cases where the domain is registered through ourselves, the Website might be hosted with, you know, Go Daddy, the, you know, there's a lot of different kind of splits and things like that across multiple networks, multiple providers. As a registrar, if the domain name is not hosted with us, what are my options? And Rod knows the answer.

My options are either turn it on or turn it off. And in the case of a compromised Website, that's not a very good option because that means that I will kill all services associated with the domain. Now just the reason I'm raising this is just because for people who are not aware of the ramifications of it. Rod and I both know that we both understand this, but, you know, just clearing – making sure people are clear about this thing. Thanks.

Rod Rasmussen: And thank you, Michele, actually for pointing that out because that's why the first step there is there, right, determine what kind of situation you're dealing with because Michele is the right person wearing his registrar hat if the domain has been registered maliciously. If he's – if you want to contact him wearing his web hosting hat that's because it's been compromised and – that might even be...

((Crosstalk))

Rod Rasmussen: What's that?

Michele Neylon: I obviously do have a split personality.

Rod Rasmussen: I don't think I've discovered them all yet. So can we get the next slide then real quick? There's- the next one – and this is kind of a catch all but there are other important things which aren't necessarily Internet crimes, so to speak, or Internet abuse issues where you may look up information around a domain name. So for example, if you're investigating say a murder or a series of thefts or something like that, as a law enforcement person, and you come across a blog that talks about some events that may be only the bad guy would have known about, you might want to know who actually that that as part of your investigation, that's, you know, a hypothetical yet real example, right, of the kinds of things.

But that has nothing to do with abuse on the Internet or e-crime or things like that, it has to do with standard old real world crime and somebody happens to have some sort of web presence, Internet presence, email, they might have their own email system set up, I have my own domain name for email, for example, that may show up somewhere that you would turn around usually as a police officer in this case, it might be a private investigator or something like that, but this is typically some – in the area of police.

And so that – you need to – in order to be comprehensive and talking about this category and you're talking about that. And then you might have infrastructure that's also affected by some incident somewhere else where you may need to give a notification or something like that, so that might be a victim of a DDoS attack. So for example, when you reverse engineer some DDoS bot you may see or they're attacking this particular Website, and so you would take that information about the domain name and maybe get a hole of that person because hey, if they're under DDoS probably their email and their Website is not working so you need to call them on the phone or something, right?

So that's a real world thing that happens all the time is somebody is getting attacked, they don't know what's going on and you want to give them information about the attack. So that's a case where it is on the Internet but it's not really – you're not really part of it per se. So that's why this is kind of the other touch points is just where this kind of stuff comes up in an investigation.

Chuck Gomes: Okay, Greg has a question.

Greg Aaron: Hi, Greg Aaron here. So I wanted to follow up something Michele said about hosting. Even when the problem is at the hosting provider, not with the domain name itself, one of the real life situations is that hosting providers don't like to talk to ordinary random people who are calling them. What they do like to do is talk with their customers who are the domain name owners, a registrant contact or an admin contact, or a technical contact, who's actually authorized to speak with them and get the problem resolved.

I've had cases where I call a hosting provider, they don't know who I am. I give them good information, tell them exactly what the problem is but I'm down in the queue. But if I can get the domain owner to call them, the problem gets resolved quickly.

Chuck Gomes: Thank you, Greg. Chuck speaking again. Go ahead and continue.

Rod Rasmussen: Okay, and I have – the remainder of the slides, I think there's like three more, are all about individual use cases. And I wanted to run through that quickly just so we can get that out of the way.

Chuck Gomes: Go ahead and go through all of them and then we'll open it up for...

((Crosstalk))

Rod Rasmussen: Yes, then we'll just open that up. Okay, so if you could move to the next slide. Think of these use cases would all fit within that framework of stuff I just went through, ok? And so here are some of the things to think about you know, as far as, you know, if you're doing – if you're that person and, you know, doing an investigation or something like that, these are things you might do, right, which is determine the status of the domain name, notify those parties that, you know, notify somebody that their Website has been compromised, notify them that their domain management account has been taken over.

This is something we have, you know, there's a lot of that kind of stuff going on, hijacking and things like that. You might notify the registrar if the domain name is malicious. Actually, you might notify the registrar too if there's an account that's been compromised too, that would be nice for them to know especially if there's a whole lot of accounts that have been compromised, that might indicate something wrong with their systems or, you know, somebody is doing some sort of, you know, brute force or something like that.

And then we've already talked about expanding knowledge. So I've already talked about these but this is a list here. And I just pulled these out from the – there's even more in the document on that. So you have the next slide.

Automated processes and I talked a bit about this, but you – some of you will use automation in some cases to try and determine what the status of a

domain is. You will – but typically that will be around creating some sort of reputation score so that I can do things for protecting against spam or protecting my network against attacks and things like that. That's what those reputation scores are typically used for. They're not used for evidence in an investigation, they're basically for network protection and making sure things still work.

There are some things you can do with automation around notifications of issues, so if I'm getting a lot of spam from you I can notify automatically to the technical contact, hey, you've got something going on here, things like that. And then you can use tools to basically take, you know, automatically take known things and expand them out. And I mentioned the kind of the stuff you do with the manual stuff, that's often fed by automated processes going out and harvesting data and bringing it back and organizing it for you so that you can look at those thousands of data points.

Could have the next slide. Okay, and this is last – this last one kind of ties as a solid use case to the one I mentioned earlier which is there's some real world crime and you've got a domain name that happened to come up in it and you want to go figure out how that – who is tied to that either the registrant or potentially the hosting company because you suspect that this person is using like a website for some personal stuff, you might want to call them – hosting company and get the customer information from them about that, right, and file a subpoena and what have you, that leads to lots of different processes.

And that was the last slide, so those use cases were there to kind of flesh out what those, you know, well they're there as the use cases and the categories what I wanted to concentrate on because those are the broader topic spaces where all these different uses, hundreds of different use cases that you can come up with all fit into and these exemplify them. And I will end there for questions on that or any of – did you want to chime in? Okay.

Marc Anderson: Thank you, Rod. This is Marc Anderson for the record. And, you know, first I have to start off by thanking Rod. He did the heavy lifting in our group and despite having a very busy schedule, pulled a lot of this together. So thank you, Rod. You know, and I also, you know, if you haven't read the document – the full document yet, I encourage you to do so. It was a really good experience for me. I learned some things I didn't know already. Particularly if you're looking at Slide 9, around automated processes, there's a – that was a very informative for me, there is a lot there I didn't know about and so I really appreciate the exercise of doing this.

Susan and Lisa, I know this was sort of an idea the two of you came up with and the purpose of that was to broaden everybody's knowledge and understanding of these EWG purposes and at least for our group I thought it was an excellent exercise for that and I learned a lot going through this. So thank you. And thank you for Rod.

Chuck Gomes: (Chris).

(Chris): Thanks, Chuck. (Chris) for the record. I'm starting to believe that what my good friend is actually doing there actually ties into the legal and the regulatory process in both ends actually. I'm not saying that it's – it can be as well as independent, as interlinked into these areas that our two teams have been working on. Actually what is there actually would actually be on one side and on the other side as well. So when you're looking at the case scenarios you will be investigating and when it goes to the other end, where the action needs to be taken up obviously you know, so that – the way I'm looking at it I'm starting to see a kind of work flow in there. That's my personal perspective.

I think when we start to listen to everyone it will come to a point where once we get the workflow kind of thing in there, we might be able to see the whole thing together, that's what I wanted to actually mention. I see a connection there.

Chuck Gomes: Thanks, (Chris). This is Chuck again. And again, like I asked the team, keep in mind that – you know, seeing where there's overlap, we talked about that on Saturday, and the key is to end up with some documents that make it easy as possible for the working group to deliberate so feel free to come back with any recommendations in that regard.

Keep in mind that we won't avoid all duplication across these things, that's okay. But if there's serious duplication, and maybe it makes sense to combine them, that's okay too. But feel free to come back with those kind of recommendations.

Now, before I ask the measurement question in terms of the level of understanding, are there any other questions? Maxim.

Maxim Alzoba: Maxim Alzoba for the record. I think we need to understand that there is no such thing as like worldwide operating law enforcement, worldwide recognized. And it means that we might face a situation where we need something like 3D or more dimensional matrix of the who requests data, who requests whose data and, yes, even jurisdiction of registrar or registry might cause different accessibility or absence of accessibility to particular data. Because yes, law enforcement agencies are law enforcement agencies, but different countries have – and each country usually has its own opinion on how these law enforcement agencies are exempt from privacy protection laws because obviously without such thing they will not be able to operate at all because they will be not able to identify bad actors and even to, yes, to search through data of potential bad actors, because not all of them are bad, some of them might be proven bad, some not.

So we need to – from very beginning of design, to add at least notice that like relevant law enforcement because even in this GDPR thing, which, yes, is talked about a lot this week, GDPR doesn't recognize role of law enforcement in non EU countries. For example, some country it's outside of EU, its police

wants to access data of its citizens – or citizen particular on its territory where they have legal right to do so. So we have to...

Chuck Gomes: Thanks, Maxim. And we're going to have to get into that in more detail when we talk about users more specifically so we'll get there. Rod, go ahead.

Rod Rasmussen: Yes, Rod again. And he raises an interesting point, and these use cases are basically all data access use cases, right? And there's nothing here about putting data into the system. It assumes there's certain levels of data in the system, and these cases are based on what's currently in the system. There is a little bit in there about if you read the report there's what's in the traditional Whois system and we make some references to systems like Whois systems or if third parties that have that kind of data. We didn't talk about the legitimacy or anything, this is what actually people do, so this is – it gets into a little bit of the hypothetical slash future slash what have you on that.

I think though, that the – where we – no matter what if you're law enforcement it doesn't matter what country you're in, you're going to go through this process. There may be, at the – so these create the purposes or use cases that drive purposes in general and then within specific things you may have different access restrictions to different data that are beyond the reason for providing the access in the first place. So there's kind of two levels, right?

There's can anybody access this data at all for these purposes? And then there's the okay, who gets what, which is – that's the fine tuning of these cases, and I don't think we're at that level yet, but I do want to recognize that that is a legitimate area that we're going to have at least touch on. Thanks.

Chuck Gomes: Okay, thanks for the great work by this team. Now I'm going to ask you to let us know if there's some things you don't understand. And if we don't get anybody saying that we're going to assume that we have pretty good

understanding of this, not perfect understanding, we'll probably never get to that point, but we do want to get a reading on the room in terms of your understanding of these proposed uses of Whois data that maybe translated into some purposes, okay?

Is there anybody that feels like you don't have a reasonable understanding of what's been presented? And I'll turn around and look behind me. Just raise your hand if you don't. So I'm going to conclude that we've got pretty good understanding now, and of course people in the working group that aren't participating today will have a chance to weigh in on this. We'll do another test after the final documents are presented and we'll have some action items that are fairly clear at the end of our meeting today but we need to move forward.

We're not going to have a formal break today, so if you're desperate I think there are resting facilities on either side of us fairly close, feel free to use them as you need to, feel free to get some refreshments if you need them. And we're just going to plow through.

And right now we're going to go back to the previous agenda item. Thank you very much, Rod, for leaving your other work and coming here and helping us and for the whole team, it's very much appreciated.

Better get my mic on. Chuck again. And so now we're going to go back to the domain name purchase and sale area. And Lisa was the coordinator there and I'll let you take it and whoever from the team is going to share.

Lisa Phifer: Thank you, Chuck. Lisa Phifer for the record. So the first thing some of you might notice if you're watching closely is that the name of this purpose morphed from business domain name purchase and sale to domain name purchase and sale because it became increasingly apparent as the drafting team worked that the situation wasn't much different if you had a business – a domain name registered by – for business purposes for any purpose.

The team that worked on this included – well Rob Golding was on our team but I don't believe he joined us for our calls, Fabricio Vayra, Sam Lanfranco, both of whom are participating remotely today, Brian Scarpelli, Benjamin – I'm not even going to try – Benjamin A., and Erica Varlese. And Erica is kind enough to actually volunteer or be volunteered to present the output of this team, so I'll turn it over to Erica.

Erica Varlese: Thank you, Lisa. This is Erica Varlese. So I'll wait until we have it up there. So I think a large part of our – what the group worked on as we discussed and went through the drafts, we focused a lot on trying to streamline things and keep it simplified. So I'll say as we go through this you'll see, but a lot of where we began in the first draft had a lot more granularity and there was – we had teased out a few more user roles and things like that in both the definition and in the user roles section.

And as we spoke, we realized just like with the title of this purpose, we didn't want to limit ourselves by being too specific and included some of those elements as examples instead, so that's one thing to keep in mind as we go through this and for questions too, if anyone disagrees with this.

So in terms of the definition that we came up with, the – what we have is the purpose enables contact between domain name registrants and third party buyers, in which we included some examples such as small businesses, corporations, trademark owners, things like that, for the purchase of domain names and also for both parties to complete and confirm the domain name transfer from the seller to the buyer.

Okay, now it's large enough so I don't need to read it fully. No worries, I didn't want to – I didn't want to talk through it without people seeing it.

So that's where we landed with our definition. Actually I don't know if in each section we can stop for questions or if that's – I assume, keep going. From

there we went into the tasks which in terms of purchasing or selling a domain name we landed on using the registration data primarily as a way to contact the current owner, whether that's directly contacting the owner or if they're using a privacy or proxy service, communicating through that service or through a legal contact if necessary for example, again, we spoke about trademark if someone had purchased a domain that was a trademark infringement, if you needed to contact them through legal measures, or simply just contacting a registrant about purchasing the domain from them.

Likewise one – the metaphor that we came back to in terms of acquiring a domain was the comparison to purchasing a house. And using Whois history in the sense of like a title search, so being able to see the domain's registration history for prior associations as well as certifying ownership and that the registrant or the person that you're in contact with is the person that can indeed transfer the domain to the buyer.

Let's see, and ultimately in summary, you know, informing buyers and sellers that they're working with the – who they're working with, facilitating verification and then using the information to carry out the purchase and sale and ensuring that the domain name actually changes hands before the final payment is made so using the Whois to confirm that change when the ownership changes as well.

Yes, any questions on the tasks so far?

Maxim Alzoba: Maxim Alzoba for the record. Are we discussing user roles here or we're going to discuss a bit later?

Erica Varlese: Yes, well, user roles are next, this is just the test for – so if you have questions.

Kal Feher: Kal Feher. I don't quite understand why history is required to prove ownership?

Erica Varlese: We came to history more from the sense of determining – Lisa, correct me if I'm wrong, Lisa, if I'm explaining this from our discussions, but in the sense of who owns the domain now so if there's any relevant information in terms of the domain's history, if it was passed along previously or sold previously to ensure that you're communicating with the registrant and, yes.

Susan Kawaguchi: Do you mind if I add some insight even though I was not on this team? But did a lot of domain acquisitions when I was at eBay and Facebook. We would investigate what the Whois history to see what the domain name – who had owned it before, if it had been used for porn or something, then we would move away and look at a different target. So the Whois history was really important to knowing – to really – and also to value the domain name.

Lisa Phifer: This is Lisa Phifer. And I'm actually echoing a comment that Fabricio Vayra put in chat, and he was part of working on this purpose. He pointed out to us several examples of cases where being able to access the previous history about the domain name went to merchantability and how the domain name previously was used if it was used in a way that was incompatible with the desired new use of the domain name.

Maxim Alzoba: Maxim Alzoba for the record. One of the potential uses, yes, relevant to history is to understand if it was involved in some kind of not criminal direct activity but activity which led to, for example, being, yes, the domain name basically being filtered by anyone or been marked quite badly, so we will have to spend a lot of time proving that you're not unaffiliated registrant and basically it will cost you in terms of time and money to just clear the name, I'd say, of the name. So it makes the asset less valuable because you have to put into calculation those, yes, the time and money you need to invest into the process.

Chuck Gomes: This is Chuck. Let's remember that a lot of these tasks, even like with history, involve research that goes beyond the RDS, and that's okay, but let's also

keep in mind ICANN's mission and focus when we're talking about these things. And again, some of these things we're going to have to get into a little bit more later on but that's okay, it's good that we're talking about this for understanding, I just want to remind us all of those limitations, okay?

Man: At the risk of overly pedantic, I would say that – the use cases you're describing though, don't – it's not own issue, you're talking about reputation. So perhaps you might want to reflect that.

Erica Varlese: This is Erica. That's a good point, thank you. So moving onto the users, we broke this down into three separate roles, the third party buyer, so the person who's attempting to buy the domain name, the domain broker, so a person who may be facilitating the purchase and lastly the registrant, the person who currently holds the rights to the domain name. And originally this was an item that we had broken out into separate – many more user roles and we decided – we made the decision as a group to change from having each specific role to labeling the as primarily just third party buyer.

We felt that – we felt that being too specific there we may be limiting ourselves and we didn't see enough difference between what we had in terms of – and what those buyers would be doing. We felt ultimately the goal was the same in the end and they would have the same – primarily have the same purpose, so we moved those two examples such as a small business owner, corporation, people along those lines. Maxim.

Maxim Alzoba: Maxim Alzoba for the record. Just about the users, to avoid confusion, could we call the first – third party buyer like potential registrant, because when – if the party buys the domain they're going to be registrant. And the reason is because to avoid confusion between third party and affiliated parties, because sometimes we saw situations where the affiliated parties were filing – buying domains to just recognize the portfolios but for some reason they couldn't, for example, do it for free because in some jurisdictions it could be

seen badly from the tax agency's point so they could add like say no, no, no, the real cost was that and you was trying to avoid taxes, for example.

Chuck Gomes: So, Maxim, this is Chuck. You would add a fourth user role, as a future registrant?

Maxim Alzoba: I'd change it to avoid third parties or affiliated parties, it's too long. Just potential new registrant.

Lisa Phifer: So, Maxim, we actually had quite a bit of discussion on this point, and we ended up with third party buyer as the most comprehensive single term because the new – the party involved here may not be the registrant themselves, but might be an agent. It might – the domain name might ultimately be registered through a proxy so there are many cases in which you're involved in purchasing a domain name but you won't end up being the registrant.

Maxim Alzoba: I was thinking that it falls into the broader – so either you – which is for your entity or your own use, or it's broker who is between either, yes, for some time or maybe for indefinite period of time.

Erica Varlese: Okay, I think we could bring that up I guess in the next call, would that? Okay. One more.

Kal Feher: Perhaps a bit explanation but or maybe I'm jumping ahead, I'm sorry, I don't quite understand why you've got trademark infringement and legal action for this purpose, for the purpose of purchasing...

((Crosstalk))

Kal Feher: Yes. I mean, they might be there incidentally for those other purposes and you might use them for those, but for your purpose...

((Crosstalk))

Kal Feher: Oh I'm sorry, I've jumped ahead, sorry.

Chuck Gomes: Yes, get close to the mic when you're talking. I'm not even having mine on. So get – you have to get fairly close to the mics to be heard.

Erica Varlese: Okay then moving into data, this is Erica. And maybe I can answer your question then a little bit as we hopefully go through that. Registrant name of course so we know who we've come – we've discussed knowing who you're speaking with and the contact for transferring the domain. Likewise contacts, a way to get in touch with the registrant.

In terms of, let's see, the registrant's country, in some of the examples that we had discussed as a group, one of the items – one of the examples that came up was around trademark if someone was – if someone had registered a domain that was a trademark infringement you might need to contact the legal contact. And it wasn't – I don't know – was your question more about why that would be – why that's included one of the data elements that might be used or if that should be like separate from this purpose?

Kal Feher: Kal Feher for the record. Yes, basically so if you're talking about one of the other purposes, one of the legal purposes, then I could understand why this data might be there. And you might benefit from the presence of the data, but then what's your purpose for this data in the case of a domain name sale?

Erica Varlese: Right.

Chuck Gomes: This is Chuck. And Griffin, you can go next, but I just want to point out legal contact, as I think everyone knows, is not a current contact in Whois, okay. But it is one of the suggestions from the Expert Working Group. I just – for those that don't know – have that context I wanted to make that clear. Griffin, go ahead.

Griffin Barnett: Thanks, Chuck. This is Griffin Barnett for the record. I think maybe what this is getting at, and you guys can correct me if I'm wrong, but maybe sometimes in the context of an IP enforcement, you find a domain that you say oh that looks like it might be infringing, you contact the registrant and say hey, we think there might be, you know, an issue here. But as a means of settling the matter, you say we'll buy the domain from you and that will be the end of it. And so that's why it would be involved in a domain sale purpose. But that was maybe my interpretation.

Kal Feher: Right, I see, so you start off by finding a domain name that's infringed, and you resolve it by making the sale. I would still argue that you should at least here only things that are involved in the sale because ones involved in like investigating and tracking and identifying a concerned domain and a contact and then now your resolution is the sale so let's focus on the sale.

Chuck Gomes: And this is Chuck again. And again, the team is going to take all this input in as they prepare a final version of this, so certainly if anybody on the team has a question – further question, please ask.

Erica Varlese: Thank you. And again, coming back to the data as we discussed before in terms of the merchantability of the domain, we have the date of registration to establish the history. Legal contact, which again goes into what you were just talking about in terms of if there was a trademark infringement and that was the ultimate result being able to deal with that through legal means. And this came up more in the context of maybe a larger corporation purchasing a domain that had been registered.

And lastly from the EWG report one of the suggested data fields was the domain name specified for registrant, so again coming back to more of a – if it's a larger business or a corporation that's purchasing a domain or if there's – this was suggested in the context of a merger so we included this as a means of accounting for those situations as well if it's two corporations

merging and they might need the – all of the domains for the particular registrant of the other company or that the other company owned.

And that was where we landed on everything, that was our whole purpose and all the elements that we had listed out so if anyone has questions about that or feedback as well.

Chuck Gomes: Thank you very much, Erica and to the whole team. Is there anybody that doesn't have a reasonable understanding of this particular use? Okay, good job. Now just a little side note here, especially for those that are new, Erica, this is only her second ICANN meeting and she's relatively new to the working group, and I'm bringing her up to point out that if you're new don't be afraid to jump in and contribute. Your input will be welcome and thank you very much.

Okay, we'll bring up the next use...

((Crosstalk))

Chuck Gomes: Okay, technical issue resolution, and, Rod, guess who was the coordinator here? Oh he's gone. So that won't work. So, Michele, you're up. And I'll let you introduce your team members and talk about the document that your team produced.

Michele Neylon: Thanks, Chuck. As people hear my voice quite a lot, I'm not going to do any of the talking, I'm going to hand it over to another person with dulcet Irish tones.

((Crosstalk))

Michele Neylon: Oh, come on. So no just I'll do the basic introductions before handing it over. So we were looking at the technical issue resolution. Greg, Alan, Greg Shatan, Stephanie Perrin, who I think is at another session at the moment,

Greg Shatan isn't here, Jonathan Matkowsky might be here, I know he's in Abu Dhabi, not sure if he's in the room, Nathalie Coupet I haven't seen. And James Galvin, I believe is here, staring at from across the table.

Message from Jonathan Matkowsky to everybody, which I was duty bound, is that he wants to – wanted to go into more detail on some stuff around the contents of various RFCs, and we probably will get an update from him at some point in the future. I don't think – I don't know if he's in the room today.

I will now hand it over to Alan and Greg and others will pipe in when they feel that they need to.

Alan Woods: Alan Woods for the record. And I'm assuming they probably will need to. But so I suppose from a beginning point of view on the first one, the technical issue resolution, from my point of view and when I first looked at this and noting the task is purely to define the – what that means in the context of using the information that is provided, I thought that was – it's one of the more obvious uses considering it is probably the initial basic use that was envisaged.

So we put just – we had our meetings and we put together the document and came up with, you know, just a definition around it trying not to just say it is for the resolution of technical issues. So the definition I'll just read that out very quickly for those – for the benefit of those not seeing the document.

Use of Whois data elements in the tracing, identification and resolution of incidents which relate either entirely or in part to technical issues relating to the DNS, use of such data should ordinarily be limited to those who are affected by such issues or by those persons who are tasked directly or indirectly with the resolution of such matters on their behalf.

So we went on a – adding to the definition somewhat in order to, you know, tie it down to that original and pure purpose, I suppose. So the next part of

the document there you'll see is actually just the Expert Working Group itself, and we left it in because I think again, it was a very well put and self explanatory rationale for registration data and again that's to facilitate the contact with the domain contact, the individual role or entity, who can help resolve technical or operational issues with the domain name. And that's including example the DNS resolution failures, email delivery issues, Website functional issues, compromised hosting, etcetera.

So and also noting that the other two teams have put in an awful lot of effort into these, I mean, it wasn't from a want of to do this quickly or anything it was just that the tasks that we came up with were very, I suppose, self explanatory and easy enough. So the tasks that we are suggesting are things such as looking into compromised hosting, again, the email not working as was pointed out in the rationale, identifying a hosting provider or a registrar whether problems with the DNS hosting or, for example, if you can't access a Website or the name doesn't resolve, or the name servers are not responding you would need access to the data, or, you know, again simply to all encompass of that, the website itself is just offline.

There is a note there just I suppose just to point out that resolving technical issues it does also involve data, other data with multiple domains as well, so you could be looking at the domain, the mail domain, the name servers of the domains, or specific services which are used on that domain. And again, this is all example through the data that you can find.

The data that we envisaged people to be using in such instances, of course, are again, rather self explanatory in this one, the technical contacts, whoever they may be within it, and of course there may be instances, again, it's not just limited to the technical contacts, the registrants contacts themselves and again, looking at the name servers, the server status or the expiration data as well because these might be things – yes, Michele.

Michele Neylon: Sorry, just to clarify on the first point on the technical contacts, what we mean the contacts who are capable of doing technical things, not the tech C, just so we're clear on that one, before anybody asks. Maxim. Of course Maxim does.

Maxim Alzoba: Maxim Alzoba for the record. I think you might want to need abuse contacts because if I'm not necessarily a registry but hosting company, and I see that maybe someone's site was compromised and they are attacking my network most probably I need to report it to just its not very technical but it's abuse contact which is a different field now, as I understand.

Alan Woods: I 100% agree with that one, yes, it was probably more of an oversight than anything, but that makes perfect sense so we can definitely add that in. Now sample users, I mean, we brought in just two...

Michele Neylon: Excuse me, Alan.

Alan Woods: Yes.

Michele Neylon: ...but...

((Crosstalk))

Kal Feher: Kal Feher. Could I just clarify when you say "server status," do you actually mean domain or EPP status?

Alan Woods: Yes.

Kal Feher: Okay.

Alan Woods: Yes, exactly.

Kal Feher: Server status is one and you might have clients that...

((Crosstalk))

Alan Woods: Oh pardon me, yes, sorry that was the registry in me probably speaking to that one. Yes, it's – again if a Website is down and there's a server hold on it or a client hold, that's a good reason why you'd see straight away. Turn myself off there. I'm done.

Okay, and so the sample users then again, we just put down again, those who purely we would think as being the persons for this particular reason would use it and that would be abuse responders and then all encompassing an Internet user, I mean, again this was a difficult one to define narrowly but I think we defined it as narrowly as possible and in an all encompassing way if that makes any sense whatsoever.

So that was the first one, it was short and sweet because again, we believe it to be rather self explanatory in that one, we got – well one would hope an easy job in that one. Any questions on that one? Except for Michele? Yes.

Michele Neylon: No I'm just – sorry, it's not a question, it's more to just expand a little bit. The – part of the rationale behind some on this one is while a lot of the data that you might use would appear in what is now called Whois, because it's very, very technical in order for the domain to actually resolve on the Internet, it's also available via the means such as, you know, you're looking at other things, you're looking at DNS lookups, that kind of thing as well. So it's not – and as my learned colleague, Mr. Woods stated, I mean, this is the original purpose of Whois; this is what – where it all came from and where maybe it all will go back to, who knows. Thanks.

Marc Anderson: Yes, Marc Anderson for the record. You know, I know Internet users is a pretty broad net but I might break out another sub-category for you know, maybe IT administrators, IT professionals, I think they're a pretty specific use case for people that might need a technical contact. So a minor tweak but I think I'd add that as a separate bullet point.

Alan Woods: Absolutely, thank you for that. Again, we were resisting urges to just say “everyone.” But yes. So for the next one, I don't know, Greg, do you want to from the beginning or do you want me...

((Crosstalk))

Chuck Gomes: Hold on. Hold on. Okay, this is Chuck. So is there anybody that doesn't have a reasonable understanding of this use area? Okay, good.

Lisa Phifer: I had a question.

Chuck Gomes: And Lisa has something.

Lisa Phifer: Sorry, just before we leave this one and transition to the next, I notice you have (unintelligible) responder but of course that was almost all that Rod talked about. So how do you see these two intersecting and where would you delineate?

Alan Woods: Great.

Greg Aaron: Hi, this is Greg Aaron. I'll give you an example from the other day, and it has nothing to do with abuse. I went to a Website that I enjoy, part of it was broken, one of the features was broken, so I needed to find the contact so I looked up the Whois information and contacted them and they fixed it, and now I'm happy. So.

Lisa Phifer: So I understand how that would be technical issue resolution. My question is, is how abuse would actually fit into this or if it's something that could be clearly delineated.

Greg Aaron: I'm not sure I understand the – where you're going with it. I mean, a lot of the things that Rod talked about kind of do overlap with this problem. Abuse is

caused either by the registrant in some cases, they've registered the domain name to cause a problem and we have to figure out who they are, in some cases they've compromised somebody's web hosting or something else and we need to figure out how to get that problem solved either through the hosting provider or some other means.

Lisa Phifer: So my question was specifically around the sample users being an abuse responder, as opposed to someone who encounters a technical issue and wants to resolve it, abuse responder maybe would be a third party and that's why I'm trying to untangle this.

((Crosstalk))

Maxim Alzoba: Maxim Alzoba. Yes, just following up, I think we could add abuse reporter because to properly report abuse, you will need to access these kinds of data and in commas maybe, yes, ISP provider stuff because when they see spike in bandwidth consumption they want to investigate because for them bandwidth means money. And the other party which – oh pardon me. And the other party could be a hosting provider stuff because they see for example that the space is being consumed and they want to understand the reason why and they see traces going to some particular domain mentioned somewhere maybe in the court, maybe somewhere. And so abuse reporters and in brackets, like ISP provider stuff, and hosting company stuff most probably.

Marika Konings: Yes, this is Marika reading a comment from Steve Metalitz from the chat. "Just a comment, it seems that the ability to search across multiple domain names to identify common registrant names, servers, etcetera, is a common theme across several users' purposes. Note that strictly speaking this is not a feature of the current RDS, in the sense that it's not something contracted parties provide today. They did in the system ICANN inherited but that is another story. Third parties provide this."

Alan Woods: Thank you. Yes, thank you for that. I can't really disagree or anything with that. I mean, again we're just pointing out the uses that are put to it at the moment so if there's a new one from that, I can't disagree with that.

Chuck Gomes: Thanks, this is Chuck. And again, you can take the input you're getting today and as you produce a final version for the working group, you can incorporate it as the team sees fit.

Alan Woods: Perfect. It's Alan here again. And just responding back again to Lisa, I completely take your point on that as well. But I definitely think I have to noodle on it a little bit more and perhaps noodle on whether or not there is a clear delineation between abuse in this sense and abuse in another sense. So, yes, absolutely. Thank you for that.

Chuck Gomes: Okay, let's go to the next and last use that we're going to cover today. Give her a chance to bring up that slide and then we'll switch over the other slide that has your statement.

((Crosstalk))

Chuck Gomes: You won't find too many of us criticizing you. Go ahead, Greg.

Greg Aaron: Hi, this is Greg Aaron. The other half of ours was academic and public interest DNS research.

Chuck Gomes: And just to help Greg out, notice that this team covered two of the uses so it's the same team members as the previous one.

Greg Aaron: Okay. Okay and if we could move onto the next slide please? Okay, so part of this – at the broadest level is domain names are used by people to do things. It is actually one of the main ways that people interact with and use the Internet and they use it for all kinds of things, they use it for social interaction, for commerce and many other uses.

And so research into this area wants to understand how people are using domain names but also through them what they're doing on the Internet. And who is doing these things on the Internet. So this is often the use of aggregated Whois information, often across many, many domain names. But – and sometimes using large data sets to understand these things. And in various iterations it uses pretty much all of the information and data fields that we see in current thick gTLD output.

It uses information about registrants and their contacts, name servers, registrars and so forth. And as we go through our slides, I will mention a few specific uses and a few specific studies just as examples.

Chuck Gomes: Hold on a second. Kal has a interjection, Greg, if you don't mind?

Greg Aaron: Kal, can you – I don't know you so can you introduce yourself?

Kal Feher: Kal Feher. Thank you. Neustar. It might be just an oversight but you've got lifecycle research there and you don't have EPP status.

Greg Aaron: I'm sorry, can you speak into the microphone?

Kal Feher: Oh I'm sorry. It might be an oversight but you've got lifecycle research there and you don't have EPP status or anything...

((Crosstalk))

Greg Aaron: Kal, can you speak into the microphone? I can't understand all of your words.

Kal Feher: Right, you don't have EPP statuses in your data.

Greg Aaron: Oh, okay. Yes, so as I said, various fields that are used would include EPP statuses to understand what the domains – what's happened to domains.

This includes information about – actually probably be better if we go to the next slide, I'm just going to go through these specific examples, Lisa, and I'll give you some examples, so keep going down to the table. No, back up. There you go, right there.

Example use cases, domain name registration history, enabling the historical research about probably multiple domain names during research. An example of this would be a study from the University California San Diego that was done recently was called From Academy to .Zone and it was a study of the introduction of the new gTLDs to find out how many domain names were registered, who registered them, whether they were getting renewed and therefore looking at registrant information, create dates, expiration dates and those kinds of things.

So it was actually a study of the phenomena of the introduction of these new zones into the DNS and then how people were using them and in what quantities and also in some cases how they were using them, for example, how were open TLDs being adopted, and what was happening with dotBrand type domain names.

So in these studies a lot of times what you're going to see is people looking at large sets of domains and then teasing out information from the registration data to figure out what happened and who did it and what they were using the domain for, and that's a very typical example.

Internet researchers doing cyber crime research, again, this is going to overlap with what Rod talked about, but understanding patterns of registration, hosting, and so forth. I do this kind of research myself with the Anti Phishing Working Group. We look at all of the phishing attacks that we can find in a given period of time and we find out where they were hosted, what registrar they're hosted at, in what TLDs, we see – look at the registration dates and then see when we saw the phish to figure out how long it took for a phish to appear.

That tells us whether the domain name might have been maliciously registered by a phisher. We also look at the hosting, maybe that tells us if the domain name was compromised. We then see how long it takes for those problems to be solved in other words, contacting the hosting provider.

So in this case it also involves retrieving historical information, in some cases some time may have passed, the domain name may have had – expired but we want to go back and get some historical information. And that's going to be usually in a historical database that a third party has maintained or that we maintain ourselves for research purposes.

Whois accuracy studies, actually one of the very first accuracy studies was performed in the year 2002 by the US government. The Federal Trade Commission wrote a study about the importance of having accurate contact information, noting that it's important for contactability, it also tells us something about if people are going to be able to be reached for legal process, in other words, cases of cyber squatting and those kinds of things.

ICANN itself does these accuracy studies. It's had a program to measure accuracy over time and it's done several iterations of that project and it involves looking at whether the information has been filled in and then several layers of increasing checks to determine whether the information is syntactically valid and whether it is actually factually valid in other words, is a person who registers a domain name have they said truthful information or not. Also whether proxy or privacy information is being used, which tells us something about the preferences of domain name registrants.

If you can scroll down just a little bit to the next items? Studies of Internet proliferation can be about how the Internet is growing, how it's being used in various parts of the world, in developing parts of the world for example. ICANN funded one of these studies recently, it was published in June 2017, and it was the African Domain Name System Market Study. And it did things

like understanding which countries domain names were registered in. So in this case they looked at which registrars were used, I think, and looked at the country of the registrant according to the registration data.

And then they also used that information to look at what the domain names were being used for and who was using them. For example, were they being used for business, not for profits, etcetera. And that data, some of it, was coming from Domain Tools, which maintained a historic database of information that they could go back and look and also find some of this information easily.

Legal and economic analysis, some of that would be for commercial use and some would be for noncommercial or academic use. Of course, this might be done to look at what's happening with GDPR in the future. We're going to have GDPR affect what data might be published in Whois in the near future, we're going to look at – sites have been done about the use of proxy and privacy, that kind of research was done in a PDP not that long ago to find out how many domain names were protected. And then how to relay information onto the domain name owners and so forth.

Research has also been done on the effects of various policies on users including law enforcement, the effect of policies on markets and used in consumer protection.

And that includes ICANN policies, there are several initiatives underway at ICANN right now that will utilize this kind of information. One is the gTLD Marketplace Health Index Assessment, another is the DAAR project, which I'm working on. And if you can scroll down just a little bit there is another one.

The new gTLD program is having follow up in subsequent procedures work done right now to understand how the first – or this last round of gTLDs worked. And we'll see what comes out of that.

A lot of these studies require use of data that's accumulated over time. Of course when you're doing an academic study you want to get it right, you need a lot of data, and you want to see trends over time. And again, these are just a few examples of what people do. These – and shorter studies are done by a variety of people like the Internet Society, the Electronic Freedom Foundation, people who are interested in a wide variety of subjects about what's happening on the Internet and how people use it, and what affect it has on people and organizations. So those are just a few of the uses.

Chuck Gomes: This is Chuck. Greg, could you – and Lisa, would you scroll back up to users and tasks, just real briefly so that people see what was in the template there. Tasks and – oh data elements that's what was I was looking at there, data elements is one of them that we didn't talk about.

Greg Aaron: Yes, and that list of data elements is not inclusive, it's...

Chuck Gomes: Okay.

Greg Aaron: At various times in these kinds of research pretty much every field that's available is used in some fashion.

Michele Neylon: And, Chuck, this is Michele for the record. Just having, I mean, if you're looking at the research one that we were exploring, I mean, one of the discussion points I think that we were kind of struggling a little bit with was, you know, how do you draw the line between doing research so that you know how wonderful, you know, the Internet penetration is in Country X, which, you know, you can use for purely academic research type purposes, versus how many modems will I be able to sell into Country X, because there's no clear line between market research and research for, you know, some kind of more academic abstract purpose.

I mean, and the other thing just from my personal – as the more I listen to this, realize that, you know, as Greg says, you use every single data item

that's there, and if there were more data elements available with more bits of data you'd use them for good or for bad. I mean, you could just keep on adding to it.

Greg Aaron: And one of the things we also see in these studies for example, that are done at universities, for purely theoretical or purposes, is they then get used for practical purposes, which may be noncommercial or may be commercial. For example, there's a lot of good cyber crime – very useful cyber crime research that comes out of universities, and it's done by people who are just doing it for research but then it may have applications like any other kind of information or science, you know, we have.

So I think we're starting to get into a discussion of what's an acceptable use and what's not an acceptable use at this point. So I don't know if that's for another time.

Michele Neylon: Yes, thanks Greg. I mean, just to respond to that, I think it was just to give – make the people understand really that this was something that came up in our discussions around it rather than – it wasn't a case of judging, it was just really a case of one of the members of the group had kind of looked at it and went, okay, technical and academic so let's stick to technical and academic and she had problems with that, and it was a perfectly reasonable question to ask. And if you look at some of the discussions other people have had in talking on other tasks, you immediately see that there is – it's not – there aren't clear lines between each of these use cases, there is a distinct overlap.

Greg Aaron: Yes, maybe another way to say it is that a tool can be used for different kinds of purposes and different motivations.

Michele Neylon: Maxim.

Maxim Alzoba: Maxim Alzoba for the record. I think it could be a good idea to have a separate, yes, like stream for ICANN Compliance because in ICANN

compliance they check all fields, not just fields you chose. They have to because of, yes, to be able to understand how properly you follow the contract as a registry or registrar, they, for example, take your escrow records and compare it to the Whois or RDS record to understand if it's like some...

((Crosstalk))

Michele Neylon: That was covered under another use case though, Maxim.

Chuck Gomes: Yes, so we have the...

Michele Neylon: Regulatory, legal...

Chuck Gomes: Excuse me, contractual enforcement covers that, but you guys can keep that in mind in terms of your final draft and so forth. But Michele is absolutely right.

Marika Konings: Yes, this is Marika. I have another remote question from Steve Metalitz. "Since virtually all the examples Greg is presenting require the aggregation of RDS data and ability to search across multiple domains, do we need to treat this aggregation itself as a use case or purpose?"

Greg Aaron: I don't know. That sounds like a method rather than a use. But that is also a method that's common across many of our examples that we've been talking about in our meetings this week. Not unique to this one certainly.

Chuck Gomes: Good question, Steve. This is Chuck. And again, we'll let the team take all this input in and deal with it. So oh, Maxim.

Maxim Alzoba: Maxim Alzoba. Small clarification, either we need to – it's the question to representation. Either we need to add something to data elements or we need to take out contractual enforcement of ICANN, because for their work

they have to have access to bigger set of data elements here. So we need to move it to some other place or to extend the set of data elements here.

Chuck Gomes: So this is Chuck. And since I was the coordinator for the contractual enforcement one, I think that's well covered in that one. You can be the judge of that yourself, but I think that's well covered there. And you guys can take that into consideration as you do yours. So we need to move on because we want to be able to wrap all this and tie it together and give the teams their marching orders for the next week and a half.

And the – so on this particular one is there anybody that doesn't have a reasonably good understanding of this particular use case? Okay, good. Let's bring up our slide presentation again and we'll go to the next slide.

Okay, so here we have what we would like each team to do and – is to come up with a one-sentence definition in the template, that's going to be easier for some than others. Now keep in mind that the other elements of the information you provided in the template will give more detail, that's where you can put examples, use cases and things like that. So what we have here is – and you can access these slides and they'll come out as action items in our meeting notes as well.

So in red there you can see information collected to enable contact between the registrant and who to accomplish what is kind of a pattern you might want to follow. And we have three examples that are given there that you might find useful. I don't know that it's – we need to, you know, read each of those. You can quickly read them, but you can also access them and the actual action items will include the examples that is distributed. But I will pause and see if anybody wants to add any clarity to this action item for each team or if anybody has a question.

Michele Neylon: Chuck, I do. It's Michele. Are we comfortable using the term "purpose"?

Chuck Gomes: It's a – I'll go to Beth in just a second. Of course that came in Saturday, as you know. And it's a good question, it's a very good question. So, Beth, why don't you jump in?

Beth Bacon: I was just going to say that I agree and maybe it's time we just make the switch so that we can stop making that disclaimer at the beginning of every time we talk about it, that we're really talking about uses.

Lisa Phifer: So while I don't disagree it's important to delineate, our goal actually is to get to purposes. And so what we need to do rather than backing up and saying, okay we'll define use cases instead, is think to ourselves in the forward direction, we have use cases, how do we get to purposes?

Beth Bacon: Well is then the next stage where we're starting to make judgments on what we've already done as groups? Because the purpose would be a judgment and I'm just saying – I don't think we need to back track and I don't think we need to change what we've done but I agree with Michele, purposes is not really a term of art, it's an actual definable thing. But I understand what you're saying, it's an end game, sort of thing, but what the group – is easy for the group.

Michele Neylon: And I love it when people agree with me.

Chuck Gomes: Yes, and I don't want to agree with him, so. Okay, so rather than spending a lot of time on this, it's a really good point, that's raised. Keep in mind we're working on the users and purposes question so ultimately we're going to decide what – which of these purposes we think are legitimate for what users, involving what data elements, we're going to have to get into excruciating detail on that. If a team is – so I would just say let's not get too hung up on that and I think that's what Lisa said.

If you'd prefer us to say let's all try to summarize each use case in a single sentence, that's fine. We don't need to debate that. But ultimately we want –

we're going to have to come up with so to the extent that you can word it like a purpose, we're that further ahead of the game. Does that help? Okay.
Griffin, go ahead.

Griffin Barnett: Just a quick comment on the formulation here of like the single sentence purpose, I don't know that it will always be the case that it's – the purpose is to enable contact like there might be other reasons for doing.

Chuck Gomes: A little bit louder, sorry.

Griffin Barnett: Oh I'm sorry. The formulation here for the single sentence purpose is – it focuses on contact between a registrant and somebody or somebody and a registrant, it might not always be contact.

Chuck Gomes: Marika.

Marika Konings: Yes, this is Marika. And you're absolutely right so I think we're really trying to get the group to think through, and maybe a way of thinking of it is what would you put in front of a registrant when they sign the registration agreement? What would you put in there to kind of justify why you're asking for that information, to whom are you going to disclose it and what data do you exactly need? And at is indeed the next step we're trying to make.

Chuck Gomes: Thanks. Go ahead, Werner.

Werner Staub: Yes, what strikes me is all these names, sentences, sorry, they don't seem to be talking about the users and potentially affected parties. I think they deserve to be mentioned because they are one of the prime interested parties with respect to purpose.

Chuck Gomes: Thank you, Werner. Now keep in mind, we're going to have to work pretty hard on all of these things once we agree on a final – the purposes that we think are legitimate. So we will continue to work on this to the extent that the

teams can get us a little bit further ahead of the game at least give us some issues to discuss that will be helpful. Let's go to the next slide please.

So you can see here the next steps and action items. We would like you through the next week, seven days, a little bit more maybe, to – not much more – continue your work as best you can, hopefully you can do a lot of that online, if you need a call next week and need a Doodle poll, we can – that can be facilitated. And I know it's hard right after an ICANN meeting but you'll see when you see our schedule why we're asking for that. And again, we don't want these teams to string out too long either.

So the Item B there, think in terms of explaining to the data subject why data is being collected for this purpose. Keep it concise and simple. Are the tasks or users identified by your team so diverse and distinct that they may be more than one purpose? If so, split it. Which purposes covered by other teams are closely related or overlap by your team? Again, we're not going to avoid all overlap but if we can minimize it it might be helpful.

Is there any data collected specifically for the stated purpose or does that purpose use only data collected for other purposes? Something to think about and possibly address in your final deliverable. Again, we realize you don't have too much time and so we're not looking for a perfect document. We would like the drafting teams to deliver their final outputs by a week from Friday, this week, so that's November 10.

And to present your – the results, in abbreviated form, to the full working group on the 14th of November call. Now, let's jump ahead, well first of all, are there any questions on any of these? Better look at my screen, oh there we go, I don't see any hands. Okay, let's go to the next slide.

Okay, so there's going to be some changes in our normal schedule. Okay? Now that's really not a change on the 7th of November, we typically don't have a working group call on the week after an in person ICANN meeting.

Note though that on – so the 14th of November would be the next meeting at our normal time, but our normal time is changing in UTC. You can see the note at the bottom.

And we did this last winter too, so please note that. And there will be messages sent out to remind people of that. So instead of 1600 UTC, as we've been doing through the spring and summer and fall, it will be 1700 UTC. And the alternate time will be 0600 UTC, okay?

Note, we made another change, if you – if you recognize the 21st of November is actually the third meeting of the month normally, because we're not meeting on the 7th, we're going to – on the 29th meet at the alternate time for – which is much more favorable for our people from the Asia Pac region and so forth.

And then in December because of the holidays, that pretty much go across the world, so we will meet again at the alternate time, and the third meeting of the month, on the 20th of December, and then we will not meet on the 26th of December of the 2nd of January. We'll pick up our meetings on the 9th, 16th, and again, the 24th is literally the fourth week of January, but that's when we'll have the alternate time.

Again, these will be sent around but if you go back up to the 14th of November, the first meeting after this one is the reason we're asking for the deliverables by the 10th is the Friday before that meeting. Any questions? Next slide.

Okay, yes, let's go ahead and go to the next slide. We're not going to go through this, but the slides do have some links that most of you probably already have but they're available on the slides as you need them, if you don't already have them. Next slide. Again...

((Crosstalk))

Chuck Gomes: What's that? Oh, the – there's also in the slides some other links that you may find, they're general links there but the main thing on this slide is to thank you and see if there are any final questions. Okay, we actually ended early, that's, I'm sure appreciated by everyone. Thanks again, you know, the two teams I led, I was just so impressed by the contributions of people and I'm sure it's the case with every team. And as Marc shared, I think this was a really beneficial exercise. Helping us to do a better job of communicating with one another, of listening to one another and that'll provide a sounder foundation for getting into the nitty gritty deliberation that's ahead of us.

Lisa Phifer: Not to steal your thunder, Chuck. Since we do have a couple of extra minutes, I actually wanted to ask if you all have any feedback on how we used the drafting teams? Our idea was to continue using drafting teams not necessarily these drafting teams, but would reformulate drafting teams as needed as we move forward. But we can refine how these work. So I know, Marc, you mentioned that you thought that it was helpful, but do you have any feedback on how the teams were structured, how they worked, things that could have helped you work better, other than more time of course.

Chuck Gomes: Well let me – this is Chuck, let me make it easy on you and quick too, I think. How many of you have found this effort with drafting teams useful, just raise your hand, and if you're in Adobe and not, you can raise it in Adobe. Okay. Any quick suggestions as to how they could be improved, besides more time, like Lisa said. We were – we had our live meeting – yes, go ahead, Beth. Yes, so there is some value in the short window, thanks. Anything else? Leadership team, anything else? Michele is trying to be the first one out.

Lisa Phifer: Sam has his hand up in the...

Chuck Gomes: Oh.

Marika Konings: No, it's an old hand from if you like drafting teams.

Lisa Phifer: Oh I see.

Chuck Gomes: Oh. Oh so Sam's hand is old in the – okay.

Marika Konings: I think it's if you like...

((Crosstalk))

Chuck Gomes: Sam, if you do want to speak go ahead. Okay, thanks. His hand is gone if you're not in Adobe. All right, thanks, guys. Have a good rest of the week. We're – we have one day more, some may have a couple days more, but hope the meetings here have been useful. Certainly I really appreciate all the work that went into this. Thank you. Meeting adjourned, and the recording can stop.

END