ICANN

Moderator: Chantelle Doerksen
April 6, 2018
9:00 am CT

Coordinator: Recordings are started.

(Lance): Thank you. Good morning, good afternoon and good evening everyone. Welcome to the Accreditation and Access Model for Non Public Whois Data call on the 6th of April, 2018 at 1400 UTC.

In the interest of time, there will be no roll call. Attendance will be taken via the WebEx room. If you are only on the audio bridge, would you please let yourself be known now?

Vicky Sheckler: Vicky Sheckler.

David Steel: Good morning. This is David Steel.

Greg Aaron: Greg Aaron.

Andy Abrams: Hi, this is Andy Abrams.

Tim Smith: Hi, it's Tim Smith here using computer audio.

(Lance): Thank you. I would like to remind all to please state your name before speaking for transcription purposes and to please keep your phones and microphones on mute when not speaking to avoid any background noise. With this I will turn it back over to Steve DelBianco. Steve.

Steve DelBianco: Thank you. This is Steve DelBianco, the Policy Chair for ICANN's Business Constituency. And what we're trying to do today is to set up a two-hour opportunity for a collaborative and constructive discussion on how to advance an accreditation and access model for the non public portion of Whois data which would probably be moved outside of public view pursuant to ICANN Org's plan to implement an interim compliance model for Whois in face of GDPR.

And I presume that the folks on this call, and I currently have over 90 attendees, and I hope we have more, the folks on this call understand the dilemma that we face as users of Whois in the ICANN community. On the screen, for those of you who are dialed into WebEx, is the first page of the draft Accreditation and Access Model which describes an introduction and the attempt there was to try to lay out the urgency of attempting to design an accreditation and access model.

We had extensive sessions on this – and let me ask if folks put their phones on mute if they're not speaking that would be helpful. Thank you. Rudy Mendoza and David Fares, we're hearing feedback from your lines right now. David Fares – on your line so please mute. Thank you.

When we met in San Juan for the ICANN 61, we did an entire session on ICANN Org's presentation of the Calzone model. And we actually don't need to spend much time on that today, if any. What we need to discuss today is if

Calzone, the draft interim compliance model, were implemented, how would legitimate purposes be served by those who need access to Whois information on how to contact the party responsible for a domain name. That information is available on public Whois today and it may not be available.

((Crosstalk))

Steve DelBianco: But it may not be available subsequent…

((Crosstalk))

Steve DelBianco: …to the implementation of the draft interim model.

((Crosstalk))

Steve DelBianco: Yes, we're all making the transition here from Adobe Connect, where we had some familiarity to something new in the form of WebEx. But it sounds as if most of our problems are the old fashioned kind where someone dials in or accesses via the web and forgets to mute their microphone or mute their phone line so that's the most important thing to remember right now or we're not going to be able to conduct much of a discussion. So if the staff that are helping us with this can identify folks who perhaps have inadvertently left their phone off mute, put it in the chat or directly to that individual.

So let me quickly state the ground rules for today's session. Brian Winterfeldt, who's President of the IPC, will take five minutes to give a history and overview of the current draft of this accreditation and access model. And then we'll have 90 minutes of substantive discussion on accreditation and access, and this will moderated by Fabricio Vayra, one of the drafters.

Each moderator or each segment will manage a queue and the participants will have two minutes to ask a question or present a refinement of the solution that we're currently discussing, and that'll be available in the WebEx screen. And then the moderator will manage some appropriate follow up, that is to say questions, answers or further discussion on the intervention that came up. But please keep in mind it needs to be a two minute intervention.

Okay, after this call we expect volunteers of the drafting group to chronicle all the comments and suggestions that we have today, the questions that came up and attempt to resolve them in another draft. I guess that would be 1.4 because we're currently looking at draft 1.3 and we would circulate that in the days ahead.

So three parts of ground rules, the first is that we would welcome criticism when it's accompanied by a solution. This is a working session and we assume that everybody on has a good intent to solve the problems we've identified by Article 29, DPAs, commissioners, the GAC, law enforcement, cyber security, IP and consumer protection.

Time constraints are going to need to be strictly enforced, that is to say the two minute per participant in the queue. And if you need more time get back in the queue. If you need more time or don't have everything ready to say, it'll be fine to send an email after the call where you could expound upon the suggestions that you may have and attach documents. And all of these emails will be publicly archived and available. And then finally let's treat – let's please try to keep it constructive and more to the point, it's fine to be critical but it's unhelpful to be critical if you don't offer a viable solution. That's what we mean by trying to be constructive.

Okay so I'll turn it over to Brian Winterfeldt but remind everyone that we're speaking of the portion of the Whois GDPR solution, the portion of the solution to solve for how legitimate actors for appropriate purposes can get access to and be accredited to have access to the non public Whois data. With that, Brian Winterfeldt, over to you.

Brian Winterfeldt: Great, Steve. Thank you so much. Good morning, good afternoon and good evening, everyone. I want to thank everyone very much for taking time out of their busy schedules at what's a very hectic time to join us today. Before we launch into our discussion of the model, I wanted to quickly run through a brief introduction of the accreditation and access model. As you know, on May 25, 2018 the General Data Protection Regulation, or GDPR, will come into effect. The interim model for compliance proposed by ICANN Org, as Steve just mentioned, currently lacks specifics about a mechanism for access to non public Whois data for legitimate public interest goals such as law enforcement, cyber security, consumer protection and rights protection.

The primary goal driving the development of this accreditation model is the prevention of a period of time blocking access without recourse to critical Whois data elements such as registrant email. The harms of blocking Whois data without a mechanism for accreditation and access are immeasurable and include restricted or even eliminated ability to address consumer fraud, disinformation, spam, phishing, bot net attacks, DDoS attacks, the sale of counterfeit pharmaceuticals and most grim, even things like child abuse and human trafficking.

In order to facilitate a quick and easily implementable solution, we've reviewed previous community work on legitimate purposes for accessing Whois. We've looked very carefully at the Expert Working Group final report

on next generation directory services, and have developed this accreditation model for community review and work.

It was first presented at ICANN 61 where ICANN Org senior staff pledged support to facilitate further community work and discussion on the model. We really want to thank the Policy staff for supporting today's call and the publicly archived mailing list for further discussion and we will circulate details on how to join that if you have not already received it.

At ICANN 61 the model was socialized and afterward further refined. We've been collecting further comment and integrating suggestions from across the community. I'm getting an echo. The accreditation model accordingly presents an available solution to the problem of access to non public data elements and lays out the types of eligible entities that may seek access to data, legitimate and lawful purposes for accessing the data, how eligible entities may be accredited to access data, a proposed operating model and terms of accreditation.

I am now going to turn the discussion over to Fabricio Vayra to facilitate the community discussion on the accreditation model and again I want to thank everyone for being here and look forward to what I hope is going to be a very fruitful and productive discussion. And again, the goal really is to collect input from across the ICANN community. The IPC and the BC got this work kicked off because we were actually requested to by ICANN staff, and even members of the Board of Directors.

We were told that this was a very important piece that people recognize needed to be move forward so we really happy to dig in and do the work. But again, this is just a starting point and we're really looking forward to collecting your feedback today and beyond today to come up with an

accreditation model that will work for the entire community. Over to you, Fabricio. Thank you so much.

Fabricio Vayra: Thanks, Brian and Steve. Really appreciate the intro. So what you see up on the screen here is a grid that we've put together that basically goes through the document and splits out by the document – the page, the document section, high overview of what the possible issue is that we've identified, a summary of the comment we received and a suggested resolution. And the resolution is highlighted in red.

What we're hoping to do today is to go through comment by comment and basically get your additional feedback either to the sections where people have commented or any additional comment. We have 90 minutes to go through this. I should be able to get through all the comments in about 30 minutes and with, you know, leaving a good, you know, 60 minutes to take any comments.

What I thought would be helpful, again, is just remind you that we have two minutes per comment. What I would suggest in addition to what Steve said earlier is that what would be most helpful is if you provide any comment, basically earmark that you have an issue or a suggestion on how to improve what we've already received by way of comment but then that you actually follow to the 3amcomments@gmail.com email address to submit your comments in so that we can actually capture concrete suggestions and then add them to the grid and move on to a version 1.4. That's been helpful today and we'd really appreciate that you do that.

We will be taking notes in the background, as Steve mentioned, and we will follow up with you, if you raise your hand to make comment to make sure that you submit written comments after the fact so that we can incorporate here.

So to start off with the comments, I thought that I would raise kind of a categorical sort of comment that we received. The version 1.3 that was posted on – to ICANN's page on March 27 contained two current categories and a placeholder. The current categories were cyber security and op sec investigators and intellectual property. And the draft contained a placeholder for law enforcement access.

To frame what we're about to go through, what we – kind of the bulk of what we received you'll see went to actually what the categories were meaning what we received was some bulk comments on the law enforcement access, that it should actually be removed from the draft. The reasoning for that was that it's a specialized category that has specific criteria that law enforcement or governments are more apt to address or tackle.

Then we received some broad comments on including two other categories. And those categories were for public safety and health organization access and business interests. On public safety and health organization, version 1.3 attempted to address that category, but did so in a way where it included some of the access reasons, purposes into the existing cyber security op sec and intellectual property. But the comments we received is that that didn't pay that category due attention and that we should actually tease it out into its own category.

And then the second being what I noted the business interests, and on the business interests, really it was to capture this concept of what businesses need access for, for example, legal verifications and M&A, for example. And what we've attempted to do throughout the comments, as you'll see, is that in some areas we've incorporated the purposes and elements into existing text, and in others we've actually broken it out as (full) category.

So with that in mind, I'm going to go through and just walk through at a very high level what the comments were and how we've attempted to address them. I'd ask that you please earmark what it is that you're, you know, your comment is so that we can go back to it and address your comment. And I'll also give the authors of those comments an opportunity first to give any feedback or input with regard to what they wrote.

And I'm getting something about a hand raised. Yes, and what I would do just go ahead and raise your hands for a queue at the very end and we'll go through the queue and I think we should be able to moderate that from this new application.

Man: The hand raised icon is in the little right hand part of the screen down near the chat window if you're in WebEx.

Fabricio Vayra: Yes perfect. All right, I saw Kiran just tested it, perfect. Thank you. And if the moderator – I don't have access to slides so what I'll do is I'll call out on this Page 1, Page 2 and if you could please flip through those.

(Lance): Hi, Fabricio, this is (Lance) speaking. Actually you have access to the slides so you can move on.

Fabricio Vayra: I do. Hold on, let me test that. It will not let me do that. Oh okay perfect, let me see, perfect. Great. Thank you. All right so with that what you see on the screen is Page 1, and as mentioned I'll go right into the comments and walk through them. Please do take note so we can go back to exactly where you have a comment.

So on Page 1, to the introduction, we had a comment from Zak Muscovitch and this was to adding business purposes into the introduction. As you see the

highlighted text we integrated business and legal verification into some of the reasonings here and we believe that that addressed Zak's comment.

The next comment was in the introduction as well and – make sure – go down. And I assume everyone can scroll through up and down at least on the page? And then I don't have to do that. And so the second comment was, again, dealing with business purpose. Zak Muscovitch asked if we could further clarify purposes by adding legal verification and contractual compliance. So as you see in the red text we've done that by (unintelligible) legal verification and contractual compliance as well as other rights specified in the purposes section. Take a second to read that.

And the third comment we received, was from Bradley Silver of Time Warner and Dean Marks at COA, this one to public and non pubic Whois and really to make sure that we were being clear about the fact that some data was still reserved as public and so we've added this language in here. ICANN has proposed a new working model for Whois system that preserves access to some data but significantly over-complies with GDPR to account for this. Take a read of that.

Final comment on Page 1 went to public and non public data, again. And this was from Tim Chen at Domain Tools, really to make sure that we were talking about access to gated data, not public data so we've made that clarifying comment in here in red. Maybe what makes sense is – is there anyone dying to make a comment on this page at all? Okay, see no hands raised or anything so I'll move to Page 2.

Page 2 on the top, and this also was a comment to Page 2 of the model. Preface and overview, we had a comment from both Tim Chen and from – Tim Chen at Domain Tools and Brian Beckham of WIPO going to the

description of the harm. Tim had asked if we could expand the definition of harm. Brian had asked that we mention the kind of disproportionate harm the elimination of Whois. And we've done that by adding this text here.

The next comment was about the preface and the overview. This was detailing potential harms. And Zak Muscovitch asked us to further spell out the harm, so we added lengthier text, go through and actually explain some of the additional harms that Zak had highlighted for us. Give everyone a second to read through that.

And then the third comment on this page starts – actually what I'll do is – go to the next page. Does anyone have any comment about these two comments topically that they would like to flag or make further comment to? And don't be shy please because it is meant to spark community discussion so don't be put off on the fact that we'll follow up with you.

((Crosstalk))

Fabricio Vayra: Nothing? Okay. All right so the next comment is to Page 3 and 4 of the model. It dealt with eligibility entities and – or eligible entities, excuse me, went to business purpose and this was by Zak Muscovitch as well. And let me go ahead and flip to Page 3 so you can see the whole thing. We largely dealt with his comment by editing, as you see in red here, and inserting some of the business purposes that he'd highlighted so investigation with legal compliance, conduction of – conducting compliance and verification activities, avoiding fraud, you know, accounting for things like legal professionals, accountants, journalists, etcetera, validation of domain names, in addition to what we had as websites before, validation of assets, insuring accuracy.

So that takes up the bulk of this page, I'll stop there and ask – take a read and see if you have any comments whatsoever on this area. Okay. And I see a comment from Jeff Neuman. Thank you, Jeff. If we want the community to sign onto this document we should eliminate some of the advocacy language like stating that ICANN model over-complies. That's a great comment, Jeff. We'll note that you've made that comment and to the extent that you have time to just review and make specific comments back to the email address, that would be greatly helpful too.

So back to bottom of Page 3, starts a comment that went to Page 4 of the model again on eligible entities. There is a comment from Tim Chen at Domain Tools, really to make sure that we redefined or used different language for aggregators really to be threat intelligence providers which is what we were speaking about at the time. So we've made that change as you can see by deleting "data aggregators" and let me switch to the next page, and putting in "threat intelligence providers."

The next comment received was to Page 4 of the draft, again, about eligible entities. And this again was from Zak Muscovitch dealing with business, legal contractual compliance. He wanted us to add legal compliance to the list that expand the list of examples – example organizations. So we've done that here at the bottom. And let me check the chat here.

Got a comment from Mary, there's an earlier question from Maxim. Third comment, "Is there any info to support an assumption that lack of access to info has, for example, in UK led to mass consumer fraud?" I believe that we could get that information for you, that's – and, you know, and I don't know that things probably have a combination of – on the evidence issue, I don't know that – we might be conflating two things because lack of info leading to the fraud is one thing; lack of information to prevent the fraud is another.

And I think that much of what the argument is here is that it's a combination of the two. We have preventive measures by threat intelligence providers who aggregate and correlate the data to try to prevent the data at the front end, but when the – prevent the harm at the front end, but when the harm is, you know, can't be prevented at the front end, having access to the data helps stop the harm quickly. And surely can find you information on – and evidence on at least on the back end. So I hope that answers that question.

All right so we were on eligible entities and Zak's comment about adding legal contractual compliance in. So what we've done in categories so you see here we've added at the end here, to enable legal compliance verification of fraud prevention we've added examples of security related at the top and then some examples of different legal compliance related entities from Zak.

So I'll stop there. Let me look at the chat here, do a better job of that. And if there are any comments in the chat or anyone want to raise their hand and chime in on this comment here? No, okay perfect.

Moving on to our Page 5, this was a comment to Page 5 of the model, again, about eligible entities, also from Zak Muscovitch, asked if we could expand to include IP-related abuse. And so what we did there was change the header to include "and IP-related online abuse" you see the red text here, the addition of – as well as victims of online abuse, expanded by saying intellectual property and other rights and at the bottom of the bullet points we added three bullet points responding to trademark related claims, trademark clearance, IP evaluation and investigation.

And let me stop there while you read that. I'm going to address this comment. And we have here a comment from Maxim Alzoba as well to Page 4, "The

document might be better perceived by the community if examples of entities not to be limited to commonwealth." We will take that note. Maxim, we might have follow up with you on – I think I get what you're saying but we'll take that note and go back to you on it.

And then we have another comment in the chat that says, "Why journalists is added to the list of eligible entities, defined above, this kind of entity – any relationship with security investigation or any subject related," so this was – and maybe we can ask Zak, I hope he's on the line, to give thought on this. My understanding of this is that adding "journalists" – I see Zak's on here. Zak, I don't know if you want to unmute and if you can chime in or directly?

Zak Muscovitch: Absolutely. Thank you so much, Fabricio.

Fabricio Vayra: Yes.

Zak Muscovitch: There was an option, in my view, to include journalists and investigators in an entirely separate category but based upon some feedback that I and others received it seemed a strategically preferable and more prudent to try to condense the categories as best as possible and to include journalists and investigators as part of a broader notion of security and verification. And to paraphrase one congressman in the 60s, you never want to pick a fight with people who purchase ink by the barrel.

And journalists have a very important role to play in fact checking and they need access to Whois. So that's the justification for including them. And I also briefly explained the rationale for including them in the first category rather than opening u a fourth category all together. Happy to answer any further questions.

Fabricio Vayra: Thanks, Zak. Really appreciate that. And hopefully that answered the question but if you have specific feedback, continue to either put it in the chat or please do feel free to submit the comments to the email address we had noted earlier, 3amcomments@gmail.com and we'll get them from there.

Okay, so moving onto the next comment was to Page 5 of the model, eligible entities. We had put in a footnote about the IPC presenting more – basically giving us additional detail to eligible entities for this category for IP. And the way it was written came across as a negative and it wasn't intended so it was rightly picked up by Bradley Silver and Dean Marks with the COA and so we've redone that footnote to "ICANN's IPC has been asked for additional detail regarding eligibility in this category."

Let's see. We've got another question in here real quick from Stephanie Perrin. "How do you manage subsequent use of data in journalist cases?" Zak, I don't know if you had thought on that? My initial thought is there are many ways to handle that. You could have through terms of service that ensure that the – both the person accessing the data understands that they're subject to the GDPR as their own controller once they access the data, terms of service that puts liability on them for passing on.

could do codes of conduct for anyone who's accredited. I think there are multiple ways of dealing with it but that's my initial reaction. I think Stephanie, that's a great question and I think one that the community should take up and make sure that we start trying to answer now because it's one of the things that we need to – a hurdle we need to pass to make sure that accreditation goes through. And, Zak, I don't know if you had any further thought on that?

Zak Muscovitch: Yes, indeed, that is an interesting question that Stephanie raised and Jeff also alluded to. And it's going to deserve some additional thought as I think you mentioned, Fabricio. I'm going to turn my mind to that because I think that a journalist would not appreciate being – having access to the data and not being able to use in the story so we're going to have to turn our minds to that and further consider it as soon as possible. Thank you.

Fabricio Vayra: Thanks, Zak. And thanks, Stephanie, for the question. Let me get through this one last one – well actually I'll stop here because the next comment goes into the next page. But does anyone have any comments specific to the – Zak and Bradley, (Dean) comments about expanding out IP and correcting the footnote? None, okay. I'm not going to read out the comments in the chat just to keep this moving but we're definitely making note of them and I assume others are looking at the chat as well. But if you want me to call anything out please let me know.

((Crosstalk))

Fabricio Vayra: Yes.

Marc Trachtenberg: This is Marc Trachtenberg.

Fabricio Vayra: Hey, Marc.

Marc Trachtenberg: I just did have a comment that was specific to the comments from Zak. And I did put it in the chat but I just wanted to raise it briefly verbally.

Fabricio Vayra: Yes, please.

Marc Trachtenberg: When you added in as well as victims of online abuse, I just wanted to get clarity on, you know, what that was intended to cover and is that – was that intended to cover individual victims that may have been defrauded online? Because if so that seems like a pretty broad category which would be difficult to efficiently or effectively accredit or verify.

Fabricio Vayra: That's a great comment. Thank you. Thank you, Marc. And I see that you put your hand up so thank you for following that rule. I didn't pick it up. Yes, no, thank you. And we'll note that and go through. If you – if you take a look at the model, and again, have anything (unintelligible) this could be you know, better addressed under another category or if you just think it all together should be removed, I mean, would love any kind of drafting discussion there. But the point is well taken. Thank you.

The next comment here was to page 6, eligible entities again, public safety and health access. This was from Bradley Silver and Dean Marks, COA, and (Chris Oldno). We received a comment back that – as I mentioned at the beginning, that public safety and health should be its own category and shouldn't be subsumed into other existing categories. So what you see here on page 6, is our attempt to go ahead and create a category that falls – follows the structure of the existing category, cyber security, op sec, and intellectual property.

What you'll – we've already actually receives some subsequent comment to this as well saying that folks are going to take a stab at tidying this up and making sure that it's a nice tight category. Take a read at this, this is a longer section. Let me know if you have any comment. Okay, any comments to this attempt for public safety and health category?

Stephanie, I don't know if this is to this section but you say, “I would suggest that accreditation standards would not different significantly from the kind research ethics protocols that academics use although I realize that folks may find that to be a burden after years of free access.”

And to the question here, “Was the document sent out?” it was sent out I believe Mary Wong circulated it yesterday evening but if it was not we will go ahead and make sure it gets circulated after this call. And Stephanie clarifies here that that was with respect to subsequent use of access to data. Okay, thank you, Stephanie. We’ll note that. And any suggestions seriously would be welcome if you have them.

All right so not hearing anything specific to this comment let me go ahead and move onto the next comment, which is to Page 6 of the model, legitimate and lawful purposes. Zak, again, offered a expand legal actions. Zak, I think that you had asked at some point to do it standalone. In looking at this we attempted to incorporate it so I hope that’s okay, as expanding the header to legal matters and actions, as you see at the bottom here of this page. And let me move onto Page 7, which then added “asset investigation and recovery, locate a person or service of process identified parties and non parties,” you know, not only just take legal action but respond to actions. So folks consider that.

And then the next one was Page 7 of the model went to legitimate and lawful purposes. This was from Zak again, thank you, Zak. Comment was to broaden the purposes to include contracting elements so as you see here we’ve done this in red by not just contractual enforcement but contracting contractual enforcement including the concept of doing due diligence and investigations. And then in purchase and sale making sure that the brokering and escrow was a capability.

And Zak…

(Lance): Fabricio, sorry for interrupting but we have a hand up.

Fabricio Vayra: Perfect, thank you. And the hand is from Dean. Dean, go ahead.

Dean Marks: No, sorry, I was just making a chat but I was trying to lower my hand, I apologize. Thanks.

Fabricio Vayra: That's okay. Thanks, Dean. Good to hear your voice. Glad you're here. Page – and, Zak, I'm going to go ahead and cover into your next comment as well because I think they're somewhat related. This went to Page 7 and 8 of the model and this, again, for purpose and entity mapping, you'd asked us also to broaden the purpose and reasons to include business purposes. I'm going to quickly – you see where we're going here – I'll quickly toggle to the next page so people can see it but I'll come back to this page so that we can get any comments.

But we added into that section purpose and reason things like compliance and legal verification, research and investigation, and also, you know, being able to practice your law, for example, court cases, due diligence for litigation, journalism, which I believe we've gotten some feedback already that would like further, and consumers so for example, verifying the registrant details, consumer trust, etcetera.

Let me flip back to Page 7 and ask does anybody have any comment and, Jeff, I'll get your question in one second, does anyone have – want to speak up about anything here on Page 7 dealing with legitimate and lawful purposes of

– basically Zak's comments about broadening the scope to business purposes. Okay, so we've got (Steve).

(Steve): Hi, just wondering if we want to specifically mention things like reverse Whois or ownership history of domains. You know, both of those are critical to enforcement of legal rights especially under the UDRP so I don't know if that's something you feel may be covered in other areas or should be mentioned under these purposes. Thank you.

Fabricio Vayra: Yes, that's great. And that might be here in legal verification so maybe what we do is either legal verifications here on Page 7 or practice of law here on Page 8, we expand out the reasons so thank you, we'll note that. Real quick we have Steve DelBianco, did you mean to raise your hand?

Steve DelBianco: Thanks, Fabricio. It's Steve DelBianco. We've now begun the discussion of purposes statements and the question that can't be answered on this call is whether DPAs would give any specific guidance about whether these are in fact legitimate purposes of what we're laying out. And I know you can't answer that question, Fab, but in terms of next steps when we look ahead, do we anticipate doing what ICANN Org has done, which is to offer at some point offer a model such as this for DPAs to evaluate and give specific guidance about whether we've adequately described appropriate purposes? Thank you.

Fabricio Vayra: Thanks, Steve. Appreciate that. And Jeff, you have question in here that says, "Is it the intent of this group to make the list of eligible entities be public so that data subjects know who could have access to their data?" And I think – I don't think it's the intent of the group, I think it's the intent of the GDPR, right? You know, I think that all those who are data controllers who comply with the GDPR actually have to have a purpose statement. The purpose

statement must be told to the data subject and the data subject needs to know exactly where the data is going.

So it's not really us who is dictating that the GDPR. And yes, I think that those who have legitimate lawful interests and purposes and for which the purpose of the data, you know, the data is being collected for that purpose the data subject would have to know. So I think the answer to your question is yes but not something we're dictating, something the GDPR is dictating.

Okay, so we have a comment from Maxim here and that is, "Ownership history is not provided now via Whois so it is a new item." Question here too, and please make the questions directly to the – questions or comments to the – "What about RDS providers? WIPO for UDRP for example, rules require the provider to serve on the contract as set out in Whois." Not sure I understand that one.

I see the chat is continuing on. So here's what I'll do, I'm going to continue on, if the moderators could just let me know if there's a question to this and we'll go back on these comments.

So having received no further comment on this page, we'll go to Page 8 and we have here on Page 8 – we've already gone through this top comment so really we're dealing with one comment which is process for vetting and accreditation, language clarification and this was just really to eliminate a redundancy so I'm assuming nobody has any issue with this but please take a look.

Okay, if no comments I just wanted to point out Zak clarified that what Susan was asking about was UDRP providers and how they require access. And I

think that's meant to be captured earlier in legal actions and things of that nature but if not we should make note and capture that.

We have a comment here from Maxim. "Formerly ICANN can access all fields of data without Whois via escrow and having direct contact with ICANN where the interested third parties might eliminate need for public Whois." Okay, and I think you will see something about that later in the discussion, Maxim. Thanks.

Having no comments on Page 8, let's go ahead and move to Page 9, and we're almost done with the comments so thank you for bearing with us here and for your feedback as we're going through this.

So we had a couple comments from John Levine and I will – I'll just go through them really quick. We had a comment about workability of federated model, really about presenting credentials and how you can do that and also about volume and handling credentials online that only RDAP can do. We're going to hear a little bit later in the discussion about temporary access protocol that I think goes to Maxim's comments and goes to John's comment. So if we could table those that would be fantastic.

And then move right to the next comment which is to Page 9 and 10 of the proposal about accredited users. This was from Bradley Silver at Time Warner and Dean Marks at the COA, really went to if you're going to remove accreditation for someone you should do it in writing so we've proposed this language. I'm assuming nobody has any issues with that.

We had a – to Page 10 of the model we had something from – coming from Tim Chen regarding accuracy and really just pointing out that auditing really

didn't drive accuracy so I believe he's right; we went ahead and struck that language out.

Then we had a comment to Page 10 of the model and this was about referring what they thought violators to the DPAs. And Bradley Silver from Time Warner made the comment that they're not exactly in a position to determine whether someone has violated those terms, so we struck that language.

And then the – let me see – and then we had another comment and this was from John again about query volumes. And again, I think we'll table that because I think we're going to get something in the temporary access protocol. So any comments really about the addition of these three in the center – these comments in the center which are mostly editorial? Okay, Dean, I'm going to assume that hand is just still up from before. Okay.

So let me go ahead and more to the final page of the comments and start on the page of Page 10. And this is to – comment to Page 12 and 13 of the model, went to penalties. Bradley Silver of Time Warner and Dean Marks of the COA really question whether we should be talking about financial penalties so we've proposed striking financial penalties from that list, you know, basically subjecting people for example to the penalties under GDPR as opposed to coming up with different penalties.

Maxim, I see your hand raised, I'm assuming it's to this comment?

Maxim Alzoba: Maxim Alzoba. Do you hear me? Okay, I hope so. The question is, under GDPR if leak happens for example of the personal data which was given to the Registrar A who then gave it to Registrar B and then the leak happened via the third party which has access granted by this model hypothetically, actually all the entities in the chain are subject to financial penalties. And thus it's

quite interesting to see that the third parties want to have access and without sharing the consequences because under GDPR all parties should care about the data they handle, the processes that they established and basically they are subject to GDPR.

So I'm not sure that it's going to work because under the law – under the GDPR those parties might be, yes, subject to financial penalties without additional requirements from the model. Thanks.

Fabricio Vayra: Thanks, Maxim. And just to clarify, I believe the intent here, and Bradley and Dean, I believe you're on, feel free to chime in here, but I believe that it wasn't the intent to say that those who down the chain acquire the data aren't subject to the same penalties of the – say the GDPR or any other local laws. Really to – that they weren't subject to additional kind of contractual penalties, so to speak, financial penalties in that regard, but that they were actually, to your point, subject to the same penalties that say, you know, Registrar A, B and then the receiver acquired.

So if that's not clear, we'll definitely make that clear but I believe that – the intent is the intent you're raising. And Bradley, go ahead.

Bradley Silver: Thanks, Fab. Yes, that was the intent. I can confirm that. So yes.

Fabricio Vayra: Great. Thank you. And thank you, Maxim, for flushing that out. We'll make sure we make that very clear. The next comment was on data access, is Page 13, came from Brian Beckham of WIPO. Question about proportionality and whether accredited users who have access to all Whois records from contracted party meet the proportionality test. We've put in a comment here that the access is only meant to be correlated directly to the purposes identified.

And so we didn't make an edit because you know, the intent here is that people only have access to data that aligns with the purpose both for collection that has been disclosed to the data subject and that the third party accessing has agreed to only collect for and use for those purposes. And then I'm going to leave that one for a second and see if anyone has any comments to that. Please feel free to raise your hand. Okay.

Data misuse, we had a comment here – and this goes a little bit to what Maxim had talked about and I think an earlier comment about data breaches. So incorporating the comment here that really it's data that – incorporating the concept of taking reasonable steps to protect the data and so, you know, breaches are really dealing with those who have actually attempted to take steps here so we've added this language in here and that comment came from Bradley Silver at Time Warner.

And then the final comment we have here is – and I see Maxim, you've put in a comment so I'll read that out in a second. The final comment we have here is dealing with audits and abuse. And Brian Beckham from WIPO had asked the question really I guess are we conflating audits for credentials verse audits of abuse of credentials and that the accrediting body or the validating body really would only have the ability to check for abusive credentialing dealing with the accreditation itself and that the – say the registrar would have the ability to audit for abuses of those credentials.

And we think that that's correct. We've noted at the top of Page 11 of the model has a section about operators are able to obviously demand audits to check for abuses, so we're going to take on to make that more clear but, you know, obviously open up for comment here.

So with this page, we've covered off on the financial. Maxim, thank you for your comment. We had the proportionality, the breaches for making sure it's clear that those who take reasonable steps to protect data and the question about auditing. Any questions there that anyone would like to raise with their hand on? Otherwise, I will open the floor to comments generally specifically, etcetera. We have by my account 50-some minutes, I think that's right – 40 some minutes, sorry, 45 minutes for discussion.

(Steve), I see your hand up.

(Steve): Hi, I'm focusing on data access on Page 13 and it talks about automated queries for analysis and not rate limiting these. Going back to my earlier question about things like reverse Whois and archived Whois so that you can tell when a person acquired a particular domain, as I mentioned, these are both rather critical for UDRP practice.

And I guess this is more of a question, is it perceived that the model would allow for access only to the domain name of concern or would it allow for access to the entire Whois database for purposes of this type of analysis where you need to see what other you know, domains a particular individual might own or you need to look back and get, you know, like take snapshots of let's say all domains, all Whois so that in the future you can just have an archived picture and determine when a particular registrant acquired a domain that was, you know, earlier created?

So that's my question is this – this question of analysis on Page 13, is it focused, you know, on access to the entire Whois database or only one or two domains that are of particular concern for a given query? Thank you.

Fabricio Vayra: So, Steve, I'll take a stab at that. You've picked up on something very important and that through this document and in particular having received feedback during ICANN 61 from the contracted parties, we didn't delve too deep into getting behind the gate that the depth of the access was because what we were asked was to decouple accreditation for getting through the gate and…

(Steve): I see.

Fabricio Vayra: …what you got behind. And the reason being the feedback we received was that we would make more progress on the accreditation side, you know, focus on that without getting into an argument what we got behind the gate. That said, to your point, I think that – well I shouldn't say I think – we heard both from the European Commission and there are two letters to ICANN and most recently from the GAC and their GAC communiqué that there is an importance to exactly what you're talking about, fast access to data that you can correlate to stop harms on the Internet.

And obviously, you know, ICANN has received a mountain of public comment on that and the need to be able to correlate not just for law enforcement but for data security companies and things of that nature. So we didn't fully nail it down here purposefully because of the feedback and requests we received from those at ICANN 61 but clearly I think governments have stepped in to say that there's a need for that.

(Steve): All right good to know. So the basic answer is that it's too early to really broach the subject fully.

Fabricio Vayra: I think that's right. I mean, in this model we haven't. I think the subject has clearly already been broached, right?

(Steve): Okay. But in this model, I understand. Thanks for that, Fab.

Fabricio Vayra: Yes. Maxim.

Maxim Alzoba: Maxim Alzoba for the record. I have a comment about the historical data. Formerly no registrars nor registries do not have this kind of data. Those items are stored in third parties' databases and are available by contacting them. And so I'm not sure that adding this to this particular model will change anything because even if you have right to access the data you don't have in the system it doesn't change things a lot. Thanks.

Fabricio Vayra: Thanks, Maxim. And just to make sure I'm clear, are you saying historical data is not in the system or that aggregation of common ownership or control is not in the system?

Maxim Alzoba: Historical data. For example, client of the company – some Client A, registered domain two years past then he decided not to pay anymore then it was dropped and it was registered by, yes, some other client of some other company and the system at that moment has no information about what happened prior to the second registration nor on registry, nor on registrar level. So even if you grant access to this kind of historical data it's not in DNS, it's not in Whois, that's what I was trying to say. Thanks.

Fabricio Vayra: Thank you, Maxim, appreciate that. Any other comments or discussion points about the model or – Steve DelBianco, I see your hand up.

Steve DelBianco: Thank you, Fab. In response to Maxim's point, whether the historical or correlated data is in Whois is where you've been focusing your question. And I understand that. But remember, this documents anticipates that a legitimate

purpose could be to extract that information so that it were available outside of Whois for historical or a correlation. So those become purposes of querying Whois and accumulating the data in a way that it can serve those legitimate purposes. That doesn't mean who changed Whois, you just preserve the opportunity for historical and cross reference databases to accumulate the data they need to satisfy those purposes. Thank you.

Fabricio Vayra: Thanks, Steve. Appreciate that. John, I see your hand up. Go ahead.

John Levine: Thanks. It's John Levine. It's not clear to me whether we are addressing the question I brought up in private email about how you would actually invent an access scheme that would work. You know, I point at – my specific comments are first that adding credentials to Whois is simply impossible. That's why we invented RDAP. And the other is that the scale that – which this needs to work is really quite hard, is really quite large. I mean, VeriSign currently upwards of 20,000 queries per second and this will be less than that, you know, but it's the not the sort of thing that one or two web servers could handle. So I'm wondering do we know where we're going to address that and, you know, and…

((Crosstalk))

John Levine: Yes, the other question is have we involved the large scale registries and registrars who would actually need to implement this so we know whether they are willing and able to do it?

Fabricio Vayra: So let me address the last part first. We are trying very hard. So yes, I believe that we are engaging them. I don't know that we've received concrete answers. And I know – and obviously they're working very hard themselves so understandably.

((Crosstalk))

John Levine: …introductions if you need them.

Fabricio Vayra: Listen, the more the merrier. We've got some ourselves but, you know, listen, I think the point of this conversation, right, is we're hoping that they're here and they're on, the folks like you're here and that we don't wait until after you know, things go dark and kind of – as I keep referring to the parade of (unintelligible) begins before we actually start addressing it because I think there are logical questions that we should just work through.

To your question about not addressing your – we had three comments listed for you here and I believe they're – let me flip back here real quick, Page 9. We deferred these top here of Page 9, workability of federated model, workability of implementation. We're going to be speaking about a temporary access protocol model right after the comment – after we finish the discussion here. And I'd love for you to be present for that and give your thoughts and opinions on what we'll present there.

But I think that'll go to addressing the concerns you've raised so if you could look back on that that'd be really great.

John Levine: Yes, I could stick around, thanks.

Fabricio Vayra: Great. I really appreciate that. Any others about the – any specific questions we didn't raise here or that weren't addressed by commentators? Just a public service announcement, just please remember that we're accepting written comments at 3amcomments@gmail.com and we'll be collating all those comments into a grid like this that will go into helping establish version 1.4.

Zak, Bradley, Dean, Tim, John, thank you for having submitted comments in this manner, it's been greatly helpful as you can see to put concrete changes into the document. Any others?

Reg Levy: This is Reg Levy from Tucows.

Fabricio Vayra: Hey, Reg.

Reg Levy: I'd like to thank you guys for the opportunity to allow us to listen in. And we appreciate the time and effort that's gone into this but our concerns that our presence on this call might be taken for some kind of agreement or assent. We stress that the contracted parties do not explicitly agree with any of the proposals presented here today but are taking notes of your specific requests and concerns and will consider them while we each develop our GDPR compliance systems.

Fabricio Vayra: Thanks, Reg. And listen, you know, speaking – you know, I don't get to say this much but speaking in my personal capacity, I hope that the fear that someone's going to hijack your participation and recast it as agreement to everything that's said here doesn't keep you from bettering the model and participating because as John pointed out earlier, we desperately need your feedback and we desperately need something that works. And so to that extent, you know, I hope that you will – you know, you won't hold back and hold back punches on this for fear that that's somehow going to be used in a different way. We need your feedback, we need your criticism.

Reg Levy: Thank you. And I'd also like to stress that the people who are present on this call represent the largest of the registries and the registrars, the ones who have the wherewithal to dedicate people to take the time to take this kind of call,

but most of the impacted parties are going to very small registrars who are just trying to bring themselves into compliance.

Fabricio Vayra: Oh understand. Any other comments on this?

Kathy Kleiman: Brian, this is Kathy Kleiman. I'm on audio only.

Fabricio Vayra: Go ahead, Kathy.

Kathy Kleiman: Hi. Terrific. Hello to Brian, to everyone on the call. I want to second what Reg said that participation is not – is participation only. We're listening, we're watching, but I want to raise that I haven't heard and maybe, you know, I came on late, I haven't heard kind of the overall goal expressed here, which is that there's a fundamental right to privacy that the GDP protects that we haven't been protecting in ICANN and that we need to talk about. And that's kind of not the focus here. We're talking about how many people can have access to the data for an array of purposes. I really think as we go through this we need to talk about the concern of that access to personal and sensitive data and that protection that's being given to it under the GDPR. We can talk about journalists accessing the data but it's the journalist data that will be accessed where they will be arrested in certain cases. That's what NCSG works with.

I wanted to point out that the purpose statement that's in your Annex A I believe now, is not a limited purpose statement. It's not a purpose statement that goes through and looks at the collection and processing of domain name registrant data within the limited scope and mission of ICANN. And extensive comments will likely be filed on that shortly. But let's look at the overall goal, everyone, and that's the protection of the protection of the fundamental right of privacy and it all has to be looked at.

Everything we're doing has to be looked at through that lens and through the balancing ultimately of the secondary uses of the data, and that's what we're talking about here is largely secondary uses of the data versus the underlying right to privacy that the registrants have. And so, you know, this data, name, address, phone number, email, if we haven't learned anything with what's happened in the news with Facebook lately, it is, you know, we have learned that this data is very important and compromising and giving it out is of great concern now and the world's awake. Thank you.

Fabricio Vayra: Thank you, Kathy, really appreciate that. Marc, you have your hand up.

Marc Trachtenberg: This is a slight counterpoint I would say the focus of this effort is not the fundamental protection of people's privacy; that is an important goal and that's the goal of GDPR but not the goal of this effort. The goal of this effort is to make sure that those that need access to the data can still get it for a variety of extremely legitimate purposes including protection of individuals against fraud, which they will be subject to in much greater degree if the proper people don't have access to Whois data.

Fabricio Vayra: Thanks, Marc. And I would just add, if I can, onto what Marc said just to say that the focus that you just articulated is all done through I think to Kathy's point, or at least we've attempted, through GDPR, right, and through compliance with GDPR to make sure that there's compliance there. If we've somehow not struck a balance or there's something that changes that balance Kathy and others, again, really would appreciate written comment to how we could actually fine tune not just topically fine tune the document and move a model forward for access that has proper compliance balance, submit those to 3amcomments@gmail.com.

Marc, do you still have your hand up or want to interject? No, okay great. And, Maxim, I saw you pop in and pop out, did you want to make a comment?

Maxim Alzoba: Maxim Alzoba for the record. I have a question, do you envision any kind of proactive review mechanism for the participants of the accreditation model access? I mean, people change jobs, they got fired, they might occasionally lose credentials so there is a need of review before the leak happens. And do you think there could be something about it in the final document?

Fabricio Vayra: Yes, I mean, I'd love to hear from others who participated in this but I'll give my two cents. We attempted to capture that at a high level through the concepts of once people get accredited they have to – it's not a perpetual accreditation, you have to reaccredit yourself on certain intervals. Maybe we got the intervals wrong, so we'd love, Maxim, your comment on the intervals there.

And then obviously the concepts to do a backend sweep of both logging and auditing and we put in there a concept of having third party auditors who take sample sets and check. It doesn't get necessarily to your point but it's to try to pick up misuses or abuses. And I think one of those misuses or abuses maybe we have to call it out is those who obviously picked up credentials under one auspice, and like you said, have moved from that position and are no longer there. But would love any comment from anyone here. And, Maxim, please do check that section out on accrediting and reaccrediting and the intervals. I think that might address some of what you had to say. Others on that?

Greg Shatan: This is Greg Shatan. Can I get in the queue? I can't find my hand.

Fabricio Vayra: Go for it, Greg. You're up.

Greg Shatan: Thanks. Just a couple comments to what I've heard in the last few minutes. First it's great that we have, you know, representatives or not representatives – people from a lot of different stakeholder groups or no stakeholder group at all, and that was the intention of this call, I guess need to make it more clear in the marketing that attendance does not equate with assent or consent in any way to what's being discussed and – which is of course generally true of mot things at ICANN but should be clear here.

You know, so it's not intended to be a hometown type of meeting or a rally or some sort of thing like that. And it's good to identify problems; it's even better to identify potential solutions. You know, this is not the first accreditation exercise in the history of the world. So there's obviously, you know, things that we can learn from elsewhere and to try to apply here and to deal with cases such as the one Maxim brought up which you know, I don't think that breaks the – that doesn't break any of the discussion here, is' just – it's one of those things that happens in an accreditation model and needs to be dealt with as you get down to brass tacks on it.

I think also there are some assumptions being made. Kathy, for some – for instance, assumed that this is a secondary use. I disagree with that. And I, you know, Whois itself is useful but intended really for use by third parties and not by the registrar and the registrant; they have their own, you know, data in their business relationship. So – but I don't want to derail this conversation the way say the RDS group which has just gone into hibernation, got derailed by these discussions. They are obviously important discussions to have but this is a discussion about an aspect of the overall possible way things work.

It assumes that other things will be dealt with appropriately as well such as dealing with legitimate interests and purpose in ways that comply with Article

30, for instance, of the GDPR. So, you know, it's great to point out the weaknesses or the fact that this exists in a larger context but that doesn't stop us from concentrating on discussing this particular aspect and mechanism that could be applied in order to gain legitimate access.

And GDPR is not only about data privacy; it's about access to data as well and under what circumstances and really, you know, spends a lot of time on that so I think that is at least as important an aspect of it. And the idea that there is no such thing as good access to data you know, is just – I don't think anybody is actually saying that but that seems to be kind of the starting point that some people like to come from. That's not really the starting point of the GDPR – it shouldn't be the starting point of discussions here. Thanks.

Fabricio Vayra: Thanks, Greg. And I just – if I could add something when you raised assumption several times there and I would say that one of the assumptions that the drafters of the accreditation model that's being proposed here and obviously those who commented on it thus far have had to incorporate is a big assumption which is that we have this Calzone model and that that is going to be what's implemented. So, you know, we have to basically account for that assumption because we don't know if that's the model or not the model and we're having to react to that. So that's one very big assumption going into this.

Maxim, I see your hand up.

Maxim Alzoba: Maxim Alzoba for the record. I just have a short comment about law enforcement, actually quite large part of the discussion about the access of law enforcement to the data was done in so-called Spec 11 framework group and it's all documented. And yes basically the thing is that on local legal legislation level there is only local law enforcement, if no cross country

agreement is in place, for example to Country A recognized law enforcement agencies from Country B and vice versa. And only this situation the company from Country A formally will recognize law enforcement from Country B.

In other cases in some cases the agreement to hand in personal information of citizens to law enforcement from other country might be seen as a treason and might lead to very unpleasant consequences. And effectively the only thing which unites all law enforcement unfortunately it's Interpol and only via Interpol they will be able to have their identity hidden, for example, law enforcement from Country A requests local Interpol notice for something, it goes to headquarters then it goes to local bureau of Country B and only then it goes to law enforcement of Country B. And it enforces access to data on local level which is well regulated by local laws.

So there is no need to invent something – yes I know that such kind of information request is like 30 days or something is there really fast but maybe there is an idea of suggesting they find some faster electronic means of interaction. Thanks.

Fabricio Vayra: Thank you, Maxim. Michael, I see your hand is up.

Michael Karanicolas: Hi, thanks very much. I'm also mainly here to listen but I thought I would just offer a general comment because I feel like this process has taken something of a wrongheaded approach to the challenge whereby the intent seems to be to list out any possible potential uses of the Whois and then work backwards to design a system which preserves and facilitates them. And I think that that's contrary to the point of the GDPR which is based in the concept of data minimization.

If ICANN doesn't need the information to serve their purpose, they shouldn't be collecting and processing it. There's a fundamental problem with the model presented whereby it doesn't seem to accept that the utility of the Whois will need to be restricted going forward, and if we don't have that as a starting point, I'm not sure that this process is going to be very productive. So I wanted to ask the drafters, do you accept the utility of the Whois to things like IP enforcement will need to be decreased going forward?

Fabricio Vayra: I'm happy to – before I speak does anyone else want to jump in or?

Vicky Sheckler: This is Vicky, I'm happy to jump in.

Fabricio Vayra: Go for it, Vicky.

Vicky Sheckler: This is Vicky. And I am speaking for myself. And I think that that question is misappropriate. When we look at the GDPR, yes, the concept is that we're going to protect fundamental privacy rights but it also contemplates that those fundamental privacy rights have to be balanced against other important rights as well. I represent the copyright industry, the copyright industry is also – rights of authors are also listed in the UN declaration of fundamental human rights.

So the question isn't I think, you know, what needs to be limited or what doesn't need to be limited; the question – the proper question I believe is as we battle into this stuff, how do we justify what are legitimate uses? And these documents are an attempt to do that. If there's concern that the attempt is overbroad or that the use is too broad, or that some of the uses don't fit in the acceptance of GDPR, those are the questions I think we should be discussing. Thank you.

Fabricio Vayra: Thanks, Vicky. And that was Vicky Sheckler for the record. Thank you, Michael, appreciate your comment too. I see Steve DelBianco has his hand up.

Kathy Kleiman: And Kathy Kleiman…

((Crosstalk))

Fabricio Vayra: Okay, Kathy, you're in after Steve. Go ahead, Steve.

Steve DelBianco: Thank you, Fab. In response to Michael Karanicolas's point about trying to restrain the data that is gathered by registrars and registries, when people register a domain name, versus discussing how it may be accessed by accredited users, Michael, I think that this was made abundantly clear in the San Juan meeting that ICANN Org has moved ahead with an interim compliance model that it's already seeking approval from DPAs on. And in that model the registries and registrars continue to collect what they do now. And ICANN Org is very comfortable that they can justify the continued collection and retention of that information.

The purpose of this call, Michael, isn't to reexamine that premise, but rather to say how do we design an accreditation and access model for legitimate purpose that are fully anticipated and recognized under GDPR? So we're trying to be constructive enough to design a way that one can get accredited and then access for legitimate purposes to the information that is public today but won't be public under the ICANN interim model. A number of those data fields for identifying the person who's responsible for that domain name would go behind the firewall and would be nonpublic Whois.

So this is about a laser focused effort to accredit and give access for legitimate purposes for the nonpublic Whois data. So I don't think it's constructive to try to revisit, at least on this call, to revisit whether ICANN is collecting too much or too little under the contracts that it already has. ICANN Org is already presenting that to the DPAs. Thank you.

Fabricio Vayra: Thank you, Steve. And I have Kathy and then – Kathy Kleiman followed by Stephanie Perrin. Kathy, go ahead.

Kathy Kleiman: Great. Thank you, Brian. And I'm not going to speak to the data minimization except to say I think it's still an open question. There may be other forums but I think it's there that it's still very much an issue in play, privacy by design and what data elements need to be collected. So but you're right it may be another forum but it's very much still in play.

So what I wanted to do was something different, returning to what Vicky said, I'd like to read a quote from the Hamilton law firm memo and then ask a question specific to what we're looking at on the screen. So the quote is, and it's Page 7 if anybody has the Hamilton memo, Number 3.

"A layered access model does not automatically qualify as legal grounds to disclose personal data to a predetermined group of people of parties including law enforcement agencies even where a legitimate interest has been identified and determined on the general level. For existence, Article 6.1F GDPR, can most likely not be used to provide all law enforcement agencies unfiltered access to all Whois data but such access would likely have to be assessed in light of Article 6.1F GDPR with the appropriate balancing of interests in each case."

So that's the end of the quote. And here's the question. How is that balancing of interest on a case by case basis envisioned as part of this model? Thank you.

Fabricio Vayra: Before the drafters – thank you, Kathy. Before we answer that, I wanted to be sure, which of the three Hamilton's letters was it? Was that the third one or…

Kathy Kleiman: Yes, yes, Brian, that's the third one. And it talks about it not just for law enforcement agencies but similar reasoning for access by others. This case by case evaluation, because of that underlying fundamental right of privacy in so much of this data. Thanks.

Fabricio Vayra: Anyone want to tackle that? I can – I'm happy to take a stab at that. So with regard to the Hamilton memo, I think we, you know, we've seen multiple legal opinions come out that all together or slightly contradict what those opinions said. I think Hamilton itself actually contradicts itself in all three of its memos, which is why I asked which memo version it was.

But I think the balancing test and proportionality test and things of that nature are important to do and we've tried to account for them here by making sure that, you know, when we're listing out the purposes, the access, that there's a tether between the purpose that's stated, the access the granted and for what use. And to make sure that that complies with GDPR like Article 6.1F.

You know, making sure that someone has legitimate interests and that that legitimate interest that way. So for example when we talk about things like protecting child abuse, whether that outweighs someone not being able to display or keep private their street address, you know, I think we could argue all day about that but I think the majority of the people on the call would say

that hey, if we can protect child abuse or network, you know, massive network abuse or fraud abuse that needs to happen.

And I think that that concept more importantly was recognized in the EC letters and in the GAC letters that recently came out. So we have a law firm hired by ICANN who is giving legal opinions that are threading the needle and then we have objectives basically supporting that a lot of the use cases that are put in here and a lot of the purposes that are put in here do actually tip the balance in the proportionality and you know, fairness, etcetera, and say that access should be allowed. So we're attempting to strike that balance here and if there's something that's particular within the draft we'd love to get that comment.

Stephanie, sorry, you're up. Stephanie, if you're speaking you are on mute. No, maybe it was an errant hand. So real quick, I wanted to go back to a question that Claudio had asked a while ago and was lost in the chat. "Has this group considered how the EU institutions are approaching GDPR compliance such as the EU IPO Trademark Office?" and he gives a link in the chat.

I believe that we have. You know, we've tried to look at everything. And mostly I think that there have been comments up in during the interim model proposals that have actually cited these. So yes, we have taken those into consideration but again would encourage that if there's something specific about the draft that is sparking that comment from you we would love an annotation of some sort to pick that up. And I'm told Marc Trachtenberg, you had something in the chat. I'm just trying to scroll down. If it's easier, please raise your hand and state it here, it would save me time scrolling through the chat.

Marc Trachtenberg: It's there but if you can't find it I'm happy to make the comment verbally but…

Fabricio Vayra: Yes, that would be great if you could.

Marc Trachtenberg: I mean, I'm in full support of this effort and the accreditation model which, you know, hopefully we can come to some sort of agreement on. I was just making the point in the chat and didn't want to take away from the discussion on this model which is that, you know, even if there was agreement on this model today and it was accepted by ICANN and the community, it's pretty unlikely to be implemented by May 25, which means at that point Whois goes dark from a practical perspective to be useful for any sort of investigation of illegal activity infringement or consumer protection purposes.

And I just wanted to get the view of people on the call, maybe not right now because I don't want to take away from this effort but just have them think about you know, whether they'd be okay with ICANN maintaining public accessibility for, you know, just a minimum amount of data elements that are needed for, you know, reasonable enforcement activities and investigative activities which I think would be something like registrant name, organization, registrant email, registrant city and country. So just throwing that out there because I think you know, at least many people on this call are interested in maintaining some accessibility for Whois after May 25, which, you know, is again is the purpose of this call. Thank you.

Fabricio Vayra: Thanks, Marc. Stephanie, can you speak yet? Are you unmuted?

Stephanie Perrin: …now? Hello?

Fabricio Vayra: You there?

Stephanie Perrin: Can you hear me now?

Fabricio Vayra: Yes, we hear you. Great, go ahead, Stephanie.

Stephanie Perrin: …records. Thanks, I just wanted to raise the point that in the evaluation of those who are fighting cyber crime, the data protection authorities have written in some of their Article 29 documents about the problem of the delegation of lawful authority and this came up with respect to the earlier comments – much earlier – on the 2013 RAA. So it's a pretty well known problem. Most governments are constrained by their constitutions and starters as to what they can do with respect to the basic human right of privacy depending on their constitutions.

So law enforcement agencies are covered, grosso modo, obviously there are countries where that's not the case and we talk about in the cyber crimes treaty discussions, however, that's a generalization. Unfortunately, the cyber crime folks do not necessarily have delegated authority from law enforcement to be fighting the kinds of crime that they are fighting. And I wondered and I beg your pardon if I missed it this morning in the discussion, I was having trouble following the document, have you looked at any kind of provision for accrediting cyber crime fighters through their own lawful law enforcement agencies and through the international agreements that the various countries might have?

That's a complex problem but it's necessary if you're going to have accountability for the recipients of this data particularly the deeper data that they're getting from the actual registrars, in other words, the financial data and the address data and the personal data accompanying the registration. Thanks.

Fabricio Vayra: Stephanie, I think that an attempt has been made to at least account for – and obviously that's the broader debate around law enforcement itself, right, because you know, I think that we need some feedback and precisely why we're having this call, we need some specific feedback like yours but directly to the draft on criteria like that, right. You know, that would make that – the section if we, you know, if we stayed in law enforcement but if there are certain criteria you think would be better please make them because we'd like to incorporate stuff in there.

Greg Shatan: This is Greg, if I could jump in again?

Fabricio Vayra: Yes, go for it, Greg.

Greg Shatan: Maybe somebody can tell me where to find the hand in the tablet version of WebEx at some other point. But in any case, I don't think necessarily it needs to be looked at as an issue of delegated duty. There are a lot of moving parts and different pieces in fighting – in dealing with cyber crime and in some cases those involve civil actions as well as criminal actions so this is not, you know, merely a law enforcement issue in that regard. So I think while there may be a concept of delegated duty, it's not the only concept by which we reach the needs and purposes of cyber crime investigators.

And I think while it might be interesting to get involved in figuring out whether somebody is going to accredit cyber crime investigators, you know, at the national level, clearly that's not just going to be something for Whois access, it will be something much broader and that's probably a five-year project and I don't think we have five years for that if there is some existing activity going on in that area that we can hook into so much the better. The more existing accreditation plans or projects that can be involved so we don't have to reinvent the wheel would be great. But I think that, you know, for the

limited purpose of Whois access, you know, trying to get the world's governments to accredit the world's cyber crime investigators on a one to one basis is a process far beyond the reach of this group or project. Thanks.

Fabricio Vayra: Thanks, Greg. I see – I can't tell what order they went up in so I have Maxim on top. Maxim, you want to go first?

Maxim Alzoba: Maxim Alzoba for the record. I have a question, GDPR also regulates cross border flow of data effectively outside of the EU. And it has provisions saying that the process should be regulated and I haven't seen the design proposal for the regulation of cross border access, for example, which, yes, I'd say accredited entity for this model has allowed, yes, is allowed to access data from which source. Because currently I'm not sure that even the Whois system contains, yes, true information about Whois data is stored. For example it doesn't have information about residency because GDPR protects residents of the Union, not only citizens. And you can find this information in the system.

So do you envision something about the I'd say tiered access based on the territories or something? Thanks.

Fabricio Vayra: Yes, Maxim, so I would say we've looked into this quite a bit with regard to what you would call the three categories of data transportation that the GDPR considers. You know, obviously those that are covered one under the GDPR, two category which would be those that are not under the GDPR EU but would be considered to have equal protections and then the third category which is those that don't have equal protection or any protections.

And one of the things that we had (views) with, we have not put this in here but left the opening for it is to create a code of conduct for those who are

accredited that would put in the proper mechanisms and securities that are offered under the GDPR through that code. And where we thought that would fit would be in the terms of service of the accreditation. So when you go through the accreditation you also have to agree to a certain code of conduct for access. That I think would be in development but again I think we decoupled the two so we weren't presenting multiple things at once just like we were not tackling definitively what access once you get there means.

But yes, that concept has been there and hopefully – my answer lets you know that we've been thinking about that in great detail so we do plan to address that.

Stephanie, we have exactly – sorry, one minute left and it looks like your hand is up.

Stephanie Perrin: Can you hear me now? Can you hear me now?

Fabricio Vayra: We hear you.

Stephanie Perrin: I think you can hear me now. Great. Stephanie Perrin for the record. I just wanted to raise the point that – to respond to Greg. Yes, we're in a rationale, we're in a rationale because ICANN has refused to grapple with a very difficult problem for the last 18 years, and I really think it would be more mature if ICANN would express more ownership of the reality the data protection law including in Europe, including under the Article 95 (unintelligible) and all the data protection laws that came in a result of it they have been disregarding.

So, you know, quite frankly the fact that we're in a rush now and we haven't got the time to grapple with the hard problems because it was thrown on the

too hard pile 20 years ago by the Commerce Department is I think something that just is no excuse for not starting on hard multiyear work. We are certainly not going to accept a cobbled together solution that (unintelligible) next 20 years. There has to be the kind of deep look and deep respect for the liability that is being loaded onto the contracted parties because of this refusal. I mean, ICANN has not even acknowledged yet in a fulsome manner that it is the data controller. Well, quite frankly we're long overdue for that discussion, long overdue.

So don't tell me we haven't got time to start the hard standards work, the work on delegating, because right now if you are a contracted party and you wind up with cyber crimes fighter that claims to be a cyber crime fighter and turns out to be a criminal gang, you're going to get the fines. And we're all going to sue. Thanks.

Fabricio Vayra: Thanks, Stephanie. And on that, seems like a lot of people are going to start suing for a lot of different reasons. So appreciate all the feedback. We are at our 90 minutes for comments. Thank you for letting us go through the comments and for your feedback. To not cut from the next presenters, I'll just leave with please submit any specific comments to the draft to 3amcommetns@gmail.com, that stands for 3 access model comments @gmail.com. Thanks again, really, really appreciate everyone's time in walking through all these and the consideration you've given.

With that I'd like to pass it over to Susan Kawaguchi. Susan, hopefully you are on and you will give us a temporary access protocol overview proposal. And John, this is the section – John Levine, this is the section that we said may address the questions you had brought up earlier.

((Crosstalk))

Fabricio Vayra: Perfect. Susan Kawaguchi can you hear us?

Susan Kawaguchi: Can you hear me now?

Fabricio Vayra: Perfect. Yes, there you are.

Susan Kawaguchi: Okay, sorry.

((Crosstalk))

Susan Kawaguchi: …control my mute on WebEx. So just really quick, there's been a lot of brainstorming going on and one of the ideas that has come up is actually using existing technology that ICANN uses right now. And what this would do it would be a component of the accreditation model but it – this does not address how people are accredited. It also does not address the data that they would be receiving. But it would address and facilitate white listing of IP addresses once you are accredited then to access that information through Port 43 you would have to have a IP address.

And in today's world, the registrars all use RADAR, which is a technology and a database where they white list their own IP address to be able to access other registrars' Port 43. And so the brainstorming part was we were thinking that we should leverage existing technology for this temporary solution so that once accredited your IP address would be white listed in this database, the registrars wouldn't have to implement any new technology. They would – they are used to going there and downloading a file of IP addresses. And so this would not – there might be a few changes to allow the accreditation model to insert those IP addresses but for the most part would not make – have any new technical challenges.

And ICANN could manage this process of once validated the IP address goes into this database, sort of a RADAR-like database and the registrars could go and retrieve that. And then you would be given access to Port 43 for that registrar. So there's a lot of details that would have to be worked out but what we're all looking for here is a model that we could stand up quickly and relies on existing technology that doesn't create an additional burden to those in the system.

So that's – that was just a really quick high level and, you know, it's more of the brainstorming so if anybody has comments or concerns?

Fabricio Vayra: Thank you, Stephanie – Susan, sorry, I'm looking at Stephanie's name here. Thank you, Susan. John, I see your hand's gone up.

John Levine: Yes, I mean, if the registrars will do that, that would be great. I mean, a lot of us have been trying to get white listed at registrars for years and for them to finally do it, that would certainly be a perfectly adequate interim solution.

((Crosstalk))

John Levine: I presume this applies to registries – one question, I presume this applies to registries too for thick Whois?

Susan Kawaguchi: Yes, I would think we could make it work that way (unintelligible) saying, you know, this is a brainstorming so we'd have to look at it and talk to ICANN. And I did notice that Maxim has brought up that RADAR is not a good…

((Crosstalk))

Susan Kawaguchi: And right now, yes, RADAR is offline, there's some security risks. But I'm sure with all the brains in the room that that can be fixed.

John Levine: Yes, I mean, it's not – there's lots of ways you can like fake IP, there are some ways you can fake IP addresses, I think it is reasonably secure particularly if we remind people they need to do logging and look for stuff that looks weird but they do that now.

Greg Aaron: This is Greg Aaron. May I?

Susan Kawaguchi: Sure.

Fabricio Vayra: Sure. We have Rod in the queue and then Greg, could you go after Rod?

Greg Aaron: Sure.

Fabricio Vayra: Rod.

Rod Rasmussen: I will defer to Greg because I'm sure he's about to say the same thing I was about to.

Fabricio Vayra: Greg, go for it.

Greg Aaron: Okay. Yes, the anti-phishing working group has just sent out some comments yesterday which talk about this access method. Go Daddy, for example, already has this exact solution in place. If you're an anonymous user and you query their Port 43 server, they will give you a thin record without the contact data. But if you're an authorized recognized IP address, they will give you a thick response which contains the contact data.

So they already have this in place; it's been running since January and of course that represents a chunk of the Com and Net data out there. So as Vicky – or Susan said, this is a technology that some people have…

((Crosstalk))

Greg Aaron: Un momento. And if others could be using it it's not terribly difficult to do perhaps. And this would provide a short term solution, I think longer term everyone could probably agree that we need to deploy RDAP and then with that have a more sophisticated credentialing system that provides user names and passwords for authenticated users that can be recognized at every registry or registrar that's running a Port 43 server. That longer term solution of course is going to take at least a year to design and implement, maybe more. And so this short term solution is really needed and this is one interesting option. Thanks.

Fabricio Vayra: Great, really appreciate that, Greg.

Susan Kawaguchi: And did Rod have a comment?

Rod Rasmussen: No, I was going to bring up the same exact thing.

Susan Kawaguchi: So it seems that maybe we should all get together, those interested, and talk a little bit more about how this could work in a temporary – as a temporary solution.

Rod Rasmussen: And let me add my emphasis – this is Rod Rasmussen again – my emphasis. This is a temporary as in really temporary, we see the end of life of this solution, not the oh it's the temporary solution that will become the permanent

solution, no, we are definitely – we have to move to RDAP, it's the only way to do any sort of long term authentication model. This is what I would call a stop gap solution in order to, you know, bridge the gap between where we have complete public access today and we have a fully thought out model that we should have been working on years ago and we'll plug that the EWG reported this out four years ago just for example, so that we can – we can have access to some of this data to people who have been authorized, credentialed, etcetera.

I would also note the access method needs to be – think about separately from the accreditation so access and accreditation are not equal things, they are two separate parts of a larger system. Thanks.

Susan Kawaguchi: Right. So appreciate all the comments and I'll hand this back to you, Fab.

Fabricio Vayra: And I'm going to hand it offer to Brian and Steve to do closing.

Brian Winterfeldt: Great. Thank you so much, Fab, Susan, excellent job. Thank you so much. Love a practical and hopefully easily implementable solution and hopefully others can join Susan in working on getting that together. First I'm wondering if – we had asked at the beginning of the call if any of the folks who were only dialed into the meeting if you could please identify yourselves for transcription purposes? All right if you're not able to participate orally…

((Crosstalk))

Brian Winterfeldt: Thank you. Anyone else?

((Crosstalk))

Dale Nelson: …from Warner Brothers. Sorry, Dale Nelson from Warner Brothers.

Brian Winterfeldt: Thank you. Dale. And I think there was one other person trying to identify themselves.

Chris Wilson: Hey, Brian, it's Chris Wilson from Amazon.

Brian Winterfeldt: Great, Chris. Thank you so much. For anyone else, if you could please email back to staff and just give them your name and organization we'd be very appreciative. We are trying to track who's participating for purposes of just keeping everything transparent and we want to thank everyone again for their participation.

Want to talk briefly about next steps. We will incorporate feedback and comments from today's call and we should be expecting a version 1.4 of the proposed accreditation and access model including the comparative redline and table of changes. I think our hope is you'd like to have your comments incorporated into version 4 is that you could get comments emailed by Friday April 13, if possible, otherwise of course we'll continue to take comments but it may not make version 4, if you aren't able to meet that deadline. Of course we're mindful of the fact that there may be forthcoming DPA advice that may be input into this and we will obviously be planning to incorporate that as we move forward in this work as well.

And we note that there's the upcoming Article 29 Working Party plenary meeting next week and everyone is waiting to see what happens there. But obviously we feel it's very urgent that we continue to move forward with this important work and we, again, emphasize that we feel like it's in really everyone's best interest in the community and that's why we're really hoping to have the whole community weigh in as much as possible.

Law enforcement and governments, potentially through or in consultation with the GAC will be working separately to define criteria for law enforcement access to nonpublic Whois data. We are going to work to identify who might draft the contemplated accreditation system terms of service and begin preparing draft terms including specifications and implementation plans. Further clarity and define what data would be provided once a party is accredited and what obligations accredit (unintelligible) data would have with respect to protecting the data. This could be included potentially in the terms of service.

We're also looking for further clarification around aggregation of data including for purposes of historical Whois and reverse Whois queries and we're also looking to further refine technological methodology for implementing accredited credentialed access both for web-based and Port 43 access or identify new protocols that can be implemented as mentioned just recently RDAP or others to accommodate credential requests.

This might include use of the existing RADAR system as Susan just discussed and outlined as a temporary IP address white listing solution that can be processed and managed potentially by ICANN.

Again we really, really thank everyone for joining us today. We do want this to really reflect the broad perceptive of the different parts of the community and we very much look forward to your comments coming in through the email that's been set up and really thank you for all the input on today's call. And I would like to note that there has been a dedicated email address set up by ICANN for this work, if you'd like to join that email address you can email today admin-accred – A-C-C-R-E-D –model@icann.org. Again that's admin – A-D-M-I-N dash accred – A-C-C-R-E-D dash model – M-O-D-E-L

@icann.org you'll be able to add to the list. It's going to be publicly archived so this work will be transparent and open and everyone will be able to keep track.

And I would like to turn it over to Steve for any final comments he has.

Steve DelBianco: Thank you, Brian. It's Steve DelBianco. I wanted to reiterate that the extra set of email comments that we hope to get from all of you on this call in the community are due by the 13th of April. The objective there is to be able to then turn around a new version 1.4 and redlines shortly thereafter. I'll also remind everyone the 13th of April is the scheduled date by which the Board and the GAC are supposed to discuss the GAC advice we saw in San Juan. And that advice while expansive regarding Whois and GDPR, contained three specific elements of GAC advice that are relevant to this accreditation and access.

The GAC specifically said they wanted ensured access to Whois including nonpublic data for users with legitimate purpose until such time that the interim model is fully operational and mandatory. And Number 5, the GAC said, to ensure that limitations on query volume that might be envisaged under an accreditation program would balance realistic investigatory and cross referencing these. And then finally the GAC said to ensure the confidentiality of Whois queries by law enforcement agencies who are doing Port 43.

So I bring this to everyone's attention because right now ICANN Org is pitching its interim model to the DPAs and they have specifically asked for guidance from the DPAs or a moratorium on enforcement, that's what those letters asked for. Those particular elements are going to come back from the DPAs at the same time the Board is supposed to be considering GAC advice and they're scheduled to do so first on April 13 when they talk together and

then on the 13th of May would be the first time the Board actually comes together to adopt the scorecard on what they're going to do with GAC advice. I'm alerting everyone to the notion that we are going to see a clash of priorities from governments, those in the GAC and those at the DPAs, and it's so important for us to move ahead on accreditation model with the full visibility of what the parties who are asking for changes are looking for.

So thanks, like Brian said, thanks to staff and thanks to everyone on this call for such a cordial and constructive atmosphere and environment that you conjured on the call and appreciate all of that and look forward to our next interaction.

END