Registrar Accreditation Agreement (RAA) DT
Sub Team B
TRANSCRIPTION
Thursday 03 December at 17:00 UTC

Note: The following is the output of transcribing from an audio recording of Registrar Accreditation Agreement (RAA) drafting team Sub Team B meeting on Thursday 03 December 2009, at 17:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
http://gnso.icann.org/calendar/index.html#dec
http://audio.icann.org/gnso/gnso-raa-20091203.mp3

Present for the teleconference:
Steve Metalitz - IPC – Chair
Tatyana Khramtsova – Registrar Stakeholder Group
Michele Neylon – Registrar Stakeholder Group
Tim Ruiz - Registrar Stakeholder Group
Marc Trachtenberg – IPC
Kristina Rosette - IPC
Mike Rodenbaugh – CBUC
Cheryl Langdon-Orr - ALAC chair
Holly Raiche – At-Large
Danny Younger - At large

Guest Presenter
Bobby Flaim

ICANN Staff
Margie Milam
Heidi Ullrich
David Giza
Liz Gasster
Glen de Saint Géry

Absent apologies:
Avri Doria – NCSG

Coordinator: Recorder is now recording. Please go ahead.

Steve Metalitz: Okay. Thank you. Good morning, afternoon or evening everybody. This is Steve Metalitz and welcome to the RAA Sub Team B call. Perhaps we could have a roll call if staff could let us know who's on the phone.

Glen DeSaintgery: Certainly Steve. This is Glen.

Steve Metalitz: Hi Glen.

Glen DeSaintgery: We have on the call Cheryl Langdon-Orr, Holly Raiche, Tatyana Khramtsova, Steve Metalitz, Michele Neylon, Mike Rodenbach, Mark Trachtenberg. And for staff we have Margie Milam, Liz Gasster, Heidi Ullrich and David Giza and Glen DeSaintgery, myself. Thank you Steve. Back to you.

Steve Metalitz: Thank you very much. Now I understand that our guests (Bobby Flame) will be arriving a few minutes later. And that's the first item listed on our agenda. And then the second item - he's going to be presenting on this law enforcement list of recommended RAA amendments and responding to questions because there were some questions on our last call.

Then our second agenda item is to review the consolidated list and as I understand, it has just been circulated. So when we get to that point, maybe we can get that document up on the - on the screen but I think it just arrived - I got it about one minute ago.

So that's - the next item we have listed on the agenda.

Woman: Steve, would you like (to) pull it up right now and walk you through briefly what we...

Steve Metalitz: Before we do that, let me just see if there are any other agenda items that we want to include. I know Holly had - sent us - sent around a very detailed set of reactions to the - to the earlier version of the list and Holly, I don't know if you wanted to walk through that or have any discussion on those. I don't think there was any discussion online about those.

Holly Raiche: No. I don't think so. Why don't we just wait until we get through the two agenda items that are already listed?

Steve Metalitz: Okay.

(Bobby Flame): Hi. It's (Bobby Flame). I'm here.

Steve Metalitz: Hi (Bobby). Welcome.

(Bobby Flame): How are you?

Steve Metalitz: Steve Metalitz and we've got a number of other members of our - of our Sub Team here.

(Bobby Flame): Okay.

Steve Metalitz: So Holly, we'll just make that item to be, if you will.

Holly Raiche: That's fine.

Steve Metalitz: And then I think with (Bobby) here, we can - we can get started on Agenda Item Number 1. Are there any other agenda items that anybody wanted to add? If not, then we'll - maybe we'll go to Number 1.

(Bobby), as you know, we've been looking on this Sub Team at a consolidated list of topics for possible amendment to the RAA. And there were some questions that arose during our last discussion about some of those that were drawn from your document, which is now up on the screen in the Adobe Connect room so we can all see the law enforcement recommendations.

(Bobby Flame): Okay.

Steve Metalitz: It might be - if you - I guess one way to do this would be for you to simply walk through this document and then people can ask questions as they - as they arise. Or if there are any other - if there are particular questions that people on the call have right now, we could - we could move around the document.

But since we have the document up there for those who are on the - in the Adobe Connect room and (Bobby), I don't know if you have it in front of you.

(Bobby Flame): I have - I have my document in front of me. I don't have it on the Adobe Connect room.

Steve Metalitz: Okay.

(Bobby Flame): But I have my document in front of me. I have the short version and then the long version which you have both and I think what you did on your list was you took out parts from the long version and broke it up into the different subject matters.

I don't have that in front of me but I have read it and seen it. So what I have in front of me is the original document that I gave you at the ICANN meeting in Seoul.

Steve Metalitz: Okay.

(Bobby Flame): So if you want me to go through that, the long version step by step, I can certainly do that.

Steve Metalitz: Yes. Unless people have another suggestion about how to proceed, I think that makes sense. Go through this detailed version document and then I think people could just raise questions as we go along if there's something that you have in there that they don't understand or have a question about. That'd probably be the best way to proceed.

(Bobby Flame): Okay.

Steve Metalitz: So why don't - the ball's in - I'll pass the baton to you and why don't you start in on this document.

(Bobby Flame): Okay. Sure. Just so you know the genesis, obviously we've been - we've started to come together as a law enforcement group, principally the United States, Great Britain, Australia and New Zealand. But we've also worked with a lot of other law enforcement agencies from Spain, from France, from Korea, Japan.

And we wanted to come up with a document where we would be a part of the process certainly within GAC and also within the GNSO and also within this working group.

So we kind of drafted things based on what was already out there. And some things we added original to ourselves. So some of you - some of it - some of this document is actually things that came from the Anti-Phishing Working Group, some came from ICANN documents, the (SBAC) abuse document.

And that - all the ideas that have been (stolen) per se have been documented or footnoted so that you know where they - where they came from. Right now, as you can see, this has been supported by five different international law enforcement agencies but its also been supported by the G8 cyber working group as well.

And also it has been presented at Interpol, the cyber working group and it has received support there. On the (G8) level, they're actually seeing a ministerial approval letter or support letter for this that would - that would go forward.

So that's kind of a little bit of the background. Now insofar as the document itself, I have one proposed amendment to the RAA. And you'll see that this

document is actually broken into two. One is very specific to the RAA and then the second portion really relates more to what ICANN can do insofar as going forward in their due diligence with registrars and registries.

So I would just focus on the first part of the document, which is the proposed amendment to the RAA. The first - the first paragraph there is - concerns the proxy registrations and privacy services which we as law enforcement - I know this is a very touchy issue and even within law enforcement we don't agree.

From the United States perspective, we don't like them. It goes against what has been written in the JPA and the affirmation of commitments. But British and European counterparts recognized the need for privacy. Obviously the Untied States recognizes a need for privacy.

But what we had done there is kind of an amalgamation of our two points of view, which is that the RAA shouldn't condone or explicitly mention proxy registration and proxy services, which they do do.

Now insofar as preceding that it's a fact of life, proxy and privacy registrations, we wanted to make sure that if registrars or any other companies offers that service that they go through the same due diligence and accreditation process that ICANN either currently does or should do pursuant to the second part of this document going forward.

Now realizing that some of the registrars are already accredited and therefore it might be slightly redundant but that should be clearly annotated that they are providing that services and that they are accredited.

Let's see. Registrants using proxy privacy services will be authentic who has information immediately published. In other words, Part B, 1B refers to if any of these privacy or proxy registrations are being used for criminal purposes or fraudulent purposes then that information would automatically be published.

I can go straight to two.

Steve Metalitz: Well, before we go on, let me just see if there's any questions on Point 1 dealing with proxy privacy registrations. Any questions.

((Crosstalk))

Holly Raiche: Just a comment.

Steve Metalitz: I'm sorry. Who was - who wanted to be - who asked for recognition?

Holly Raiche: Holly Raiche.

Steve Metalitz: Holly. Anybody else?

Michele Neylon: Michele.

Steve Metalitz: Michele. Anybody else?

Mark Trachtenberg: Mark.

Steve Metalitz: Mark. Holly, why don't you - why don't you go first?

Holly Raiche: Just a comment from the last meeting which is an additional suggestion appears to have been that proxy will only be available for individuals and not companies. Had this been considered by the law enforcement agency?

(Bobby Flame): Yes. And I think it's actually in there.

Holly Raiche: Okay.

(Bobby Flame): That and I was told by one American that is more of a European view but I would agree with that. Again, we're going to have some differences of opinion but I would agree that if we're looking to protect the privacy of individuals, then - and some others have mentioned the privacy of certain human rights groups which is certainly a valid point that they should be the only ones that are granted proxy or privacy registration if we are going to base it on the privacy principles.

((Crosstalk))

Holly Raiche: Okay. That would - that would raise more issues about how you'd determine what a human rights organization, et cetera. But...

((Crosstalk))

(Bobby Flame): I agree - I agree. I'm not - and I'm not saying I support that. I'm just saying that that's something that's out there. I think it would be more logical or rational that, you know, if we're talking about the privacy of (individual), then that would be something that should be explored.

Another question obviously that's going to be raised is how do you ascertain who is an actual private individual not engaging in commercial activity. And that's, you know, something that needs to be answered and how that would be accomplished is obviously another detail that needs to be worked out.

Holly Raiche: Thank you.

Steve Metalitz: Okay. Thank you. Michele.

Michele Neylon: Yes. (Bobby), the question I have is in relation to the privacy and WHOIS and all that. And what is law enforcement's feelings on the way (dartel) has implemented this where a private individual cannot go to WHOIS and yet on

law enforcements do have access to the - to the data and through a - through a proper channel with the registry.

(Bobby Flame): Well, that's a double edged sword because obviously what we are trying to do as law enforcement is to make sure that we can combat criminality as fast as possible and prevent it. Now, what happens that - and this has been spoken about a lot of times. The CRIPS IRIS protocols have been mentioned where we'd have tiered access.

And on its face in theory, law enforcement supports that. But the question becomes is who's law enforcement? The United States has 22,000 law enforcement agencies. Who's going to have access to that?

Now insofar as the Telnic issue, that's the British company. And although the British law enforcement may have easy access to that, how does international law enforcement have access to that which is - which is a huge problem?

So in theory things of that nature, law enforcement would like but in practice it really doesn't work. Because once you have it where you're just giving it to just law enforcement or even a national law enforcement, it may be good.

But then it relies on personal relationships. It relies on very structured, very structured organizations and the right people. And as we know in the Internet things are constantly changing. People are moving in and out. So it makes it difficult.

The other problem that we have for law enforcement is that if you only grant law enforcement access to certain WHOIS and privacy databases, it excludes a lot of the other industries in which we work. Intellectual property, the banking industry is a huge one.

And if they don't have access to that where they can do their own investigations, internal investigations, and do civil litigation and civil investigations, then that means they're going to come to us with all of that work and to be honest with you, we simply don't have the manpower for that.

So although in theory some of this sounds good and we support it from a very selfish reason that anyone wants to give law enforcement access to, you know, private WHOIS, in the long run we don't know if it's actually beneficial.

Michele Neylon: Well just one follow-up comment (Bobby). I mean if I was going to register a domain name in order to commit a serious crime, do you honestly believe that I'm going to provide valid WHOIS details?

(Bobby Flame): No. Absolutely not. I mean not if you have half a brain. And that's why the other part of this document is incumbent that we actually make some type of honest effort to validate that data in the first place.

Now I know a lot of people are going to scream about that, that how's it going to be done? It's going to cost money. And those are all valid points. But the point is that it has to be done because we're seeing that a lot of criminality in the open WHOIS and also proxy and private WHOIS; it's not just the open WHOIS, is occurring through bad registration, phishing, farming, fast flux, child pornography, botnets, you name it, is being a curse to this and we need to take more preventative measures as opposed to reactive measures.

So I totally agree with that statement but we have to start somewhere and, you know, that's why I'm glad we're engaging in this discussion to see how we can proceed further.

Steve Metalitz: Okay. Mark I think was next in queue.

Mark Trachtenberg: Right. I have some questions about 1A and B and I'll start with A. I'm just kind of wondering how from a practical perspective, you know, A might

actually work where registrars accept privacy or proxy registrations only from ICANN accredited proxy registration services.

While of course you have nothing in principle against, you know, the accreditation or proxy registration services, you know, how would the - how would the registrar ever know whether it was a proxy or privacy registration service? Because anybody can, you know, register a domain name; any person or company.

And then, you know, license out that domain name to another person. So I mean would you contemplate prohibiting any licensing of domain names or I mean how would that work?

(Bobby Flame): You know, that's an excellent question because there's always back doors to everything that you put in place. And that is a one huge back door where there's a lot of intellectual property people. There's a lot of lawyers that actually are de facto proxies for their clients and for their companies.

So that's an issue that also needs to be explored. And to be honest with you law enforcement hasn't explored that yet and it needs to be explored. Whether you ban it so that an agent cannot set up a domain name for a client, you know, I don't know. I don't have an answer for that but it is a legitimate question and point that needs to be looked at and is not addressed in here. But I think at some point it will have to be.

Mark Trachtenberg: Right. I just can't see from a practical perspective how could it possibly be workable but I mean that aside I guess. And for B, you know, I have several questions I guess.

You know, the first question is that you start by saying registrants using a privacy or proxy registration service will have authentic WHOIS information immediately published by the registrar when the registrar is found to be

violating terms of service including but not limited to use of false data, et cetera.

So I mean how would the registrar have access to that WHOIS information if it's registered through a proxy service? Are you contemplating that the proxy would have to also provide the beneficial owners with information to the registrar when registering it? Or would the registrar have to request it from the proxy service and then how would they - why would the proxy service give it to them? I'm not sure how that would work.

And then, you know, my kind of second related question is, you know, one of the circumstances that would (trigger) the immediate disclosure is when the registrant is found to use false data. I just don't know how that would ever apply because the registration is done through a proxy.

(Bobby Flame): Right. No. I think the theory behind this one is that we don't want people hiding under proxies that are engaged in that particular, excuse me, activity. Now obviously your points are well taken and how that would work insofar as how is that information reported to the registrar. What type of information will they have?

And, you know, from the law enforcement's perspective and even my, you know, FBI perspective, it would be that yes, they would have to report that information and there might have to be some structural changes on how that is reported so that if we do run to this situation, you will have the right data, you know, being published.

But that being said, if you're a criminal, obviously even if you're using proxy information, it's going to be fraudulent information.

((Crosstalk))

(Bobby Flame): So how do you...

Mark Trachtenberg: I think you run into the same problem you have with A which is - so let's say you create a system where the registrars have to have access to this other information as well. So that means that in every situation they have to identify A, when a proxy is used.

(Bobby Flame): Right.

Mark Trachtenberg: And then B, they have to build into their entire system a whole other database of additional contact information that's stored. Which from both perspectives seems kind of unworkable.

(Bobby Flame): Well, I mean I certainly take your point. But like I said, I don't - I think we have to start making some steps to tackle the problem because I think it's becoming a very big problem. I know that - I know that I have spoken to all my field office and it is a truly growing, growing problem and becoming a true menace.

((Crosstalk))

Mark Trachtenberg: I mean I could - I could not agree with you more - I could not agree with you more about the magnitude of the problem. And we definitely encounter it on an everyday basis. So I would love to find a way to solve the problem.

(Bobby Flame): Well then if you find - I mean this is our principles. This is what we want to do. And that's why we want to work with industry. You don't want to take a, you know, a sledgehammer to a very delicate problem. That's why we're putting these things out there, what we need to do. But there has to be some solutions. And, you know, are we going to get everything we want? I'm sure that we will not. But we have to start somewhere.

I mean we have to start putting things in place and we have to realize that there's going to be a cost and some people are going to be uncomfortable

and I think the bottom line is that we're probably going to have to either go to ICANN that they're going to have to absorb the cost as part of their due diligence in how they want to run a safe and secure Internet or it's going to be half the - it's going to automatically have to be passed across the board to all the customers who want to have a domain name.

You know, if we want safe and secure things, you know, there's going to be a price to them. So I mean I totally understand everyone's point but we have to - we have to do something.

Steve Metalitz: Let me just see if there are any other questions about 1A or 1B.

Michele Neylon: Steve, do you mind if I just come back to Mark on one thing there please.

Steve Metalitz: Yes. Go ahead Michele.

Michele Neylon: It's just I'm a little bit confused. My understanding is that most registrars - now obviously I cannot speak for all registrars. But any registrar that I've every had any dealings with is collecting the real - the real data - real data as in the data that to be best of their knowledge is factual and correct with regards to contact details of the registrant and that the registrant opts in to WHOIS privacy service.

((Crosstalk))

Mark Trachtenberg: ...Michele, that's only in a situation where the privacy service is being operated by the registrar. There's an increasing - there's a proliferation of third party, you know, proxy and privacy services which are not operated by the registrar and even the registrars are increasingly divesting themselves of those businesses.

Michele Neylon: Okay. Well then that's where we would need to come in and make sure that there's a marrying of those - of those two in some way that we're not going to

have third party proxy services or proxy companies that are off, you know, making, you know, offering these services or going off into left field and we're not marrying that data to make sure that it's all being ascertained. So...

((Crosstalk))

Mark Trachtenberg: Right. And again I mean I think the problem is like I just can't see - while I would find that incredibly desirable, I don't see any practical way that that could really be accomplished unless you were to completely prohibit, you know, the licensing of domain names to third parties or prohibit the registration of a domain name by anybody except the user.

Steve Metalitz: Well I'm sure there's a lot of other ways to approach it and we're not negotiating a contract provision. Let me just see if Michele has made his point or has finished his question.

Michele Neylon: I think I'll take this up wit Mark directly I think because I'm just looking for some clarification from Mark. Mark, you've got my contact details anyway. So if you could ping me, I'd appreciate it.

Mark Trachtenberg: Sure.

Steve Metalitz: Okay. Are there - if there are no other questions on 1A and B, I'm sure there are others because there's a lot to talk about there and a number of other suggestions have been made along...

((Crosstalk))

Steve Metalitz: Pardon me.

((Crosstalk))

Margin Milam: Yes. I had my hand up because I think some of this we try to tackle from the staff proposals viewpoint. And one of the things that we through of was although you perhaps can't cover all accreditation, all proxy services, if you do link them to the ones that are offered by a registrar are made available by a registrar, you certainly pick up a larger amount that could be affected by the policy.

So we recognize the concern; the thought that even if you make a step in that direction, it's better than, you know, the no step I guess. And at least that picks up, you know, a fair amount of proxy services. So I was just commenting on that.

Steve Metalitz: I'll just add to that since we're getting into the different proposals here. The IPC proposal was that something like this would apply whenever a proxy or private registration service was offered in connection with registration. So whether it was operated by the - by the registrar or spun off to somebody else if it was operated at the time of registration, it would cover and it wouldn't affect the downstream licensing necessarily.

I'm sorry I missed that hand. Margie Milam two didn't have her hand up but Margie Milam did. So I'm used to that one. Anybody else? Okay. If not, why don't we move on to Item 2. (Bobby).

(Bobby Flame): Okay. Item 2 is very simple. It's just we just - if registrars are aware or should be aware then language should be added to the effect, and this is going directly to 5.3.2.1, that we don't want registrars if they know or they should know.

And when we say know or should know obviously is something that is just so obvious where someone is either have reported to them or they're getting complaints or something is very askew, then that should be, you know, also part of that paragraph.

Steve Metalitz: Okay. Any questions? Number 3.

(Bobby Flame): All accredited registrars must submit to ICANN accurate and (variable the main) - yes. We just in list of (S domains) and some other registrar problems and also in light of the fact that the potential for new registries and registrars out there with the new gTLD process, we just want to make sure that everyone is a legitimate business with a real honest to goodness address where they can be located, where they can be served with legal process if need be no matter where they are in the world and that we know exactly what the structures at so there's no shady business.

Steve Metalitz: I will just say that there's several other proposals kind of along this line - compendium that Margie's put together.

(Bobby Flame): And I think - I don't know if you - but I think three, four, five are kind of all together insofar as we're addressing transparency that we just want to make sure everyone involved as a registry and registrar are legitimate businesses and business people with no criminal records.

You know, we have the right people running these registrars and registries and they've been vetted out. Or that's the second part. But basically that there's a transparency as to who is in charge and where these registrars are.

Steve Metalitz: Okay. Great. Are there any questions on three, four and five that people have?

((Crosstalk))

(Danny): Yes. This is (Danny).

Steve Metalitz: (Danny). Anybody else?

Michele Neylon: Michele.

Steve Metalitz: Michele. Anybody else. Okay (Danny).

Tim Ruiz: Tim.

Steve Metalitz: Okay. Tim. Welcome.

Tim Ruiz: Tim. Yes.

Steve Metalitz: (Danny), Michele, Tim. Let's start on that queue. (Danny).

(Danny): Okay. Thanks. With regard to three, four and five collectively, I would tend to think that in view of the fact that ICANN currently has the registrar accreditation applications they could post them. They could make the non-confidential sections of each application transparent and published and that would pretty much take care of three, four and five at a shot.

Steve Metalitz: Okay. (Bobby), any response to that or...

(Bobby Flame): No. That sounds fine to me. No matter how they get it, it's okay. And yes, that's fine.

Steve Metalitz: Okay. Michele, did you have a question?

Michele Neylon: It wasn't a question. It was just more a simple comment in that I've absolutely no issue with three, four or five. I think it would actually be helpful...

Steve Metalitz: Okay.

Michele Neylon: ...from a registrar perspective as well. I guess technically the - some of the problems we have (as registrars) are related to the issues in three, four and five. So I don't think I would - I can't see there being any issues with those.

Steve Metalitz: Okay. Great. Tim. Tim, did you have a question?

Tim Ruiz: Yes, I guess - yes. Just a - just a comment actually similar that what's already been said that perhaps a lot of that - I mean it might be asked (unintelligible) that need to find its way into an RAA but I think a lot of it has to do with the accreditation process itself that ICANN does and maybe some of that needs to be shored up a little bit or something additional done there.

And then that information could be available from ICANN itself. So I think the majority of it is probably being done where available. And you can - anything major that needs to change really probably needs to change in the accreditation process itself.

(Bobby Flame): Yes. I would agree with that and that's what we try to address in the second part of this document, which doesn't necessarily go to the RAA but goes to ICANN's due diligence in vetting out registrars and registries.

Steve Metalitz: Okay.

Tim Ruiz: Exactly. Thanks.

Steve Metalitz: Great. Thank you. If there are any - aren't any further questions on three, four and five, why don't we move on (Bobby) to Number 6?

(Bobby Flame): Sure. Number 6 is almost a follow up. We just want to make sure that there's no inappropriate activity with registrars and registries insofar as financially or criminally or civilly just to make sure that they're good solid companies that will be able to actually do their job and not be interfered internally or externally with any criminal allegations, criminal charges, bankruptcy, so on and so forth. Civil actions. So that's what Number 6 is.

Steve Metalitz: Okay. Any questions on Number 6?

Michele Neylon: Yes. Michele again.

Steve Metalitz: Michele. Anybody else. Go ahead.

Michele Neylon: I don't really issue with A, B, C, D and E. I can see those as being perfectly understandable. I do have an issue with F. I have a very large issue with F.

(Bobby Flame): Okay. What is it?

Michele Neylon: Well, a civil action. Any company that has more than a couple of hundred clients is probably going to be sued at some point for some reason or other. Whether that - whether that civil action is...

((Crosstalk))

Michele Neylon: ...legitimate or not is neither here nor there. And even if it is legitimate, it could - the legitimacy of the civil action could be simply something like let's say for argument sake one, a supplier - actually here's one. The UPS man tripped and fell on the stairs coming up to my office, which led to them taking a civil action to sue us for damages and loss of earnings.

I honestly don't see how on earth that has any impact whatsoever on the stability of the DNS or law enforcement.

(Bobby Flame): I agree with you. Okay. That's something that we will consider taking out. Especially where we say the - where it should be on a registrar Web site because obviously that is - I agree with you. It's - it is not pertinent.

I think that we may want to tweak the language so that if there are any legal and civil actions that pertain to the business of doing DNS that at least ICANN is aware of it. But I would agree with you that any and all legal and civil actions should number one, certainly not be posted but not necessarily need to be reported.

But I think there should be something in there that if there is a legal and civil action that pertains to them doing business as a registrar and doing DNS functions and registrations and so on, I think there should be some way to capture that information and at least have it available to ICANN at the very least so that they have...

((Crosstalk))

Michele Neylon: I won't disagree with you. I won't disagree with you there. I'm not seeing no problem if it's narrowed down to those functions that are directly related to what we're talking about here because otherwise I mean come one.

(Bobby Flame): No. I agree. I agree. I absolutely agree. That's - like I said, this is - this isn't an iron clad document. It's still a work in progress. So no, that is an excellent people and I've marked that down.

Michele Neylon: Okay.

Steve Metalitz: Anything else? Any other questions on 6. Okay. (Bobby), you want to move on to seven?

(Bobby Flame): Sure. This kind of I guess is along the lines with three, four and five, maybe even - I think we're still along the same vein here insofar as that we just want to make sure that registrars and registries are true businesses that have been truly certified as a business in their country of origin.

Steve Metalitz: Any questions there?

Michele Neylon: Michele again.

Steve Metalitz: Go ahead.

Michele Neylon: Sorry. I seem to have a lot of questions. I apologize. Well actually no I don't.

In the document you have country of operation, which caused a linguistic difficulty for me.

(Bobby Flame): Okay.

Michele Neylon: Because I am by our very nature registrars operate across borders.

(Bobby Flame): Okay. Well, where they're incorporated. I think - and if it's multiple countries, then they would need to put that. I know that everyone is engaged in transnational business. So if you have better language that would make it more clear and succinct, I'm open to that.

Michele Neylon: Well I mean I think if you just swapped operation for origin.

(Bobby Flame): Okay.

Michele Neylon: I'd leave you be. I wouldn't - I wouldn't have anything further on that. I mean if you wanted to expand it to include and any subsidiary offices or anything like that, fine.

(Bobby Flame): Okay.

Michele Neylon: But just country of operation suggests to me that if I sell a dot com to a registrant in Canada, then I automatically have to have some kind of legal entity in Canada and any other country in which I sell domains into which would basically put me and most of my colleagues in the industry out of business.

(Bobby Flame): Okay. Okay. So I totally get it. Maybe we'll make it a little bit more specific and tweak out some of that language.

Michele Neylon: Okay. Thank you.

Steve Metalitz: Okay. Great. Number 8 which I think is a new topic.

(Bobby Flame): Yes. Number 8 deals with third party beneficiaries resellers. We realize in a lot of countries outside of the United States and some of the more western countries that resellers is a big issue. But I think since they are part of the chain, since they are part of the, you know, the food chain, they need to be included.

And we make - we need to make sure that they are held and accountable to all of the provisions that registrars and registrars are so that they cannot - they cannot go off into left field. And I think that's what Number 8 is to make sure that they are included and that they are abiding by all the contractual, legal, technical, all the obligations that are mandated by registrars.

So I think they've kind of been out there and I think it's time that we pull them in and make sure that they are complying with everything everyone else is supposed to comply with.

Steve Metalitz: Okay. I see a question from Tim. One from Michele. Does anybody else want to get in the queue with questions on Item 8? Go ahead Tim.

Tim Ruiz: Yes. I think - first I think some of the - some of this is covered in the new RAA. (Might ask), you know, there might be additional (provisions) that you're looking for. But I think my biggest concern is about the last sentence about all resellers and third party beneficiaries should be listed and reported to ICANN.

First I don't - I'm concerned by what you mean by third party beneficiary. And then the fact that, you know, there are hundreds of thousands probably resellers around the world for registrars and registries. And I'm just concerned about what ICANN would have to do to try to manage and track that.

And especially given that for the most part, you know, the largest percentage of cases resellers will be compliant there are issues and for those small number of issues it seems more that those are dealt with as they come up rather than ICANN trying to somehow keep a database or keep track of tens of thousands or likely hundreds of thousands of reseller entities around the world. I think that's a pretty tall order that's going to be almost impossible to manage.

Steve Metalitz: (Bobby), any response or...

(Bobby Flame): Well, I understand the concern. I really do. But I think I'm just going to have to disagree in the fact that there has to be some mechanism or some reporting mechanism so that we know who they are and they can be tracked. These are people who are engaged in registering domain names and are part of where this information comes in and how it can be tracked, then they need to be accountable or at least someone needs to know who they are.

Now if there are hundreds and thousands of them, then maybe there needs to be less. Maybe there needs to be more stringent requirements on who actually becomes a reseller so that that number can go down. I don't think everyone should be qualified as a reseller just because they want to be.

So I understand what Tim is saying and I understand that it could be a problem. But I still think that it needs to be addressed and that we need to have these resellers brought in.

Insofar as the third party beneficiaries, that's a catchall in case anyone is being left out of the food chain. But I really think that, you know, resellers have become a problem insofar as when either they go under or they disappear or they're not recording information properly. We need to be able to track down who they are and if they are a problem, they need to be, you know, addressed accordingly.

Steve Metalitz: Okay.

Tim Ruiz: But I think making registrars responsible, you know, that's one thing. I think the rest of that's pretty difficult. You get into, you know, limiting competition and I just think it's going to be difficult for - when this is actually - you try to negotiate this, I think it's - you need to consider it's going to be difficult to probably come to any kind of agreement on some of those issues. But there just might - I can't see registrars in general agreeing to that as stated.

Steve Metalitz: Michele.

Michele Neylon: Well I've completely - I'd echo absolutely everything that Tim said. And I'd also throw this - throw this at you (Bobby). The problem with - even if (takes blue) and you somehow managed to persuade people to actually sign off on something like this, the problem would simply just move sideways because ultimately all that would happen there then is that people would just register domains to themselves and not - and not declare that they were actually reselling them.

I mean it'd be absolutely impossible to police. Whereas you would stand a much better chance of achieving your goals if you - if you would enforce the RAA on the - on the registrars because ultimately any reseller of gTLDs is doing so through a registrar.

So if you enforce the provisions of the RAA on those registrars, then ultimately you'll have the same thing because under the new RAA it is stated categorically that we as registrars are responsible for our resellers.

I just don't see how - I just do not honestly see how you could - you can think about doing something as broad as this because the situation arises that you're going to end up in a world of pain deciding, you know, what exactly is a reseller and what isn't a reseller.

If I register a domain for my friends down the road, does that make me a reseller? Do - if I register five domains, am I a reseller? Is it 50? Is it 100? You know, where do you draw the line? And so I see that as terribly problematic where I think to achieve your end goal you would be better off focusing on enforcing provisions of the RAA and on those of us who are actually party to it directly.

(Bobby Flame): Okay. No. That's good. Those are valid points because I think for us the whole - the whole - the whole point of this exercise is the end game, which is to prevent criminality from the very beginning and to be able to react to it appropriately when it does occur.

So if the proper place is with the registrars and dealing directly with the registrars to make sure that that's where everything needs to occur, then that is fine by us. We have no dog in the race insofar as going after any particular party, any particular company. We just want to make sure that things are very uniform, they're very equitable and we know how to, like I said, prevent it if it - before it even occurs.

But if it does occur, exactly who do we have to go to and how quickly and accurately can we get the information that we need? So those are valid points. And, you know, if that's how, you know, you and the industry feel it is going to work best, then we will defer to you. But just know that that's, you know, what our end game is.

Michele Neylon: Mind if I just come back and - I mean I fully understand where this is coming from. I can understand the sentiments. I just think that the problem - the problem is best addressed by enforcing the RAA on the registrars, not trying to throw cast this massive net out because ultimate to do that, you know, the bigger the net gets, the more fish get through. So, you know...

(Bobby Flame): Okay. Okay. No. Good point.

Steve Metalitz: Okay. Let's - if we can, let's move on to Item 9 and 10 about the data that the registrar is required to collect and maintain and validate.

(Bobby Flame): Okay. Well I know this is going to be a contentious issue because I know a lot of the registrars and whoever else will collect this information; I know it's going to be certainly an issue.

And we got a lot of this information based on the recommendations of the Anti-Phishing Workgroup. There's a lot of things that were taken out of what they actually had recommended based on some conversations with some registrars and a lot of registries as simply unworkable what was in that original document. They were not feasible.

So we tried to keep it to what we thought was the most feasible aspects of what is collected and how it's validated or not how it's validated but what's validated.

And in a nutshell, we just want to make sure that whenever anyone, company, whatever registrars - registers a domain name that you are dealing with the person who says you are dealing with.

Now is that going to be 100%? Absolutely not. Is it going to be an easy process? Absolutely not. Is it going to be a free process? Absolutely not. But we need to start somewhere. This needs to be done. And we also recognize that there's also a lot of registrars who actually are currently doing that.

So this is to set a bottom line, a standard practice so that we can try to prevent and eliminate a lot of the fraud that's already, you know, currently going on. So that's why you're going to see the different categories. I'm not going to go through each and every one of them.

But just so you see what they are and what the premise is, what the rationale is behind them. So if you have any questions, comments, tomatoes.

Steve Metalitz: Okay. And so taking together 9 and 10, I guess - is it correct. Nine is what needs to be collected...

(Bobby Flame): Correct.

Steve Metalitz: ...and maintained. Ten is what would need to be validated.

(Bobby Flame): Correct.

Steve Metalitz: And again I think you pointed out that's drawn from the best practices recommendations for registrars from the Anti-Phishing working group.

(Bobby Flame): Right. Drawn and edited down.

Steve Metalitz: Okay. Questions or comments on 9 or 10?

Michele Neylon: Me again.

Steve Metalitz: Michele. Anybody else?

Tim Ruiz: Yes. Tim as well.

Steve Metalitz: Tim. Anybody else?

(Danny): (Danny).

Steve Metalitz: (Danny). Okay. Go ahead Michele.

Michele Neylon: No. I think that we might - there might be some disagreement on the exact kind of wish list of data that is collected. But I don't have any issue with the

(spirit of it) for the simple reason that as (Bobby) probably knows, and is very aware of, the Visa, Master Card and the others are tightening up a lot on the PCI side of things for anybody who does cardholder not present transactions which would basically be most registrars.

So I mean most - I think most of the larger registrars we would be PCI compliant anyway. We have to be because of the - because of what we do. I think there might be a certain degree of disagreement in with regards to the technical HTTP data and everything else that is - that is collected.

It also doesn't state for how long you want us to hold the data, which is another problem. But I mean the general kind of thrust of what you're trying to achieve in those sections I don't really have any issue with because ultimately every time I get a charge back, it causes me a headache. So I don't have any problems with it.

(Bobby Flame): Okay. No. And I agree. I mean there's certainly again work in progress in some of these things, some of the specifics can certainly be tweaked out and need to be tweaked out.

Steve Metalitz: Okay. Tim.

Tim Ruiz: Yes. I just had a question in regards to 10.1A. (Unintelligible) used to register domain names and what was intended there as far as validating that. Again, maybe not how but what's the - what's the end game I guess in doing that?

(Bobby Flame): Right. Well, part of it is as, you know - we are well aware that IP addresses if you really truly want to validate them, there is not true way to validate them because you can have an IP address from a company, a legitimate company, that says they're in Boston but really the server where they're operating from, Los Angeles. So that is duly considered.

But what we are trying to do is eliminate the most obvious frauds. And also I'm not even - those are legitimate - illegitimate obviously can use proxy servers and do, you know, hack into sites and go from there. So that again being considered.

But some of the things that possibly could be done, when I say validate an IP address, not validated in a vacuum but validated insofar as you're matching it with a physical address, a telephone number, a time zone, things of that nature.

So again, maybe work on the specifics. It's just one thing to look at insofar as validating the data with the realization that it is not perfect and people can certainly circumvent a true IP address from where they're coming from.

Steve Metalitz: Okay. Thank you. (Danny), I think you were next.

(Danny): Thank you. (Bobby), I just had a question regarding the timeframe for the data retention. Do European counterparts have any particular views on that that we need to be aware of?

(Bobby Flame): You know, they have not come to me with anything. I know that they have data retention laws. I believe it's for one year. The United States I believe doesn't have any. But I think there's something RAA, three months. Is that correct? Am I - I don't know. Okay.

But no, we have not - we have not discussed that and that's, you know, something that certainly should be discussed and put forth - you know, put in there.

(Danny): Thank you.

Steve Metalitz: Michele. Go ahead.

Michele Neylon: Yes. Well I'm very, very familiar with the entire data retention thing because we're members of - we're members of (Euro isva) and I've been involved for the last year and a half in the data retention working group here in Ireland. So I know that stuff a bit too well.

The data retention legislation was introduced through a European level and is then being transposed into national law within the 27 member states of the European Union.

Each member state has a certain degree of leeway in how it is transposed into law. But one of the key things is that a lot of personally identifiable information has to be removed and most of the data retention actually refers to email, not HTTP traffic. So in many respects it's not really what you're looking for.

(Bobby Flame): Okay.

Steve Metalitz: Okay. Tatyana had her hand up I believe.

Tatyana Khramtsova: Yes. I have one question regarding credit card billing address. The (unintelligible) that for example in Russia, credit cards are not verification document. And registrars don't (recall of) data for credit cards. We have only passport data. So how can we apply this proposal for our system?

(Bobby Flame): I'm sorry. I just had a little trouble hearing. Can you repeat that or...

Tatyana Khramtsova: Yes. I can repeat. The (unintelligible) for example in Russia...

(Bobby Flame): Yes.

Tatyana Khramtsova: ...credit cards are not document for verification. So our registrars can't recollect data for credit cards of clients.

(Bobby Flame): Okay.

Tatyana Khramtsova: How can - how can apply this proposal for our system?

(Bobby Flame): Okay. So you're saying that credit card information in Russia isn't validated? Did I understand correct?

Tatyana Khramtsova: Yes.

(Bobby Flame): Okay.

Tatyana Khramtsova: Yes. We have only passport data.

(Bobby Flame): Okay. Well then how would someone buy - how would someone buy a registrar or a domain name in Russia?

Tatyana Khramtsova: By wire transfer.

(Bobby Flame): Oh. Wire transfer.

Tatyana Khramtsova: Okay. Well, you know what. That's something that, you know, we did not consider. So how would we validate that? Then I guess that's a good question. We would have to figure out how to do that and how we would validate wire transfers if that's what's...

((Crosstalk))

Tatyana Khramtsova: Okay. Okay. Of course we're trying to provide some services by paying by for example systems like PayPal where our clients can put their data for cards. But we can't recollect as (unintelligible). So we are trying but it isn't - we have only I think 15% of payments by card only for domain name registration.

(Bobby Flame): I'm sorry. What was that percentage?

Tatyana Khramtsova: About 15%.

(Bobby Flame): Fifteen, one five. Okay. Okay. No. That's very good. You know, we have - we've been working through the G8 with the Russian police and they are part of the G8 and they're actually going to support this. So that is something that we can go back to them with and figure out how to validate in that, you know, in Russia.

Tatyana Khramtsova: Okay. Thank you.

Steve Metalitz: Thank you. Thank you very much. We're almost out of time here. So let me ask that we move on to Items 11 and 12 which I think are the last two in this part of - really in the RAA amendments part of your document.

(Bobby Flame): Okay. Well 11 was just taken straight from as you see the (SBAC)s 38 recommendations. So that there's just an identifiable - and abuse contact that is - that is listed should have any - should anyone have any problem. So that's what 11 is.

Steve Metalitz: Any questions on 11? Okay. Why don't you go ahead to 12 then?

(Bobby Flame): Okay, 12 is ICANN requires registrars have a service level agreement for their 43 bulk WHOIS servers. And that's, you know, just a way to make sure we have better information.

Steve Metalitz: So the issue is that too often those servers may not be available.

(Bobby Flame): Right.

Steve Metalitz: Even though that's an RAA requirement to provide WHOIS via...

(Bobby Flame): Right. Exactly.

Steve Metalitz: (All right). Any questions on Number 12? Okay. In that case, unless there are any other general questions or final questions for (Bobby) - I know you have - the rest of your document is on due diligence and I think, you know, it's fairly straightforward. It really deals with the accreditation process rather than the - than the RAA itself.

(Bobby Flame): Correct.

Steve Metalitz: And obviously some of these things are also coming up in the discussion on new gTLDs in terms of due diligence on registries. But in - unless there are further questions for (Bobby), I'd certainly like to thank you for taking the time to walk through this and to be - to be on the spot for the entire meeting and responding to the questions.

I think it's been very useful in terms of identifying some areas where there may be problems and issues that need to be explored further and others where there seem to be some level of comfort with dealing with these or at least identifying these as good topics for RAA amendments.

(Bobby Flame): No. I agree. I agree. And thank you for allowing me to go through this. And I think all the comments and questions were extremely useful.

Steve Metalitz: Okay. Great. Well thanks very much (Bobby). Let me just ask in terms of the group, we are now at the end of our hour. We could ask - as I had mentioned right at the beginning of the hour Margie has circulated a new compilation document on all the topics that have been proposed. And none of us have had a chance to review that.

But Margie, did you have anything you wanted to say about that in terms of what people should be looking for as they review that over the next week or so?

Margie Milam: Yes sure. I'll just give you some background and I'll pull it up right now. Basically all I did was take the list - it was - and try to consolidate it into topics. Since I rearranged the topics into categories. And there's about, I don't know, there's about 20 or 18 topics altogether.

So really that's all I - I didn't do any substantive editing other than adding a little more clarity on what the issue was. And so I think you guys should take a look at it.

I did add - (Danny) made a suggestion this week as an additional topic and I included that. But really, you know, you guys look at it and see if there's anything else you want to add. But that's all I did.

Steve Metalitz: Okay. Thank you Margie. Let me encourage everybody to look at that and if they have concerns or questions, maybe circulate those on the list. And thanks Margie for updating this. This is really our basic working document here because it brings together all of the suggestions, law enforcement, from the IPC, from (Danny), from all the sources that weighed in.

Are there any questions about that? The last agenda item that we have here was the comments that Holly sent around I think on Monday. Holly, is there anything you wanted to - I'm sorry we don't really have time to go through these today. Is there anything you wanted to say just to - so to orient people in terms of responding on the list?

Holly Raiche: Just a few things. I think the first issue I raised was a lot of this relies on compliance. And I keep hearing well if this is enforced or if this is enforced. So we're looking at provision. But I think it's a point that both (Doug) and (Danny) raised.

We also should be looking at whether the provisions are actually going to make a difference or whether bad actors are always going to go outside which I think we all believe anyway.

There's a lot in the new RAA agreement that necessarily hasn't come into force yet or is just coming into force on resellers. So I'm wondering if we take another look at whether that's actually working or not.

There's a lot on proxy servers. Obviously this is going to take another whole discussion. And then there are some other issues that were raised by (Danny) and others that actually are just new and big like cybersquatting. What is - you know, what's the definition? It's going to take a long discussion.

So I sort of broke down what the last conference was about and I think at some point we're going to have to have a discussion on compliance. What's in the RAA now on compliance? Because if we are going to put in a whole new range of topics at some point, is it going to make a difference?

And how is it going to make a difference in behavior? And maybe it never will. Because I'm reading on the side that actors always go outside anyway.

Steve Metalitz: Okay. Comments on Holly's - on Holly's statement? This is Steve. I'll put myself in the queue just briefly. I think you've raised some very good points here. I think in terms of compliance, we do have to make sure that, you know, whatever goes in the new RAA has to be enforceable.

So enforceability is certainly a very legitimate topic for our job I think. I would say that the fact that some of these problems could also be addressed in part by improved enforcement of the existing RAA.

I think we have - it's not an either or proposition. We certainly have to be at least from my point of view, we have to be improving enforcement of the existing RAA in parallel with, you know, better clearer provisions. And I think

that's really consistent with what the staff, including the compliance staff, has put forward in the staff notes.

That it's not either or. It's not, you know, see - it's not a question of why adding to the provisions of the RAA if the existing ones are not (being) enforced. I think we have to do both of those things from my perspective and I think from the staff perspective too.

Any other comments? I think we want to come back to this - some of these issues in our next meeting I'm sure. Any other comments at this point? If not, and I know some people have had to - have had to jump off the call because we are over our hour.

Why don't we wrap it up here? We will get a doodle out shortly for our next call, which will include a review of some more of Holly's points and of the document that Margie circulated earlier today unless there's any last comments that people want to make.

I just want to again thank (Bobby) for his time and thank everybody for their questions. And please watch for a doodle for our next meeting within the next - the next two weeks.

Man: Thank you.

Man: Thanks Steve.

Woman: Thank you.

Woman: Thank you. Bye.

Woman: Bye.

END