WHOIS Working Group B "Access"
Teleconference
TRANSCRIPTION
Wednesday 9 May 2007
13:30 UTC

Note: The following is the output of transcribing from an audio recording of the WHOIS Working Group B "Access" teleconference on May 9, 2007, at 13:30 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-audio.icann.org/whois-b-20070509.mp3

http://gnso.icann.org/calendar/#may

Attendance:

Milton Mueller NCUC chair - wg chair

Philip Sheppard - WHOIS wg chair

Carole Bird - observer

Patrick Cain - observer

Bertrand de la Chapelle -observer

Wout de Natris - observer

Avri Doria - NomCom council

David Fares - CBUC

Palmer Hamilton - CBUC

Doug Isenberg - IPC

Susan Kawaguchi - CBUC

Tom Keller - registrar

Dan Krimm - NCUC

John Levine - observer

Leo Longauer - observer

Steve Metalitz - IPC

Margie Milam - Registrar/IPC

Lane Mortensen - observer

Melissa Rotunno - observer

Suzanne Sene - observer

Paul Stahura - registrar

Ken Stubbs - registries

Jay Westerdal - Registrar

Michael Warnecke - observer

ICANN Staff:

Maria Farrell - GNSO Policy Officer

Glen de Saint Géry - GNSO Secretariat

Milton Mueller:	Okay. This is Working Group B, do we want to - for Melody's sake call everybody's name and have them express their presence?

Glen de Saint Géry: Would you like me to go through who is in the call, Milton?

Milton Mueller:	Yes. Why don't you do that Glen with your mellifluous tone, I think it will be nicer than if I do it.

Glen De Saint Géry:We've got Dan Krimm…

Dan Krimm:	Hi.

Glen De Saint Géry:…Palmer Hamilton, Patrick Cain, Philip Sheppard, Carole Bird, yourself Milton, (Melissa Rotuno), Lane Mortensen, (Leo Longauer), (Wout Denatris), Margie Milam, (Tom Keller), Doug Isenberg, Steve Metalitz, Michael Warnecke, and Susan Kawaguchi.

Milton Mueller:	Very good.

		Okay. So, I circulated an agenda. The agenda was…

Coordinator:	Excuse me. David Fares now joins.

Milton Mueller: …that we would - first, approve that agenda. Secondly, we would review the proposals…

Man: Thank you.

Milton Mueller: …third, we would discuss the grouping of the proposals and we would develop action items for the next meeting. Is there any discussion of that agenda?

Coordinator: Excuse me. Avri Doria now joins.

Milton Mueller: Okay. Hearing no discussion, I will assume that you all think that's a good way to proceed. So, we'll move right into the review of the proposal.

                   Does everybody have the compile list that I sent out last night?

Man: Yes.

Man: Yes.

Man: Yes.

Man: Yeah.

Milton Mueller: What we do is we have…

Bertrand de la Chapelle: Hi. This is Bertrand de la Chapelle. Sorry for being late.

Milton Mueller: Hello.

We have seven proposals that I grouped into three different categories and I gave them shorthand names. So, I will take them basically in the order that I listed.

As you know, I grouped them. Basically, it seems to me that the type of legitimate third party that's being contemplated is the main difference between these proposals, and that is what seems to drive the differences and access mechanism. Although there is going to be plenty of room for debate about that once we get through the legitimate third party part.

Anyway, one group really has in mind, basically public law enforcement agencies or in the case of do process proposal at least some kind of gate keeping by public legal process.

Others contemplate some kind of apply for access and anybody basically with a legitimate need would be given access upon application and review.

And then we have a sector-specific proposal that refers only to the needs of one particular industrial sector, the banking industry.

Let's begin with the - of the proposal is - yeah, I see Mr. (Denatris)…

(Denatris): Yes.

Milton Mueller: …on the line. Would you like to quickly run us through the nature of your proposal or would you like somebody else to summarize it…

DeNatris: Yeah, what I would like to clarify is that, we are independence government agency with a mandate only for spam and spyware, and malware enforcement.

So, we don't have any sort of mandate to speak who else should be on this list or should have access. We can basically only speak for ourselves and that narrows our discussion very much to what I have written down and what we basically need is some sort of unlimited access enabled - to be able to fight spammers, and that's what we need.

And with the proposals that we read about a year ago, that would have become - impossible worldwide, maybe in the Netherlands, but we come into so much data which is a broad just to catch Dutch spammer that we need really an easy access.

And that's what we are proposing in trying to find ways to achieve that, so that's just about what my comment - and (all) of these comments are all about.

Thank you.

Milton Mueller: Okay.

Did anybody have any clarifying questions or any kind of - any points about this proposal that are unclear to people that they want to discuss?

Dan Krimm: Milton, this is Dan.

I have one question.

Milton Mueller: Yeah.

Dan Krimm: Under access process and mechanisms there's a reference to bulk access…

Milton Mueller: Uh-huh.

Dan Krimm: …is that - does that mean that you would be able to get a whole set of different registrant information in a single query or just single query across the whole database?

Man: It's last one.

We mentioned (bulk) because we - in some cases, we get into thousands of registrations by the same person and - although I'm not really the one who investigates, I'm the one who's the international liaison for - also on this subject.

My colleagues tell me that, you need to - you're going to have access to sometimes thousands of data in order to get some sort of a pattern where - who this spammer is because their - is their - registration is always full, or usually full for smart ones.

But you can still get it and through mistakes they make in this gigantic string of the Web site they've got running or with data they've got for a possible Web site, so that's what I mean with (bulk).

Milton Mueller: No. By (bulk), you simply mean repeated queries.

Man: Repeated query is very fast in one line.

Milton Mueller: Okay. Now, under ICANN's contractual system (bulk) access, I think it means something different and somebody who is familiar with this can maybe jump in to the discussion here. But…

Woman: Sorry.

Man: Okay. If necessary, I can change it, just tell me what to write and I'll change it too to that term.

Milton Mueller: Okay.

Man: So, please assist me in that. Send me an email. I will make sure that it's changed.

Milton Mueller: Okay.

Margie Milam: Milton, this is Margie. I can explain with (bulk) access.

Milton Mueller: I was going to call on you Margie. Yeah. Why don't - I'm sure you know.

Margie Milam: Okay. Thanks.

                  Yeah. Basically, all the registrars are obligated to provide (bulk) access to the entire - database for a fee and the party has to agree to the contractual terms. So, whatever the limitations are that ICANN require

such as no spam or marketing purposes that's part of the agreement under the (bulk) access.

Milton Mueller: And (bulk) access means that you give them a disk or something that contains the collection of their - the registrars' entire WHOIS records for their entire names under management at a given point in time. Is that right?

Margie Milam: Well, it could be that. It could also be like a password into the system, such as to do queries, I mean it just depends.

Milton Mueller: Uh-huh. Okay. It could mean a password. So, it's kind of password query based is what you seemed to be talking about Mr. DeNatris?

DeNatris: I think that that will work if we would get some sort of a code where we could get access to do the database which will probably help as a tremendous (law) as that would probably be (issuing) for all law enforcement agencies.

Milton Mueller: And you would not want that to be registrar by registrar, you want that to be centralized?

DeNatris: I think that would be easiest, but that - if that is possible to arrange, but - because if - you have to go to every registrar around the world, then maybe that will become - impossible to arrange.

Milton Mueller: So, it definitely will be more difficult. I'm not sure if it'll be impossible, but…

DeNatris: It would be time-consuming…

Milton Mueller: Definitely.

DeNatris: …(naming that). And if you can make it easier - because it's - we don't need access for ourselves. We adhere to all privacy rules with the European Union.

So that means that we only go for when we receive complains. And there are actually complains on our Web site which were registered by (NGUs) at the moment that we need access, but not before that.

Man: Milton?

Milton Mueller: Yes?

Man: Yeah. One question I would ask is whether you require the domain - well, if you require only the data for the names or would you like to have some kind of search availabilities that you just type in the name of the holder get out all the names that are belonged to that person (unintelligible) with that name.

Milton Mueller: That was a question for you Mr. DeNatris.

DeNatris: Oh, sorry.

Could you please repeat it again because I heard the name Milton and I've just saw something popup on my screen. Sorry.

Man: It's okay.

The question I have is whether you're looking for normal WHOIS search capabilities we have right now that you just type in the domain name and you get an answer who that person is, or what was the name or whether you're looking for a (run) search capabilities like it - do you type in the name of the person you're looking for and get back all the domain names in each.

DeNatris: I think the last one would definitely help. At this moment, we do not have that ability…

Man: Right. Your opinion - protection laws is one of the things that we would be very hard to accomplish.

DeNatris: At this moment, we will be quite happy with what we have at these days because that helps us to get to the right people to get more information. But then you know where to start looking and on the Internet, you can get a lot of information fast.

And after that, when we need to delve in deeper that's when you start writing - formally writing for information, so then you will get to bank details and that sort of thing.

Man: Right.

((Crosstalk))

DeNatris: So, it's more - it's possible and arrangeable through - the law applicable, and we would certainly be happy to be able to have that sort of extra access. This is not possible, we're happy with (this data closed) and now we - if that will still apply for us.

Milton Mueller: Okay. That's kind of a good segue to the next proposal - on here and we discuss that proposal a little bit last week. But let me just run through it.

I think the main difference between what (blog) proposal and the OPTA proposal is simply that the access mechanism is different. Basically, the (blog) makes it - everything very much like the current system in that - it simply - it delivers the parts that is supposed to be concealed or delivered in an encrypted fashion and only people who have keys can see that information.

Under that proposal OPTA would and other law enforcement agencies if they were certified would get keys and there are some practical questions about how these keys are distributed and who distributes them, they're not fully answered by this proposal.

Are there any questions about this one?

Man: One question.

I think Milton, you've already described the difference between this and the OPTA proposal, my question is also back to - from OPTA, presumably you would have no difficulty and also having a mechanism whereby you could see some of this additional data?

Man: The question is, if we would have a system to get into that?

Man: Yes. I mean, would you - I mean, the second proposal which is coming from a (Google registrar)…

Man: Uh-huh.

Man: …is offering access to law enforcement for both the WHOIS data and
                additional data which could help with identification presumably you
                would welcome that.

Man: Yeah. Of course, we would welcome that.

                The question is more or less, is it - is the data legitimate on the privacy
                laws because if it's not, then we cannot use it in court.

                So, I would not uphold the case, so that means we really have to have
                data which is within this law.

((Crosstalk))

Man: But is the data - sorry.

Man: I understand that should not risk the data that you would get with the
                key would be exactly the same data you're getting now.

Man: Yes. That's what I understand. And it's not - that is if then that would
                help us a lot, if that would remain the way it is. And that opens all the
                ways to the survey investigation.

                And if it's possible to get more on the same query, then it would help.
                But in the end, you need privacy since the data, you have to get
                through formal ways because there's no other way to get at them, so

that will mean banking details, banking transaction. And also (the private) - privacy-related information.

Milton Mueller: Right.

You're talking about a tier that goes way beyond what's in WHOIS and you're talking about getting a customer record from the registrar or the ISP, right?

Man: Right…

Man: Yeah.

Man: …that will be within a formal information request…

((Crosstalk))

Man: Yeah. I think that - I don't the (blog) kind of proposal was contemplating putting that information in the (blog).

Man: No. Right. That's not what we're asking for.

Milton Mueller: No. Everybody understands that.

Man: Okay.

Man: What - I'm curious - I miss this last call. Sorry. I still have two quick comments. I'm not sure what's the OPTA proposal is. I think I know what the (blog) proposal is. That's my first one.

My second one, I just wanted to add to the (blog) proposal which is, if we do the (blog) proposal of site benefit is that, the registrar does not know which part of the law enforcement or even in law enforcement got the information or not.

Whereas, some other methods, the registrar would know. And so therefore, it could, you know, provide the service to registrants saying, "Hey, law enforcement just got your information, pay me $5."

Man: No. That's (Paul).

Man: Yes. Sorry.

Man: Okay.

(Paul): Yeah. It's (Paul).

Man: Glad to have you.

((Crosstalk))

(Paul): Yeah. So based - my comment is, there's a side benefit with the (blog) proposal which is the registrants don't know that the law enforcements as looking at the data which is the benefits of law enforcement I believe…

Man: Uh-huh.

(Paul): …when they do investigation.

And the - and my other comment is, I don't know what the OPTA proposal is.

Man: Okay. The - I think our proposal is very close to your proposal. Of course, you know, once the registrant will know that we're investigating into because then that way it could take also the measures that would take away all the (proofs) that we are trying to find because in the end, if it's a Dutch organization, we're off because that's the only sort of organization we can go at.

We want all their information from the service and everything, but we can only get at them through these steps which are - which we are trying to get from the registrants - the registrar, sorry - and then in the end, we can do all sort of actions in the Netherlands which gets us to find our (proof) and it's from their own computers and service.

That's the very final set. And but if they're warned on forehand because we're looking into the data, then it will be very hard to find any evidence.

Milton Mueller: Right.

Man: Do you understand what I mean?

Milton Mueller: Yeah. But I don't see any fundamental incompatibility between OPTA and (blog).

Man: (Unintelligible) the few other things - well, I mentioned in the email to you - but I will get back to the old question later just saw them on my screen.

Milton Mueller: Okay.

All right, then moving quickly, then to the when this - the due process proposal…

Steve Metalitz: Milton, this is Steve Metalitz.

I had one question about the…

Milton Mueller: Sorry. Yeah, go ahead.

Steve Metalitz: (Paul), your - this turns on certification by Interpol member country National Central Bureaus, and I don't know how those are operate in other countries.

In the United States those only - the only members of those bureaus or federal law enforcement agency. So, how would this accommodate, for example, state or local law enforcement agency is that, I want to get the key to the (blog)?

(Paul):   I don't know.

They would have to get the key somehow either from the federal guys or directly from the registrars, I would assume.

Carole Bird: Can I step in here, Milton. It's Carole Bird.

Milton Mueller: Go ahead.

Ken Stubbs: Put me in the queue too, Milton. It's Ken.

Milton Mueller: All right.

Carole Bird: With regards to Interpol from the (RCMP) perspective, I haven't dealt
                 with them, but we have a colleague that did - that deals with the
                 (RCMP) Interpol group. And I asked the same question trying to better
                 inform myself, if you will.

                 And my understanding is that, any police agency in Canada, so I would
                 assume and maybe it's a bad assumption, but I would assume the
                 same would apply to the United States or any other country that any
                 law enforcement - sorry, police agency would apply to the Interpol
                 group in their country.

                 So in our case, it would be Interpol Ottawa and ask for consideration to
                 have access to whichever database it is that Interpol would (deem)
                 advances investigation.

                 And so that would not preclude any municipal law enforcement or
                 provincial for us which is the same in the state of the state law
                 enforcement from being able to access the information.

                 Now I didn't - I certainly didn't ask the question formally, I was just
                 trying to educate myself, but it sounded like at least from our
                 colleagues that is in the (RCMP) that deals with Interpol, that there is a
                 mechanism for government, police, and law enforcement agency to be
                 recognized by Interpol but that is only for the government one, so that
                 would be what you would call federal state and city wide.

I don't know if that assists, but that was just as I was taking a look at the proposals like I asked a few questions internally and that's the response that I was given.

Milton Mueller: Well, that's good news then. It means that we've been having this conversation about Interpol without anybody actually talking to Interpol. But it sounds like they do have mechanisms that at least roughly correspond to some of the things - the functions that we're talking about here.

Of course, these details would have to be worked out a lot more carefully if we were talking about implementation.

Woman: Let me just clarify there for a moment, Milton. In no way, shape, or form with the discussion I had a request for feedback from Interpol or a commitment or me even putting it forward. I was just trying to educate myself, so…

Milton Mueller: Right.

Woman: …I don't want any misconception there.

Milton Mueller: No, no. None taken. But it's - I mean, you were doing your due diligence and that's good. And it sounds like the initial probe did not produce completely contradictory show-stopping kinds of feedback. So that's why I say, it's good.

(Paul): Right. It's (Paul) again.

I got two more things. Speaking of implementation, I want to point another benefit of (blog) idea is that, implementation is relatively easy because it doesn't require some kind of out of band system, some other systems, some centralized system, something - it doesn't require any of that. It just requires a system we already have called (Port 43 of) WHOIS.

Milton Mueller: Okay.

Man: And I have a question for Ms. (Stalua).

Milton Mueller: (Unintelligible) still holding to.

Man: Okay.

((Crosstalk))

Man: Sorry, Ken.

Man: I'm sorry. Ken, you're in the queue. Go ahead.

Ken Stubbs: Yeah, the only comment that I was going to make is all of us has predicated on - of the assumption that whatever methodology we can develop in the future that ICANN would work diligently to develop some sort of an approach before communicating with the various law enforcement agencies and I think that they have the resources to do this and I mean we've been doing this around now for six years so clearly it's important enough, the governments have recognized this as well as law enforcements.

I would expect cooperation from law enforcement agencies universally on any approach that we take that's practical and I happen to think that - supports does make some sense there so just my two cents worth, thanks.

Milton Mueller: All right, any other questions about the (blog) I'd like to move on?

Man: And just one more please.

Milton Mueller: Okay.

Who is this?

Man: …OPTA.

Milton Mueller: Okay.

Man: In your - the question how are they certified - it's about third parties, what do you mean when you say that private third parties could request the information about a domain from a law enforcement agency?

I would see some privacy-wise trouble there maybe because I don't think that organization like OPTA is even allowed to get this sort of information to a private entity.

Milton Mueller: Right, I think what's intended there is basically when you said that OPTA was complaint-driven. In other words, some of the - a private party comes to you and says, I've been spammed or something then you initiated the investigation.

When you do that investigation I guess I don't know whether you reveal what you find to the private party or not but that's I guess that's a legal question that we should think consider.

Man: Okay, then that is good. But we were sort of we were thinking about reading this because we get of course complaints some private end users or sometimes a company.

I was thinking about companies like Microsoft who to their own investigations and private litigation against spam or spyware - or whatever.

Milton Mueller: Right.

Man: If they will probably need to get access to this sort of information also but there's something that we cannot give to them so I was thinking along that line so there's also private litigation and they should be able to get their information somewhere also but as I said we are independent government agencies so I cannot take it any - point on that if you appreciate what I mean.

Milton Mueller: Definitely so I'm making a note.

Man: Milton, just a comment from another subgroup which may partly assist the discussions on Subgroup C is all about whether or not the distinction to be made of that types of registrants and one option on the discussion is between legal persons and natural person.

In the case of natural persons, of course, it is they who are protected on the data privacy legislation typically whereas legal persons are not so it may be that if indeed such a distinction exists and goes forward that may provide a sub-category in terms of the provision of the information - to a third party for at least a legal persons - natural persons may knew the - a different degree of access.

Milton Mueller: Okay.

Susan Kawaguchi: This is Susan Kawaguchi from eBay. I'm just wondering how practical it would be to go to law enforcement each and every time we need the contact of registrant of the domain name.

We probably look at who is data base the minimum of 3000 times a week and so I know that if I went to my local law enforcement that here I need this information in these 3000 domains, and I need it in a hurry.

Milton Mueller: Yeah and I want to avoid debating the proposals now. I think we're just trying to find out what they are at this point.

Susan Kawaguchi: Okay.

Milton Mueller: So I understand that that would be an issue definitely I know that and if we even get to the apply for access proposals we will be looking at proposals that are designed to, you know, probably more of what you're looking for.

Man: Milton, I just want to point out that it's possible to contact the registry without knowing who they are so you don't have to approach law enforcement to contact registry.

Milton Mueller: Well, okay, no more debate? Let's go on to due process proposal. Wendy is not on the line. She said she couldn't be here so I will run-through this as the best as I understand it.

Basically, Wendy is presuming that OPAC exist and that you have the information that's published by OPAC because you want to go beyond that. You obtain some kind of valid legal request. She corrected me and said that this is not just early law enforcement agency that could be anybody.

So it might belong with the next category but it's simply much more restrictive kind of a process in the sense that you have to go to subpoena, legal process, court orders those kinds of things to get the additional information.

Carole Bird: Milton, can you add Carole to the queue for that one please?

Avri Doria: And Avri.

Milton Mueller: Okay, questions about this proposal again, we're questioning we're not debating.

Carole?

Carole Bird   I don't know but I can form it in the question format that three points come to mind when I look at this and I'm going to speak from a Canadian perspective recognizing though that the law enforcement, the countries likely have the same situation but may be not all law enforcement in all counties.

And what this proposal is talking about is being able to obtain court order. The current information on WHOIS, not the - banking information is what we call in Canada pre-warrant and what that means is it's the information that we do as we begin looking at a situation that will eventually form information we put into a search warrant obtain the banking information or whatever additional information we need from the registrar and, you know, we then go to search a house that that information will be use in that.

So if we are saying obtaining a court order will be required we're saying that law enforcement would not have access to the information currently on the WHOIS publicly available database, not the ones that are currently, you know, not available such as the banking information.

Milton Mueller: Okay, so your point is the information on WHOIS is pre-warrant and therefore does not provide sufficient information for the kinds of court orders contemplated.

Are there any other questions?

Carole Bird: Well there's…

Woman: I had a question.

Carole Bird I'll just…

Milton Mueller: Carole - three points actually, you were not finished, I'm sorry.

Carole Bird No, there's two other points.

In looking for a court order there's two assumptions that are made is that law enforcement agency that's in Country A may request the information from Country B but if the offense is not one that exist in (the laws in) Country B, they won't be able to get that information from the law enforcement in Country B.

And that goes to just such a simple thing as maybe it's against the law here for a non custodial parent to take a child out of the country but in the other country that's not an offense.

So the law enforcement effectively let's say in Country A where it is against the law and the judges are saying, "Go for it and do your investigation." Won't be able to do that investigation and that would apply to anything even as simple as spam.

Spam maybe illegal in certain countries but not in others and the final one is that if there is no mutual legal assistance treaty between two particular countries, then that information won't be - let's say, if Country A doesn't have an assistant treaty with Country B, then Country A can come in at the law enforcement in Country B for that information and the law enforcement from the second country will not be able to provide it.

So it's just - I think there's misconceptions on when court orders can be used and I just wanted to clarify that.

Milton Mueller: Okay, thank you.

So is somebody else in the queue.

Avri Doria: Avri.

Milton Mueller: Avri, go ahead.

Avri Doria: Okay I'll go ahead.

Basically, one question I mean one thing I'm trying to understand. When this particular proposal talks about (falling) to do process is it actually saying that one has to use a court order or is it saying that one has to follow the due process of the location that they're in without judging it but I don't know that it was being quite and specific, at least I didn't understand that that's why that's the question.

I'm being quite as specific as, you know, follow the US type of procedure of court order - to follow the due process chain that is enforced in any particular place.

The other thing I really want to question whether this really is a more restricted notion as you indicated in your presentation, in some sense the fact that it is an avenue that's open to anyone within the due process limitation of the countries within which they are and of course - on them as citizens or entities within their country to get their country to have the right (by their view) access - due process access.

Milton Mueller: All right.

So I think, you're highlighting Avri that this proposal really doesn't rely on national law and that national laws can both be, you know, be very varied across countries as I think Carole and you would agree on that

and we don't really know then the full implications of the due process proposal for access because it would vary from country to country.

Carole Bird: Well Milton, Carole, can I step in again?

Milton Mueller: Okay.

Carole Bird: It comes down to the definition of what you call due process. Too often in the legislation that we currently have and I'm going to assume it's the same everywhere. We use a terminology assuming it means one thing and in different areas it means completely different thing.

For example the term in Canada for having the legal authority, some people will interpret that - you need a court order, in other cases they will say, "Well, the police officer acting in the course of their duties so sometimes it's a simple matter of definition in asking whether when these outdoor actually means due process, that would assist in clarifying I think part of this.

Milton Mueller: Okay we will solicit some information from Wendy.

Man: Milton.

Milton Mueller: Is now - any other questions about this?

(Jay):   Yeah, this is (Jay).

Milton Mueller: Who?

(Jay):   (Jay).

Milton Mueller: Okay, go ahead.

(Jay):   So we're talking with a lot of the law enforcement. They're telling me that a majority of the investigation that law enforcement does is actually done by a private citizen before it actually get to them and that a law enforcement is generally an escalation stuff where, you know, private companies like eBay and Microsoft were actually given majority of the work and then basically pass it on to law enforcement.

So I think the due process proposal maybe…

Milton Mueller: Okay, I think we're - I understand your point. I think we're getting in debating the proposal now and we haven't even explain half of the proposals yet so why don't we move on to the business constituency proposal from David Fares.

This I've group in the class who's saying that basically anybody can be a potential and legitimate third party, you know, David and the data input proposal and both of these are apply for access proposals mention a certification process and definitely involve providing access to a broader range of parties.

Is David on the line still?

David Fares: I am.

Milton Mueller: You are. There you are.

Okay, would you like to - in a minute and a half run-through the essential features of this proposal?

David Fares: Sure.

So the third parties are - is probably defined to include all legitimate third parties as far as I could including those set points in the GACs guidelines and principles.

It is the application process but it's a one-stop-shop certification process that's based on self certification of legitimacy and that companies that only need to submit one single application form.

There'll be a centralized WHOIS database that - it is password-protected. And then the legitimate third parties that only pay for cost incurred is submitting their application with the rest of the cost being incurred by registrars in ICANN in some way.

First order of review Milton, I think I - submitted in half.

Milton Mueller: That was great David. That allows us to ask questions, so I have one.

You talked about a simple application form, the identified legitimate third party, I don't think you're saying simply that somebody would say they're legitimate and that would make them legitimate, would there be some review or - I mean, how would one determine - how would ICANN determine legitimacy?

David Fares: Well, I think that there will be a set of criteria that would be establishing, would have to self-certify that you comply with those

criteria and there could be some sort of export factor review if necessary.

Milton Mueller: Would anybody in the registrar community care to explain about how far we are from the centralized database and how difficult it might be to achieve that, is that a major step or is that simply an integration across database problem?

(Jay): Hi Milton, this is (Jay) again.

So I'm from the registrar constituency but I worked on the WHOIS issue quite a bit. And I would say we're extremely far away from that and that's why we're probably going further away from that in the future, I don't think registrars want to be in a centralized (tools) database.

They want to see us part of the OPAC proposal that registries themselves were very centralize who is -- stop showing us so I don't think that's something that the registrars would be in agreement with.

Milton Mueller: Well, it doesn't so much matter whether they agree with it or not at this point of our discussion. I want to know just the -- is it feasible or are we talking, you know, hugely difficult technical integration processes or are we simply talking about, you know, assuming we could bang the registrars into accepting - are we talking about something that would be implemented…

(Jay): Well, we already have a centralized (tools) database for (picked) registries, so it currently exists in the ICANN model right now if you look at that .org or .info?

Man: Well, that's not actually, it only includes each TLD but it's not one centralized database for all of the TLDs then to answer your question Milton, yes, it would be a real hard topic first to do, it would be expensive and all of the 800 registrars we have right now plus all the big registries would have to work on that, that's very complicated to achieve that.

(Paul):   This is (Paul) speaking and I agree with that. But, you know, I think you also have to look at the purpose of it.

                If the purpose is - mainly the cause or makes sense but if the purpose, you know, if we could accomplish the purpose some other way maybe that other way makes sense.

Milton Mueller: Okay.

Steve Metalitz: Milton, this is Steve Metalitz, could I get in the queue?

Milton Mueller: You are it - there's no queue.

Steve Metalitz: Just picking up on what (Paul) said, I wonder if I could ask David would the same result or similar result occur if they were simply required that each registrar honor the database or excuse me, honor the password that was issued in other words each registrar which - could still retain its own data but it would have to honor the password that was issued by ICANN.

Man: I think that would be a second best option but I think it's something that we could consider Steve.

Milton Mueller: Okay, it's been…

Wout de Natris: This is Wout de Natris from OPTA, could I make one comment?

Milton Mueller: Yes, go ahead.

Wout de Natris: Okay, the numbers of the hundreds of registrars already makes it a very good discussion to try and centralize it I think from our point of view because 800 agreements is a lot to achieve.

Milton Mueller: Okay.

Man: With the (blog) proposal it doesn't have to be centralized because you would have a key.

Wout de Natris: All right, because it gets a centralized key, that's what I mean, get a centralized key in a centralized points where we can register or credit our sales whatever we like to call it, so that would be very, very - considering all the 800 agreements you would have to get otherwise, that's my point.

Milton Mueller: Any other questions about the Applied for Access Proposal? Now, I kind of group this with the (Alvarez) proposal. (Alvarez) did not mention as broad a number of third parties as David did.

However, I think the intent and nature of the proposal was basically the same that there's some kind of a prescription or -- now, - and other question for you David is when you talk about this password do you

mean you get this password once and it's good forever for unlimited usage or is it a specific incident that you're dealing with?

David Fares: No, a more general password that you can use on an ongoing basis Milton.

Milton Mueller: Okay, it's - it would never be revoked or…

David Fares: Well, I think it could possibly be revoked if you - if it's determined that the legitimate third party is using the WHOIS database in a manner inconsistent with, you know, the criteria established.

Man: Well, would this - would the - we have to talk about the criteria, wouldn't we then because, you know…

David Fares: Right, I mean but it wouldn't be for marketing purposes, you know…

Man: Yeah, but could it be, you know, hey, I just want the whole database because I'm a law firm and I, you know, I might need it someday.

David Fares: Yeah, but I mean I think it's somewhat defined by the third parties, right? I mean you say for IP purposes, it would be a law firm using it for IP investigations, for example.

Man: Yeah, my question is can that law firm then download the whole database?

David Fares: Well, I don't - that's not what my proposal was intended to allow.

Man: We should put those in there, that would really help to clarify it.

David Fares: Okay, we can put that in there.

Man: You know, is it - they have to have, you know, the reason to believe that this (name) is entrenching or can I just, you know, download the whole database?

Man: Again.

Man: This is a one shot deal and that…

Milton Mueller: Well, I think you said it was…

Man: How many names can I, you know, query per day, for example?

David Fares: Well, I wouldn't want to put a limit on the number they can but I'm not talking about wholesale data (mining).

Man: Milton.

Milton Mueller: And went after the limit on it.

David Fares: Well, because, you know, I don't know how many investigations the company might undertake in a given date.

eBay said they get 3000 in a certain period, I don't remember what that was but, you know, it's going to depend on the type of company and the types of needs that they have.

We, as a company we don't just have needs or, you know, our network security people use it, MySpace uses it I mean there are whole host of needs that we encounter and how do I know on a given day, how many that's going to be?

Milton Mueller: Okay, so there's no limit, again, we're just clarifying the proposal here and no limit - certification process remains a bit hazy but it's run by ICANN, they get an application form and there is some possibility of (revocation) based on non-compliance with these unspecified criteria.

Is that fair enough?

Man: Yes.

Milton Mueller: Okay. So let's go on to the data input proposal, it's up in here.

Bertrand de la Chapelle: Milton?

Milton Mueller: Yes?

Bertrand de la Chapelle: This is Bertrand de la Chapelle. Just one question to David Fares concerning the potentially the (xplus) review for potentially revoking this organization. Does he consider anything like logging of request or any trace of the request that are being made?

David Fares: I'm sorry Bertrand de la Chapelle, could you repeat that?

Bertrand de la Chapelle: Yeah. In order to facilitate any kind of (xplus) review of the proper use of the accreditation, do you consider any kind of logging of the request or trace of what users have been made…

David Fares: I think we'd have to think of scalability of that. And I mean to think about that more. I mean we wouldn't be using for anything other than legitimate and either - for my companies active. But…

Bertrand de la Chapelle: But you understand that as you adapt the self-declaration mechanism which is a valid mechanism for the proposal, then there's a potential for reviews. So if there's a review afterwards on what can you base the review?

Anthony Harris: I have a comment on that. Tony Harris here.

Milton Mueller: Tony, go ahead.

Anthony Harris: Yeah. I think that's a very good suggestion really because David, basically you could have some method - I don't see the registrar have to put this into operation, but you could have some sort of (exceedingly) you click on the reason you are doing the search, you know, it could be law enforcements or IP infringement or whatever it is.

And that could generate an audit trail which would be basically what was just suggested. You could have to - have that access logged.

And I know I had somebody expressed concern that that could be a scalable problem. But with the speed and memory of current software applications, I hesitate to think that that would be the case.

Man: I got a question too.

Milton Mueller: Okay. Who is that, (Paul)?

(Paul):   This is (Paul).

Milton Mueller: Okay. Let's - are there any other questions on this proposal?

Man: Yes.

(Jay):   Yeah. I'd like to add something after (Paul).

Milton Mueller: Okay. Who are you?

(Jay):   I'm (Jay).

Milton Mueller: (Paul) and (Jay), I'd really like to move on. We're getting close to 10:30.

(Paul):   My quick question is would there be - can't spending any other penalty for bad actors besides just revocation or the password.

Milton Mueller: Clearly that's not part of the proposal. Did you have anything in mind, David for that?

David Fares: I didn't; but I would be happy to hear what others think about it.

Wout de Natris: Very good. This is (Ralph) from OPTA. I think if somebody…

Milton Mueller: Hold on, hold on. We got (Jay) was…

Wout de Natris: Okay, sorry.

(Jay): So, you know I'd like to seeing this proposal that ICANN actually act as the proxy gateway to the registrar because by allowing the registrar to authenticate with the password, we're basically giving credentials to each registrar.

And if there's 800 registrars out there that basically credential problem that everybody's now receiving fees for everybody else. And there's no way of heading a person off essentially unless that proxy goes back to ICANN.

Wout de Natris: Okay.

(Jay): I'd like to see that that part of your proposal says that, you know, ICANN is running the proxy that often the case and then goes - grabs the data from the registrar.

Milton Mueller: Okay.

Man: Good point.

Milton Mueller: One more comment with Mr. DeNatris.

Wout de Natris: Yes, thank you.

First that on the whole database being given out, the honorary request, I think that would be very much against the privacy rule because then you're just data mining and hoping to find something probably.

And then second one is that of there's abuse of the - what do you call the accreditation, the WHOIS service, then somebody's do me something wrong against one law or another.

So it would be able to re-complain to privacy agency or to anti-SPAM agency like OPTA or whoever. And then - and they can investigate and do the complaint and send somebody as probably data mining and of which is (deputy) against the lawyer.

Milton Mueller: Okay. I think that's an important point. David, do you might want to think about in terms of the binary access you're giving total access versus no access, you might want to think about modifying that in the future iteration.

Pat Cain is not on the line.

Patrick Cain: Yes, he is.

Milton Mueller: He is? Oh, good.

Patrick Cain: He's being polite because other people were talking.

Milton Mueller: All right. Maybe too polite. Go ahead. Tell us about your proposal.

Patrick Cain: We actually tried to do a kind of like the certification effort in the antifraud community to keep track of our database of good stuff we have and we've given up on the certification fee.

And so when I was looking at this, I keep hearing people say, "Oh, it's certification organize somebody to certify us although there's really nobody in the world who can certify everybody.

We start to thinking about going it the other way which says, the goal is to privacy protection. Privacy protection is always based on national law more than anything else.

So you use the registrar data, mostly the billing the data just guide how to do their privacy protection that anybody and their brother look at standard WHOIS data if they don't want it.

And we separated the access to the institute pieces. The normal law enforcement is currently doing the investigation. They're going after somebody that uses the standard stuff as it is now. I mean there's (mlock) and there's - court order places or government writ and you talk amongst yourselves…

It's kind of slow. It doesn't work really good but there's treaties in place for it and you can now actually get your data. If you just really want to get this private data from the people and not the entire record but the whole thing, you would go to the OPAC or the person and say, can I please have their data.

And based on most data where the billing address of the person is you decided on the - from the national law.

The goal here is not so much to deal with the happy people but try to figure out how to deal with the bad actors that the people who really

get in touch with who say no, we're not going to do that information. They'll know who I am and I'm taking out.

And with that responsibility to decide what the right thing to do is on the part of the servers which like agency law kind of work to deal with.

Milton Mueller: So you're proposing basically a proxy server, is that right?

Patrick Cain: Well, currently, there is proxy servers, no matter what you call it.

There are numbers of particularly big companies that don't put their home address and their registration. It's a law office some place or if they post off the box in…

Milton Mueller: Yeah, yeah.

Patrick Cain: … there are some (hot items).

Milton Mueller: But what I'm trying to get at is what you're proposing is essentially a - it's more of a working Group A topic than access proposal?

I guess the question would be, what are the conditions under what you get access to the what's behind the proxy?

Patrick Cain: I don't know if I have a concise list of that.

Milton Mueller: What I think - say it almost sounded like the due process proposal in the sense, but it depends on national law and it depends on the registry - legal jurisdiction, is that right?

Patrick Cain: Yes.

Steve Metalitz: Milton, this is Steve Metalitz. Can I get in the queue?

Milton Mueller: Go ahead, yes.

Steve Metalitz: Yeah I think I agree with you Milton that this is kind of Subgroup A
                  question because if - I think when you take that description and just
                  substitute OPAC or proxy, you kind of - you may get something close
                  to what we - some of the things that are being talked about in
                  Subgroup A which really deals with what is the OPAC supposed to do.
                  The OPAC is a gateway to the data and what is the OPAC supposed
                  to do.

                  And I mean it doesn't eliminate the question of certification. It just kind
                  of brings it to another level I think, you know, whether there's
                  certification or not, there has to be some - there may need to be some
                  guideline for what the gatekeeper supposed to do when someone
                  comes in and says I want this information.

Milton Mueller: Okay. Any other questions about this proposal?

(Mike):   Milton, (Mike) from (ESA).

Milton Mueller: Go ahead.

(Mike):   Would there be some sort of mechanism in this proposal to prevent
                  someone from giving a billing address to a jurisdiction that had the
                  most restrictive privacies plus simply as a means of gaming the system
                  when in fact there's not from that jurisdiction?

Patrick Cain: This is Pat. I doubt it because it's really easy to do you fell all the time though.

Avri Doria: This is Avri. Can I comment on that?

Milton Mueller: Go ahead.

Avri Doria: I think that that one then falls into the jurisdictional aspect of each locality. And, you know, that needs to be fixed locality in that case.

For those that object to it, I can't - I don't think any proposal can be totally gaming proof and can assume a heterogeneity - I mean a homogeneity of all the rules and restrictions and possible loopholes for gaming elsewhere.

Milton Mueller: Okay.

Any other questions about data input.

All right. Is Palmer still around?

Palmer Hamilton: I'm here.

Milton Mueller: Take it away, Palmer.

Palmer Hamilton: All right.

Basically professor, I took your standards. I thought for example, David's proposal certainly would take care of our concerns and that's

simply following - thousands flowers - decided that I would do a proposal that was bank specific because that drove much of the fraud on the consumer is through that Internet Web site that use bank names.

And so I was looking at the standard you - out of clear and implement them or definition of legitimate third parties because obviously how we get our arms around that.

It seems to me there are two key questions that we confront, one, the definitional one of determining who the legitimate third parties are and secondly, the process of certifying or authenticating the safety protection that the parties actually are what's defined as legitimate third parties.

Banks seemed to me very easily defined because limited to governmentally chartered banks that the universe, that either in or you're not in and furthermore, the certification and authenticating process begun through the bank regulators so that the burden would not be on the registrar as anyone else and you would have the comfort of billing that the certification was done by neutral governmental entity.

And that's the basic overview and I don't think I should answer any specific questions I could.

Milton Mueller: Okay, any questions about this one?

Margie Milam: Again, this is Margie.

Palmer, what about service writers that service the banking industry as an example companies that provide (anti-fishing) services, you know, a lot of banks go to companies like (unintelligible) and other ones that you have (anti-fishing) related activities, would they be part of proposal?

Palmer Hamilton: That's a good question Margie and we have not discussed it among ourselves, let me call to my folks and see what they think, how that might work.

Man: That, you know, there are a lot of volunteer organization - it's (Paul) speaking again, there are a lot of volunteer organizations like (Spam House) that also, you know, like these kind of things (Spam fishing) and so on.

So, related to that and not just companies but would individuals, you know, follow there the same thing?

Milton Mueller: Was that question was directed to Palmer?

Man: Yes, just like Margie says, she's saying hey, what about other companies that help with (anti-fishing), what about other individuals was my question?

Palmer Hamilton: Well, I guess the same question would apply what sort of access - what sort of information would banks be permitted to share with those who would be working with them to forget the fraud.

I think that it's same question whether it goes to the, you know, mark monitor or an individual who might be working with the banks and I

need those to help and that people would kind of think through how that might work?

Man: I was thinking more of that, the way the information flows. You can't replace information flowing to the bank first and then the individuals or companies that help bank with fraud or would it be…

((Crosstalk))

Man: …under the proposal is written right now, it just (close) the bank and the bank had to maintain the confidentiality of that information.

Man: I understand that. Thanks (Matt). Thank you.

Man: Milton, quite a bit that this is whether a comment on this - going through so far, I think Palmer's proposal which is SEC's specific and therefore benefits from - well, it looks like to be a workable certification process is - similar to the (LEA) proposal they had earlier which had an Interpol process certification process.

And I think those two ideas highlight them the difficulty of the broader group of third parties and the difficulty of the workable certification process for them.

So, I think…

Milton Mueller: Yes.

Man: …that is our ongoing work item in terms of the nature of certification and subsequent access and should have been different for those - I

mean you can have a third party versus those for whom or too much of a heterogeneous subgroup in order to allow certification to work.

Milton Mueller: Exactly, I think that's the big issue that we're dealing with here. And…

Man: Milton?

Milton Mueller: We - that's one of the reasons why in - I was kind of hoping in describing the (blog) proposal, where it says (private) studies could request information from and (LEA), the hope is that there would be a trickle down effect that the private parties who obviously participate in law enforcement either by initiating complains or by actually doing their own investigations would be able to benefit indirectly from law enforcement access.

However, we are out of time - I don't know whether this whole teleconference turns into pumpkin at 10:30 or not but I think we need to skip Item 3 of our agenda and we need to talk about next steps or the - for the next week's meeting.

My idea for that was that…

Man: Milton?

Milton Mueller: Hello?

Bertrand de la Chapelle: Milton, yeah, this is Bertrand de la Chapelle, can I make just a brief comment on the last point before we move to the next item?

Milton Mueller: Okay.

Man: I was thinking about the remarks that was made about the fact that we are confronted with on the one hand special types of actors that have an easy and workable certification process and the difficulty to handle a lot of other actors who do not have certification process available but are working in part with the actors that have already we've mentioned.

Would there be anything that would be worth exploring in a notion of a distributed certification process whereby change of accreditation, would allow certain number of master accredited entities to enable actors that they trust enough and that they're working with, with the responsibility of revoking them in due course that they don't comply with a certain number of rules, a bit like the registry, registrar type of thing, it's just an idea that came to mind and I didn't want to…

Milton Mueller: So, it's an idea to maybe you can develop in terms of our next steps, certainly worth looking into, so…

Wout: This is Wout, Milton.

Can I have one question in this - Milton?

Milton Mueller: Okay.

Wout: Okay, thanks.

Are you familiar with the (Dutch particle) which (with) banks and the government that (confuse) the emergency response team?

Milton Mueller: No, I'm not.

Wout: Okay, then that's something we can discuss offline better than unless everybody is interested but I think it's better to do offline considering time.

Milton Mueller: That should I do it online but do it on text that is submit - use the list.

Wout: That's possible but I can also make a phone call and doing something on text because it's probably easier to explain when on the phone bureau I will make it on text but it's something which I think is appropriate for these subject.

Milton Mueller: Okay.

Wout: That's why with this suggest to do it offline.

Milton Mueller: Yes.

Yes, that's fine.

Wout: Okay, the - I think your email is address is on the list and I will send you an email with my phone number.

Milton Mueller: All right, very good.

Wout: Okay.

Milton Mueller: Okay, thank you.

Wout: You're welcome.

Man: Okay, so what I would like to see is I guess is I would propose to the next step is that people within these categories consolidate their ideas and respond to the fairly extensive questions and need for clarifications that were proposed today in the discussion.

And if anybody based on this discussion think they have some brilliant new proposal, they could submit it and then I think in our next week's call, we will basically start talking about merits and problems of the various proposals which we try to do avoid today but obviously still (unintelligible) into the sometimes, but this - so, I'm thinking of a Tuesday's process over the next week we consolidate and integrate proposals where possible and resubmit them and then, we have a discussion about merits of the various approaches that we have in front of this next week.

How does that sound?

Man: (Unintelligible) I think sounds like good. I think from discussion how to (unintelligible) those clearly pretty good scope of consolidation, I think a lot of people have been aiming of the same sort of end point so I think in terms of access versus mechanism sections and I think there's some great scope to consolidate.

Milton Mueller: Excellent.

Man: Milton, do I understand your description correctly that it's still possible to submit a new proposal?

Milton Mueller: Yeah, I think it would obviously need to benefit from and taken to account what's been said so far and have some clear advantages over what's on the table already that definitely.

Man: Okay.

Milton Mueller: All right?

Dan Krimm: Milton, this is Dan.

Milton Mueller: Dan, how do you do?

Dan Krimm: I just wanted to find out if perhaps if there any follow-up questions we should be able to address those on the (list) through email between now and next week's call?

Milton Mueller: Yes indeed, although we're dealing with lawyers and they don't like emails as much as me do Dan.

Dan Krimm: Understood.

Milton Mueller: All right, if I maybe allowed lawyer (unintelligible) for the week, I will call the meeting to a close.

Man: Thanks Milton.

Woman: Thanks Milton.

Milton Mueller: Bye, bye.

Man: Yeah, thank you.

                 Bye, bye.

                                    END