WHOIS Working Group B "Access"
Teleconference
TRANSCRIPTION
Wednesday 30 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 30, 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-20070530.mp3

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

Attendance:

Milton Mueller NCUC chair - wg chair
Eric Dierker - onserver
Carole Bird - observer
Leo Longauer - observer
Wout de Natris - observer
David Fares - CBUC
Palmer Hamilton - CBUC
Doug Isenberg - IPC
Tom Keller - registrar
Ross Rader - registrar
Dan Krimm - NCUC
David Maher - registries
Steve Metalitz - IPC
Margie Milam - Registrar/IPC
Ross Rader - registrar

Melissa Rotunno - observer
Ken Stubs - registry constiuency
Michael Warnecke - observer
Shaundra Watson - observer

ICANN Staff:
Maria Farrell - GNSO Policy Officer
Glen de Saint Géry - GNSO Secretariat

Absent - apologies:
Philip Sheppard - WHOIS wg chair
Avri Doria - Nom Com appointee to Council
Yaovi Atohoun - observer

Milton Mueller: And you gave right after Fares.

Glen de Saint Gery: David Fares, Michael Warnecke.

Milton Mueller: Warnecke, okay.

Glen de Saint Gery: And Tom Keller

Milton Mueller: Hey. So…

Glen de Saint Gery: And Yaovi , (also on the line) but I see he's being disconnected. I'll see what's going on there Milton.

Milton Mueller: Okay. All right, so what we have is the graph of a proposed report. And we have a new proposal on the table. I would like to begin by discussing the basic outline of the reports, and see how much agreements or disagreements there is on that. And then we can go to this proposal to see if any additional blending can take place.

So the report basically is divided into three sections. One of them talks about eligible third parties and haven't changed much, except for the section on special sectors in which based on our discussion last week. I tried to encapsulate that discussion.

And then the degree of access granted, the definition of the types of access was sharpened up and there was a concluding sentence that sort of indicate where we are.

As far as I can tell based on our discussion in terms of what it read, what it supported, and what is not agreed. And then there is new section on the constraints of Port 43

Let's talk about the eligible third party first. You know, this – is agreement statements which are voted. Does anybody wish to take issue with anything that's being stated there?

Steve Metalitz: This is Steve Metalitz. (I'd like to be on the queue).

Milton Mueller: Go ahead.

Steve Metalitz: Yeah the second agreement statement, there was agreement that suitable mechanisms for Global Certification of an organization status as an LEA do exist EG Interpol National Agencies.

I think that kind of overstates how far we got in that discussion, at least in my recollection of the calls. Was a proposal in one of the proposals there is the idea that the National Agencies of Interpol would handle this, I think we also heard that that's not practical in some countries, because it doesn't take into account in the federal system the state and local agencies.

So, I think there was some discussion about (unintelligible) but, I don't think there was agreement that those mechanisms exists.

Milton Mueller: It was not agreement that suitable mechanisms exist. Okay.

Steve Metalitz: I think - I mean there was discussion about them and I think that we had further discussion, we might opt the suitable mechanisms but I don't know that we have one yet.

Milton Mueller: Okay. Does anybody have any additional comments about that issue? If Palmer Hamilto on the line, do you agree with that?

Palmer Hamilton You know what? I've looked at a lot of the discussions in the last couple of weeks and a lot of the statements that have been made. My position has been only to provide information where either, I think something can't be legally be done, or isn't achievable.

In terms of whether or not there are mechanisms, could be use to do this. I think we're too early in the process to say because sociably that

we've dove into it. I think we're still at the discussion of proposal stages.

Now, I'm looking at everybody's emails. I understand there are a lot of frustrations because everybody wanted to move forward. Yet, I still believe that whenever we look at putting any proposal for it, it's still has to have viable option, as opposed to you know, being arbitrary statements that laws that exist already to have to be change and so on and so forth.

So, I think we can say that there might be suitable mechanisms, but we'd have to certainly examine them in much more depth to determine whether or not they are liable, and whether they would meet everybody's needs. I certainly can't speak for every police agency nor for every country.

And so, I'm a little hesitant to make definitive statements that could have impact without having significantly more information from a larger part of the sectors that are affected. Did that helped them?

Milton Mueller: Yes it does. I think, yes nobody is expecting anybody to speak for all stakeholders in their particular categories. So I think that, I understand your caution about that.

And you might be just telling me that we need to change the language a bit, that we can say there was agreement that suitable mechanisms for global certification of an organization status as an LEA might exist but would have to be examined in more detail.

Or maybe a statement that we agreed that certification is a status as an LEA would be easier than certification of other categories of actor.

(Ross): I think, not the same, the second jump on this.

Milton Mueller: Yeah, (Ross).

(Ross): I think the solution here in terms of the stocking that these phrases in terms of a policy statement. The sentence that we're discussing here seems to be - .

Milton Mueller: You're kind of fading out (Ross). Can you get closer to the mic?

(Ross): Sorry. Is that better?

Milton Mueller: Yeah.

(Ross): So to repeat, I think the answer that we're looking for here is to frame this up in terms of a policy statement as opposed to an implementation requirement. The preceding sentence is certainly a policy statement.

I have my (doses) whether this one is or not. It seems to be more of a statement of an environmental condition and we're kind of disagreeing whether or not that our environmental condition is true or not.

Perhaps if we rephrase it as a policy statement, saying that something to the effect of – there must be some way to certify or something on (mills) line so we can move on and leave those implementation details to the later phases.

Milton Mueller: So you was – first something like as a policy statement that we should find or seek out suitable mechanisms for global certification.

(Ross): Yeah. Something along the (funds), I think that kind of addresses the consents I've heard so far.

Milton Mueller: How do you feel about that Steve?

Steve Metalitz: I could - that we should explore suitable mechanisms. I'm sorry. Could you repeat what the phrasing was?

Milton Mueller: Could I repeat what?

Steve Metalitz: (Ross), repeat what he suggested, go in there or...

(Ross): I didn't make a specific suggestion on text. I'm still one cup of coffee behind the rest of the world cup. Let me I think I could suggest probably would make much sense at this point.

Steve Metalitz: Yeah – but I agree that if it's a statement that there would need to be a suitable mechanisms and that that should be explored, I would agree with that.

Milton Mueller: Good, okay. Okay let's go on to the private party's paragraph. Do I correct in saying that, there was no agreement? Or was that too strong of a statement?

Ken Stubb: Milton?

Milton Mueller: Yes.

Ken Stubb: Yeah it's Ken. I just want to make sure. Would somebody please define again exactly what constitutes a private party? Is a private party an individual person? Is a private party a – in intellectual property, agent, lawyer? Exactly, how are we defining that?

Milton Mueller: It's all of the things. Is anybody whose not...

Ken Stubb: LEA.

Milton Mueller: …an LEA or a governmental agency?

Ken Stubb: So in other words, a financial institution would be considered to be a private party here?

Milton Mueller: Definitely, yes.

Ken Stubb: Okay. The same, it's a shame that we – well, you know, I'll just (re-services) again. It's a shame we can't come out with some sort of a policy, or at least a recommendation that we try to establish a methodology for stratifying private parties.

Because I think we're tossing a lot of babies out with a lot of bath water. And I think there's a significant (currents) there in that. If not, I think we may - we can make it abundantly clear in the presses exactly how we're defining this to.

(Dan): This is (Dan). I would suggest that by not defining categories within the private sector we're actually opening the possibility of becoming certified to anyone that has a legitimate interest based on their actual

need, rather than some sort of general categorization. I tend to think that adding the layer of categorization actually confuses the issue more than it helps the issue.

If you're going to say, well, all banks should get access while maybe only some banks who get accesses or something like that, depending on the one's with actually having need for access. And it should be based on specific need rather than the category of institution or individual.

Ken Stubb: You know, let me respond very quickly to that. I'm concern about that because from a practical standpoint, I don't like the idea of self-certification for what constitutes a legitimate purpose.

You know, I mean we've seen enough over the years of abused. So that, you know, what's legitimate for one person is clearly not necessarily legitimate for the balance of the community. And I – I'm - that's really concerns me when you...

(Dan): I would agree that we don't want to deal with self-certification but if we can try to find well defined protocols for certification that could be implemented by jurisdiction with authority to do that. Then it's not self-certification but it's still a used-based certification rather than a category based certification.

David Fares: This is David Fares. We moved away - Milton, from your comment moved on to the point of certification because I do have a comment about (document).

Milton Mueller: About what?

David Fares: The (sentence) says none of these proposals incorporated well defined rigorous methods for pre-certifying.

Ken Stubb: Do you want - my question, do you want to finish your first question which is, is there no - is the statement that there is no agreement about private party's accurate one - accurate reflection of the...

Milton Mueller: Yeah. I would like to find out if we can say something better than that. Was it, it was - there is some construction of agreement there but - so, I think we just heard restated the basic problem which is that if the problem is going to - a problem of certifying access is going to be manageable, we start talking about categories and distinctions which may use as a basis for excluding some people and permitting others to have access.

On the other hand, that (Dan) points out those categories may not match up with actual need and - our legitimate need, I should say. Need itself, I don't think anybody believes qualifies you for access to this data. It has to be some kind of a protection against, from the lower fraudulent activity. So that's the basic...

Coordinator: Excuse me. Melissa Rotunno now joins the call.

Milton Mueller: And I haven't seen any magic way of getting out of that conundrum yet.

Ken Stubb: Okay. So for the - just like, put myself in the queue, I do want to talk challenge notion being assertive that pre – that self-certification is not justified.

Milton Mueller: Okay. Why don't you go ahead and do that.

Ken Stubb: Okay. There in a - it relates to the sense that I was talking about under the section on private parties that none of these proposals are incorporated well defining rigorous methods for pre-certifying the legitimate private party - private actor.

I think that that subjective statement in that which shall remains factual in this. There is precedence or self-certification and I would use the EU Safe Harbors as one those examples which is addressing privacy.

Where private actors self-certified that they are complying with the set of privacy principles and there's expose factor review if a problem arises.

So I think this thing government mandated and recognized self-certification processes. And I think that we should just provide a more factual statement here that most of the proposals included self-certification for legitimate private actors relying on some form of affidavit in the exposed spread of discovery reviews because I think that there's a disagreement in this group about whether pre self-certification - regarding self-certification and pre-certification.

Milton Mueller: Yeah. I think – let me just - I understand sort of why you made the objection but in terms of the actual meaning of the statement, the actual language there really isn't any different from what you've said. Maybe I can remove some of those adjectives, like well defined and rigorous.

But the point was that the proposals are not talking about pre-certifying. They're not talking about filtering people out before they get access. They're talking about giving anybody who wants access, access and then filtering them out based on exposed discovery of abuse.

Ken Stubb: I will be fine with (that Milton). So if we were to read something like none of these proposals incorporated a mechanism for pre-certifying the legitimacy of private actor. Most relied on, I would be fine with that.

Milton Mueller: Okay.

Ken Stubb: And at the factual...

Milton Mueller: You're right. I should probably note that there is disagreement in which we just heard from Ken and from (Dan) about no certification as a method, which again goes back to the unfortunate first statement of the paragraph.

Well, let me ask this. Is anybody who doesn't like self-certification convinced by David Fares's mention of the EU Safe Harbor President?

(Dan): This is (Dan). I think from a privacy advocacy point of view, the legal environment that we're living in today is transitional and not to be in as (accident) stone and perhaps there's room for improvements. So I would say, at this point not yet convinced.

Ken Stubb: Milton?

Milton Mueller: Yes.

Ken Stubb: Yeah. It's Ken Stubb again. I have to apologize for my skepticism. But having just spent ten days in Venezuela, I hope you can understand where I'm coming from.

You know, I mean from a practical standpoint, I'm very - still very concern about, because if you for instance take the proposal that Michael surfaced here where some of the definitions are combating socially abusive uses of the internet.

And helping users identify where people responsible for online content and services, I just see still too many opportunities for abuse in this self-certification process. And I just frankly need more clarity as I see it, you know, maybe I'm just too skeptical, I don't know.

Milton Mueller: All right. So I think that answers my question fairly well. And so, we're still stuck with disagreements here but maybe we have phrased it a little bit better.

Wout de Netris: This is Wout from OPTA.

Milton Mueller: Yes.

Wout de Netris: What I do think, there is agreements that private third parties, whether they are have the right to litigate or whatever you call it in English against perpetrators, are conduct to something we all agree on.

But after that, it's how do they, after due process research, get the information they need about WHOIS behind websites or domain

names or IP numbers, whatever. But we do agree that everybody has a right to research.

Milton Mueller: At this point, maybe we should open the (paragraph) for that statement that private third parties have a right, of course to litigate, but even stronger to investigate.

(Dan): To due process.

Milton Mueller: Through – well, yeah.

Ken Stubb: I think there's a difference of opinion on that.

Milton Mueller: There is a difference. But private third parties have a right certainly to initiate various kinds of action against people, who they believed are violating their rights, defrauding them, stealing from them, whatever, right? We all agree about that.

I hope, or don't we. I mean, I shouldn't express my opinion.

(Dan): If it's a question...

Steve Metalitz: I agree with that statement, yeah.

(Dan): …(my answer is) yes, yeah.

Wout de Netris: Then you have your way at least to look at what do these party needs to be able to investigate. And what do you...?

Milton Mueller: Question of what they have a right to investigate is not a question of need. In other words, it would be nice if, you know, every time I – person who scraped my car, if I could go to the internet and type their drivers license in and see what their home address is. But I don't have that right. And…

Wout de Netris: No. But you don't have the right to access that directly but you do have the right to get that information through due process which I think you call it.

Milton Mueller: Yes. And that's a very important distinction.

Wout de Netris: That is a distinction, I know, but doesn't – you can look at the ways that these private third parties can reach at that. But the basis is if everybody has a right to what you call, investigate. It's fine. That's fine definition by me. So that's my (unintelligible).

Milton Mueller: Well, I think that's a good point. And we should put that up at the top of that paragraph that we're recognizing this. And see their – the problem is our disagreement about the conditions through which these private actors obtained access to, otherwise private information.

It doesn't move as very far in terms of a policy but at least clarifies what the obstacle is.

Oh. So should we move on to the sectoral issues?

Now here, again I got - I came out of the last week call was very strong view that there simply was not the consensus that we should devote our time to a sector specific proposal.

Palmer took issue with that. So maybe Palmer – again we're not talking about the merits. We know you believe in the merits of a sector specific proposal. We're talking about how much support there is for that.

Palmer Hamilton: Well, nope and my objection was simply the use of the term agreement, alternate view et cetera. Because it seemed to me that it would be necessary. And I understand the desire not to harden position.

And I'm not suggesting we move to a formal voting process but since we're not going to have formal voting process, I was simply suggesting that we not use terminology that suggestive of a formal process.

And that you could say there's a lack of consensus as to whether they ought to be sectoral differentiation without using that terminology.

Milton Mueller: Well, you remember when I called for a straw pull to determine agreement or its absence, so I was slapped on the wrist.

Palmer Hamilton: Right. And I'm not suggesting we should move in that direction. All I'm saying is absent doing that, I think we need to avoid the terminology.

(Dan): This is a process problem Palmer or there is a substandard point that we're missing here?

Palmer Hamilton: Well, It has the (defacto) effect I think of taking out of consideration this at the next stage by suggesting that there's no support for it and therefore the working group doesn't need to consider it.

(Dan): I think that's a very accurate statement.

(Eric): This is (Eric).

(Dan): This language might have that affect yes.

(Eric): If I may, when we're using the term sectoral, we're talking about the how or the who, correct? Completely, that's what it means.

Milton Mueller: Yes. It means a well defined…

(Eric): Who?

Milton Mueller: …sector of actors who have something in common.

(Eric): Okay. And then on the next word was – Palmer you have a problem with the term agreement?

Palmer Hamilton: I'm just thinking that if we use that terminology, when it goes to the next stage, the working group takes it up. The working group will say, "Oh well, there is no support for this position therefore we don't need to give any serious consideration.

(Eric): I didn't see this global concept that Milton was referring to. I think no matter what, you have to take the consensus sound in a working group as within context.

If someone wants to take it out of context they certainly can, but it would be inappropriate, I think. I understand your concern but I don't

think it's a fair one because it would be a misuse of the language rather than a proper use.

Palmer Hamilton: I'm sorry, who was that?

(Eric): That was (Eric).

Palmer Hamilton: Oh (Eric). Okay.

(Dan): This is (Dan). I would just point out that this terminology kind of comes from the charter of the working group where there was this sense of, you know, agreement, support, or alternate views.

And that, you know, agreement is based on a consensus process. So, seems to be our charter, you know, what's been given to us to work with.

Milton Mueller: Right. Definitely is. Indeed it's what the working groups are for. But the subgroups are for and ultimately the working group. Now...

Steve Metalitz: Milton. Can I get into the queue? This is Steve.

Milton Mueller: Okay. The fact that there is no consensus in this working group about banking specific proposal, Palmer, it does not help you when you get to the larger group. So - but it does not fully precluded from consideration.

It maybe that you would work your persuasive magic on other people in the interim or it maybe that somehow people would see that focusing on this narrow problem in the future deliberations of the full group

would maybe make some progress where they thought more progress as possible but then they discovered that it wasn't.

But I don't think we can avoid the fact that there's simply isn't agreement on this. And by agreement, I don't think we need to take a vote of any kind. I think what I was told last week, and I think it's correct, is that we put a proposition before this group and we listen, and say to people, agree with this or not. If nobody disagrees then we say it has agreement. We don't need to take a vote.

If somebody disagrees but only one person then we might talk about rough consensus. And if a few people disagree but it seems like everybody else agrees then we might talk about support. That's my standing.

Okay. So Steve, you had something to say.

Steve Metalitz: Yeah. I just was raising the question of whether the subgroups are supposed to be, you know, a filter or a funnel or just what the right metaphor is. I wasn't – it wasn't my understanding that anything that's put on the table in the subgroup would automatically be excluded from further consideration in the working group as a whole.

I think – I thought the idea was to surface proposals to try to narrow the range of proposals if possible and then to bring the proposals to the full working group with some indication of the level of support, but not that anything would fall off the table necessarily.

Milton Mueller: I think we agree. I mean, again as I said, if Palmer – well, let me just give me my own perspective is that if I thought at this stage that we

couldn't get an agreement on anything, and as soon as we realize they have people are going, “Well, let’s do something about banks. At least we'll get something done.” You know, if that happened a month from now, I might go along with it.

But, you know, I'm not trying to commit myself to anything in the future. But the point is people could change but I think at this stage, the agreement is pretty much as I stated it.

Certainly, I think we all agree including Palmer, that a solution and compassing all legitimate users would be preferable to one restricted to a sector.

Wout de Netris: This is Wout.

Milton Mueller: Yes.

Wout de Netris: I think the word sector might not be the right one. Let’s consider this just an example: The Estonian government is being bombarded. All institutions in Estonia were bombarded last week or two weeks ago by somebody just stopping their infrastructure. That is something that needs to be looked at quite - in (every) possible way.

So I think what the distinction should be, what is the urgency of the need for the information the specific subject have had. So that might mean in the form of bank, not as a sector but as a fishing problem.

Then the urgency to stop that to help protect end users might give it completely other view than that it's a bank, or a trademark, or a

copyright which will have to have some sort of – yeah, slower process of investigation.

And they do not need this information right away. While in other, like the Estonian example, but probably many others of text that happened on the internet, you would need to have information fast to shut websites or whatever servers of computers down.

That I think if you look at it from that way, that might help to get your consensus faster than looking at a bank, or a PayPal, or a Coca Cola, whatever. (Unintelligible).

Milton Mueller: But think that is how we're looking at the problem was the - we mentioned in the report the high incidents of fishing and the high financial stakes.

Wout de Netris: Right, right. But we keep coming back to the word sector and the word – but I think we got - if we drop that and focus on problem then we might be able to reach some sort of agreement faster than if we keep looking at the word bank, or the word Visa Card, or whatever. That's my point.

Milton Mueller: But the point is that not all of the subjects of fishing are governmentally chartered banks. Credit Cards, and PayPal, and those kinds of – even AOL, I think is subject in a tax. Now...

Wout de Netris: And also the online companies are subject to a tax because they're being bombarded in the inaugural service attacks. And then they get an addition – what do you call it, an external – extortion email. Well,

you want to know where that comes from too very fast (for sure), that sort of company.

Milton Mueller: That's right, so.....

Wout de Netris: So if you look at it from a problem perspective which is much wider than just fishing, then we might have a way of who needs access and what way and how fast and WHOIS going to give that access.

Steve Metalitz: Milton, this is Steve. Could I get in the queue when you (unintelligible)?

Milton Mueller: Yes.

Wout de Netris: That's my point. So, thanks.

Milton Mueller: I understand. I understand the point. But I think you're actually reinforcing the problem with the sectoral approach. It's that you're talking about urgency of the problem regardless of how it is concentrated on a particular sector.

Wout de Netris: Right.

Milton Mueller: And the proposal that we're talking about is indeed concentrated on a well defined sector. So that's what would - that's the debate we're having is that should we prioritize the sector or something else.

Okay, Steve?

Steve Metalitz: Yeah. It maybe the part of the problem is the template we've been working with. I mean the first column – the second column is which

third parties. You basically have to answer that question before you could complete the rest of the template.

And I think what Wout is talking about is maybe the right question is what types problems need – are to be addressed. And that obviously has some congruence with which third parties. But as he points out, fishing is not simply a problem for governmentally chartered banks.

I think actually, if you look at the blended proposal it kind of has some of this in there, because it's not only which third parties it also addresses what types queries would be accepted in this process.

But maybe that's the reason why we're having so much trouble on this section is that we're asking the question of who, rather than the question of for what purpose.

Wout de Netris: That's very well defined, thank you.

(Dan): This is (Dan). I would concur with a lot of what's been said here. I was one of the people that also concurred with the alternate view that we could use to the bank proposal as a model or test case for developing a broader solution.

I think one of the reasons that that seems sensible is that in the case of the bank sector there are law enforcement processes and structures that are set up that seem to be amendable to a kind of, you know, quarry screening model that was proposed.

And because we know that there are perhaps more difficulties in other sectors with a proposal like that. This, you know, focusing on a bank

solution as a starting point, allows you to focus on just part of what the issues are without having to get into all of them. And then as you expand to, you know, beyond financial institutions, then the issues of jurisdiction become more important.

Milton Mueller: Okay. Well again, I think – yes, I think we pretty much, at least - I pretty much figured out long ago that the issue was not so much who but what type of problem.

And that's why we started with this basic distinction and when we said, “Who should have access?” one of the categories was anyone. Remember, Steve? And you objected to that.

The point being that if you say anyone could have access, then the issue becomes well, what is the nature of their problem. And that requires some kind of fairly serious and potentially manual filtering. And we never got, you know, beyond that point. We never got proposals for, you know, seriously...

Steve Metalitz: Milton. It either could require that or it could require some form of self certification with a mechanism for dealing with abuse.

Milton Mueller: Right.

Steve Metalitz: And that – there's several proposal out there that have that feature. And at one point, you just missed Michael Warnecke's proposal because you said it was too complicated and had too many tears in it.

It had too many different types of people or types of entities that might be able to gain access. But if again, we focus on the problems and if

we can list the problems that would be the justification for access, then that's – maybe that's not such a big issue.

Milton Mueller: Well, If you could narrow down the problems to the point where it, you know, it's not people saying, “I want to know whether a domain name is for sale.”

Steve Metalitz: Well, we started that process, I think. And I think there was, you know, that one may have been struck off the list. But, you know, I think that maybe a way to proceed as to look at the types of problems that we need to solve. And working from the - maybe working from bottom up, there are some that don't require access.

Milton Mueller: But the issue was not just identifying problems that would acquire access, it's a process for, you know, scalable process for filtering through those. And also there was a lot of...

Steve Metalitz: Well, I think you've been – there has been scalable processes proposed that involved self-certification. I know not everybody agrees with that, but all I'm saying is that there is some support for that in the task force. And...

Milton Mueller: Okay Steve, can I finish my sentence?

Steve Metalitz: Go ahead.

Milton Mueller: That's the second time you've cut me off in mid sentence. The point is we just have a discussion about self-certification. And there's not agreement about that, a lot of concerns about that. So...

(Dan): Milton this is (Dan). I would also suggest that the more recent proposals have a kind of a two tiered certification paradigm where there is a pre-certification of those eligible to have query, to be able to make queries in the first place.

And that first step would probably be manual but on a fairly sporadic basis. And then when you get to actual specific queries, that's where the process gets more automated and it's on a more timely basis.

So it splits the manual part off to something that doesn't need to scale quite as much, and then the stuff that really needs to scale, that that's where you look to try to automate the process as much as you can through well defined protocol.

Milton Mueller: Yes. All of which requires the completely new - (in a system) to be developed.

(Dan): That's right.

Milton Mueller: Which is something that – my understanding is that the registrar in registries is not thrilled about.

(Dan): I would not be asking the registrars and registries to develop the system. I think it's probably is something that ICANN should coordinate. I would even suggest that it might be possible to do this through an open source project to reduce cost, increase standard interoperability, increase security and reduce user fees.

Man: What – (unintelligible) one question I don't understand. What exactly are we talking about? Are we talking about the protocol to facilitate the

data or is it about the – I want to call the expert (unintelligible) process for someone to be able to have access to the data?

(Dan): I think it's more in the access side. And actual quarries would still go through the registrars of course. But once the data has been queried by someone who has got authority then this is a mechanism of granting a prevision of that information indirectly to other third parties. And that doesn't need to involve the registrars at all.

Milton Mueller: Okay. So we're going to have to move on. But what I would like to see is if you believe that progress can be made here, then I would encourage you to work with others to develop a truly blended of proposal.

One in which is not restricted to banks, and which takes into account the discussion we just had. And also the agreement points about the types of access, and incorporate this to tier notion of a first manual path for certain parties and...

Steve Metalitz: Actually Milton, if I can interject very quickly there. I would like to see a policy discussion. Today we had a lot of discussion about process, we had a lot of discussion about implementation, after very little of policy. What I would like to see in terms -- personally speaking -- in terms of running proposal, is something that deals with the policy implications.

Milton Mueller: Talk of manual, and automatic, and technology and open source of security, et cetera, et cetera, et cetera, et cetera. At least to the level that we're discussing today are all very much operational concerns and not policy concerns.

Steve Metalitz: Yes. I stand corrected and I think that's a very important and good point. What we do want to be talking about policy, that's why we have this ideal type of access. And we're trying to decide what kind of access should be to provide and not about implementation.

(Dan): I would agree with that Milton. I would just say that, I think that some of the policy considerations were in danger of being detailed by claims that they were not possible to be implemented.

Milton Mueller: Yes. That's my point, is that the - when we talk about a blended proposal or some kind of a consolidated proposal that incorporates and might build more support than the usual one.

I'm talking more about how it handles the basic policy trade-offs, and not about whether it's an open source or, you know, using a particular protocol.

But the question of, you know, who will this actually give access to what potential, or will it have for abuse, what safeguards will it have, and is there agreements on those basic policy principles?

And what would be the role of public law enforcement agencies versus private party? That's something that we can talk about policy. So, feel free to take up that gauntlet.

Now moving on to degree of access, again we identify these four different types. And we concluded with the statement is agreement that LEA has being granted at least Type 1 access in support for Type 2 access. These people could see that as accurate as a policy statement.

Wout de Netris: This is Wout from OPTA. I would like to bring something in which might verify things. But I have to say a few things first. I want to make clear again that OPTA is an independent gash authority. And we do not represent any of the LEA in the world nor any EU country government or institution, we just represent ourselves. So if we say anything than it's - when there's a third party access is just to help the process and nothing more than that. And if we talk about LEAs, we just talk about ourselves, which I think is a very important distinction to make.

We have the idea with that, we do not have much decisive influence on which either way this (structural) discussion is going which might be frustrating but it also makes it very hard to take any responsibility for the advice or the conclusion of this working group.

So that's something which we are not going to accept whichever way is comes out, is not something which we are going to take responsibility for.

Any other outcome for OPTA which is left them, number two, then we go for number three really, is not acceptable. Because we will probably not be able to do our job anymore if we are going to be stuck with option number one.

It's something we can not work with because then, just about spam enforcement - spyware enforcement will stop, full stop really. And I mean it's an account stressed at more than this.

Why there are no other – I'm glad that you have to see is on board on this call, I heard him on the roll call. Why the any other LEAs in the

world where when this major problem for them is so accurate, and at the present, I don't know.

It's just that we are in on this on our own and we are just OPTA. I'll say that again, to help the discussion maybe. The EU privacy laws which are one of the reasons why this discussion is going on I think, in general.

Do not prohibit access for WHOIS to WHOIS information for LEA's. It's just that it has to over go in due process. This means that we as OPTA have in our OPTA law and in the general administered law of the Netherlands.

We have the right to investigate, to get information, to sanction perpetrators of the Telecommunications Act. So that means for us that is reason enough to get access to WHOIS data, because that's the only way we can do our job.

And maybe consensus is not reach of this work group because of this misunderstanding that EU privacy law do not prohibit access to WHOIS information.

So, I think this is very important for you all to understand that we as OPTA have a job to do, given by us through the law. And if we do not have access to this essential information to find perpetrator, then we will probably be the end of safeguarding the internet against guys like these.

That is something that I wanted to say to the group. But I also would like to find out in which way can OPTA -- and (if he is) now listening --

have influence on this group because we don't have any sort of stature.

And why that is, I don't know. I don't know how I can work, just on something completely new to this. But we do need to have some stature and some decisive influence.

And I don't think that we're having that at this moment, especially not when we go back to the main group when other - the other people are going to be involve and after that on the GNSO board. When where is our meaning being heard?

Milton Mueller: Okay.

Wout de Netris: In our opinion. So that's something I wanted to say, and that is very important for institutions like or perhaps who have access.

Milton Mueller: Yes, yes. Wout, everybody understands the - that law enforcement agencies like yourself have particular interest and needs that they are pursuing to this process. I think we, you know, the broader issues of how you participate in the ICANN process is really way out of scope for this working group.

Wout de Netris: I know. I know that. But it's important in the end.

Milton Mueller: Now, we have about five minutes left. And based on what you said, as it relates to the three statements. Again, we're not talking at policy prescriptions here. We're talking about how much agreement there is on policy prescription. And I think it's very important to establish that.

So you said - I mean there is support for granting LEA Type 2 Access. You said that you want a Type 3 access. I think that they might not be correct. In the sense that Type 2 access basically is the same as Type 3 access. It's simply contains some kind of record keeping and auditing that means that you're not using it as a random data mining.

And my understanding is both American and EU law is that, you know, a law enforcement agency does not, you know, have a right to look up the domain name, address of an internet user that the law enforcement officer thinks is pretty and it might want to contact for a date, right?

Wout de Netris: We justly agree on that. It's just that we see too many undefined words in the number two, which could go anywhere when defined. Then the question remains is there still a good access or not when everything is defined. So, that's probably the point I would make last.

Milton Mueller: What is an undefined about query-based access to any domains?

Wout de Netris: I haven't got it by hand. But there's a few words in there that which could limit the access and that's one of the fears we have.

Milton Mueller: I don’t know. It's Contractual Legal Restriction of Queries to Records of particular domains under Registrants causing problems at specific time. I emailed discriminate - indiscriminant data mining. So if you have problems with specific words, let's talk about how to modify those words.

Wout de Netris: All right. Well, I'll – could we get back to that? Can I do that?

Carol Berg: Milton, can you add Carol to the queue?

Milton Mueller: Yes. Carol?

Wout de Netris: (Or is it) now that we've – we can't get back to that.

Milton Mueller: Okay. Carol?

Carol Berg: Two quick points. I have this for what my colleague from OPTA is saying. Sometimes the devil is in the details or in this case, I think the devil may be in the definitions. We may not all be coming from the same definitions or the definitions may - the words may have different definitions in our countries.

When we say no indiscriminant data mining, let me give you an example and you tell me whether that falls into bad data mining or good data mining. Let's say I got a complaint of somebody selling toxic drugs over the internet and innocent members of the public are purchasing them in good faith thinking that in fact these are safe drugs to consume.

I'm going to pick, you know, something generic like aspirin – but it's not the real aspirin, okay? I don't want to besmirch someone's name. Anyways, so they launch a complaint with the police.

The police start to investigate and we find Company XYZ has been registered as one register. We now want to go and see if they've been savvy enough to register in a number of different locations.

Is that considered indiscriminant data mining or not?

Milton Mueller: Clearly not. I mean, you have a name of a suspected perpetrator who – you're searching based on that, right?

Carol Berg: Right. But I might be searching for a couple of different variations of that name because not everybody always uses the same name when they set up. If you will, dummy companies as part of a criminal offense.

So, would that constitute indiscriminant data mining? I mean, I appreciate your example of running checks on all of our friends and family and then wholeheartedly agree with you if it's not in support of a police investigation, those queries shouldn't be run.

But sometimes, in support of a police investigation, we need to run, if you will, associated queries. But the name won't be identical every time. I may have spelled Carol Berg with an e in one case and without an e and another.

Milton Mueller: You know, I think if all of our – if your concerns are limited to that, as we – we really don't have a serious problem. Because these are just verbal clarifications and we seem to be in agreement on the basic policy which is that law enforcement agencies in pursuit or in support of an investigation given fairly broad kinds of access, as they can now under due process, you know.

You can – you could subpoena all the records of an ISP under certain kinds of legal investigations that go well, well beyond the WHOIS record data. So, that's – I just don't see that as a problem.

If you have a problem with the wording, if you want to avoid certain misunderstandings and all I need are some suggestions as to how to fix that. I think we can fix that.

Carol Berg: Okay. I – because I think a lot of the misunderstandings come under different people having different definitions for certain things such as indiscriminant or due process.

The other point I wanted to add Milton, is subsequent to our last teleconference. I did in fact check with our Access to Information Act and Privacy Act section within the RCMP.

Just to get clarification on degree of access number four, and in fact, if let's say we were - the RCMP had access to the WHOIS database and someone came and ask us to run a query for them. Unless it is pursuant to an investigation, we can't pass on that information.

So I just wanted to say, I checked it with our sector that deals with the legislation in Canada and it's just not something we can legally do. And I just wanted to add that clarification in there.

(Bob): This is (Bob). This is the same as for OPTA. Because we've seen our OPTA law, even the interaction law of OPTA that we're not allowed to do this. So, but I had already mailed that to the group.

Milton Mueller: So, you said unless pursuant to an investigation, you can't pass it on. Does that mean...?

Carol Berg: Unless pursuant to a police investigation particularly by the police agency that has access to the data. So, if for example, somebody

came to - let's say we had access to the data, and somebody came to us but they wanted something pursuant to a civil action not a criminal action, then I don't think legally we can provide it.

Therefore, you know, perhaps -- and I know I'm throwing this out of the 11th floor -- option number four should be indirect access by a government. And let the governments of the countries identify how best to put something that would allow access in place but respecting that country's laws. And by that I don't just mean the police, I do mean the privacy legislation that those countries have in place.

Milton Mueller: Yes. I think that might be a good clarification of what was intended by access type number four.

(Dan): Milton, this is (Dan). I would definitely concur with that. I think it's a very constructive comment. And also, with regard to the terminology issue, it may be that - I think data mining is considered with a very technical meaning by and certain people in the technology community and I think that sort of narrow term of artist really what was meant, data mining in the sense of looking across all the records of a database for certain global patterns in it to try to look for certain kinds of things.

Milton Mueller: Right. And again, law enforcement agencies may indeed get the right to indiscriminately data mine. At least in the US, they have, whether you support that or not, there's a question but it's not impossible under various national legal regimes.

All right. So again, taking into account these modifications, let me – again, direct your attention to that paragraph at the end of the Degree of Access Granted section. There – if there's anybody not agree that

LEA should be a granted at least Type 1 access. Then negate keepers' due process?

Is there anybody who does not support granting them Type 2 access?

Carol Berg: I think Milton, could we ask the question in a different way? Could we say that "Do we have agreement that they should have Type 2 access?" And if we don't, then voice it then do it, we at least have support. And then you cover it off whether the base limit should be Type 1 or Type 2.

Milton Mueller: Well, the difference between saying, "Does anybody not agree?" If I say, "Does everybody agree?" then you all have to say "Yes". And I can't tell whether there's anybody out there not agreeing. If I say, "Does anybody not agree?" and I hear a silence, I know that you all agree. Do you understand why I'm doing it that way?

Carol Berg: Yes I do. Thank you.

Milton Mueller: Okay. So, does anybody not support granting law enforcement agencies Type 2 access?

(Dan): I'm still stuck on the bullet point there Milton because it's consistent with my understanding of law enforcement requirements. But if there's silence on this issue, I'm not going to pick this issue up.

Milton Mueller: What bullet point are you talking about?

(Dan): Around auditing and record keeping of their queries. That's heard repeatedly that this would be an acceptable form of access for law enforcement community.

Carol Berg: Let me step in on that one Milton, if I can – if I may.

Milton Mueller: Okay.

Carol Berg: Again, I think we're going to need to flesh out what kind of an audit process would be in place. So here is my concern with regards to that. To be quite frank, if we're doing a national security investigation, we don't even share it within our department with other police officers that we're doing those investigations. They are that sensitive. It goes down to “a need to know”.

So, we would have really grave concerns with - or very strong concerns with anybody outside of our agency auditing the queries that we do.

Now, having said that, there are a number of different national databases and I suspect international, but don't quote me on that, where protocols have been established that require the agency to do self audit and report back on the auditing result and then have firm protocols in place.

For example, in the RCMP, not only do you have to sign a user statement that you're only going to use our databases for queries related to your work. But you only get access to the ones that you actually require for your particular function.

And above and beyond that, for certain ones, like our Canadian Police Information Center, we actually have units that go out and audit the use of the database within the RCMP.

Something like that that's within the agency, I think is beneficial. Something outside where we don't know if the people have been security cleared where they will know about investigations that we don't even share within because they are that sensitive. Because the risk is so high, that will cause a great concern for us.

Milton Mueller: Yes. Again, that's why we're not talking about implementation, we're talking about more of the policy principle here where I'm sure everybody would agree that even national security agencies need and sometimes to be accountable to national law or even international human rights norms in terms of what they do.

There's always some kind of a check, you know, there's a – for example, in the US, there's a limit group of congressional oversight which is very restricted in terms of how it's supposed to handle information.

So, as a general concept, Type 2 access simply means that there's some kind of mechanism oversight or auditing to make sure that it is not indiscriminate and abusive use.

What those particular mechanisms are and how they deal with very special cases like national security of course is not something that's addressed by this.

Carol Berg: Right. But I think, maybe clarification on that point might be beneficial to avoid interpretation later of our intention that might be different than what we actually intend.

Milton Mueller: Okay. I can put something in there about special cases. It's not just national security, I mean, there might be ongoing criminal investigations where you can't reveal who you're looking at and I'm sure that that's handled in various ways. But there's still some kind of a benchmark of accountability but that there are shields or protections of how the data is handled, right?

Carol Berg: Yes. But they can be internal shields within an organization or within a government. And I – and so I think the clarification will have to be some sort of auditing structure, be it internal to the organization or external as yet to be determined.

Because - I mean, just to give you another example, and I don't want to go into that length and take up everybody's time, but we routinely do child sexual abuse or child exploitation investigations.

Once a person's name comes out, it's very difficult to say “Whoops! Sorry.” It turned out that they weren't the person who did it. Their computer had actually been taken over by somebody else and it's a completely different person that did it.

So, there's so many cases where the information as to the type of queries we're running can't come out until or should not in any case come out until such time of the case is before the court and the court have the chance to determine whether or not, yes, the person did

commit the action or no, they didn't because the ramifications on the individual long term can be substantial.

Milton Mueller: Okay. But what we're maybe overlooking here is that we may be moving from support for a Type 2 access really aids to agreement? Is…

Carol Berg: I agree.

Milton Mueller: Is there any disagreement here?

(Bob): Well, not for me. This is (Bob). But I know there are one or two persons, in this group who would apparently not on this phone I called but they are completely against. And what is their stature or we agree now? Is – they – can they veto this?

And what I also thought is that why this some sort of auditing or monitoring came in is because there are completely legitimate alias in the world which we probably do not want to have a full access to with data which is one of the problems with these ladies brought in, I think – I think their ladies.

So, what's going to happen when they redo our conclusion of today of agreement? That's my question more or less.

Milton Mueller: Well, object on line and we will have to move back from agreement and support, if they don't or they will object in a larger group. So that's not an issue. I mean, we have to read our answer report and re-circulate it and we'll see what happens at that time.

Carol Berg: But let's be clear on what we're agreeing on. Are you saying that the statement should read, “There is agreement that alias will be granted at least Type 2 access” is that what we're agreeing on?

Milton Mueller: No. There is – yeah. We could be moving that alias be a – not at least because there is opposition to granting Type 3 access to anybody. But we would be moving – the same what would be there is agreement that alias be granted at least Type 1 access and agreements for granting them Type 2 access, maybe under the proper conditions or something like that.

Carol Berg: Yeah. I don't know that we can make that statement. I have to say I agree with my OPTA colleague when I say our preferred option would be to have the open access in Type 3.

Simply because it addresses all of the issues that we currently have and yet I know it doesn't address some of the issues, some of our other colleagues on this work group have.

Milton Mueller: Right. But this is agreement across the working group, not agreement among law enforcement agency.

Carol Berg: No. And I concur but, see, I would be looking at that statement to say at least Type 2. Because once we say there's an agreement to Type 2, it implies that we have disregarded Type 3.

Milton Mueller: Well, that - there is no agreement on Type 3 access.

Carol Berg: Yes. I understand that.

Milton Mueller: So that's all that it's saying. I – we can – we understand that you may still want Type 3 access. What we're talking about now is not what you want. We're talking about what the group as a whole can agree to.

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

Milton Mueller: Yes. I'm going to cut this call off and I'm – after you're finished. So, I really have to go.

Steve Metalitz: Okay. First, just on Carol's point, I think if everyone agrees on Type 2 and some Type 3, then at least Type 2 is an accurate statement. I just wanted to say that in the last sentence, I would suggest – of that section, I would suggest that to say there's agreement that it would not be consistent with the OPOC model for private parties to be granted Type 3 access.

I don't think my constituency would want to be on record in opposition to the status quo of Type 3 access.

Milton Mueller: Okay. I think I can do that but the point is when we – when Warnecke and – when the Warnecke proposal and the Fares proposal we're being discussed, they explicitly disavowed the idea that they wanted access to anybody at any time for any reason. They said, “We only want this (broad) access because it's easier for us to pursue the people we need to pursue.”

Michael Warnecke: Milton, this is Michael Warnecke. Could I get in on this, please?

Milton Mueller: Go ahead.

Michael Warnecke: Yeah. I – and – I agree with Steve's point on this. I mean yeah, I – that's true. I mean, we did take the perspective that we're limiting it to those situations.

But, it's because of the, you know, it's the framework of OPOC and that's what we're working with and that's what's in that framework that's what we're proposing.

But I – as I believe I was clear earlier, I mean, the status quo is something that would be our preferred approach but in the world of OPOC this is what we're putting forth is as a second best alternative.

So I don't think it's – I don't think it would be fair to characterize my statements last week in saying that Type 3 access is something we no longer are interested in.

David Fares: This is David Fares. I think that that's problem – that's an act of reflection of my perspective to have us focusing on implementation of OPOC.

Milton Mueller: Okay. So, I will notify the reports in another draft as sometime in the next two or three days.

Man: Thank you.

Man: Thanks Milton.

Milton Mueller: Thank you. Bye-bye.

Man: (Unintelligible).

(Bob): (Unintelligible) the next meeting.

END