WHOIS Working Group B "Access"
Teleconference
TRANSCRIPTION
Wednesday 23 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 23, 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-20070523.mp3
http://gnso.icann.org/calendar/#may

Attendance:
Milton Mueller NCUC chair - wg chair
Philip Sheppard - WHOIS wg chair
Yaovi Atohoun - observer
Eric Dierker - onserver
Carole Bird - observer
Patrick Cain - observer
Leo Longauer - observer
Wout de Natris - observer
David Fares - CBUC
Palmer Hamilton - CBUC
Doug Isenberg - IPC
Susan Kawaguchi - CBUC
Ross Rader - registrar
Dan Krimm - NCUC
Lane Mortensen - observer
Steve Metalitz - IPC
Margie Milam - Registrar/IPC
Palmer Hamilton - observer
Melissa Rotunno - observer
John Levine - observer

Michael Warnecke - observer
Melanie Halloway - observer

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

absent apologies:
Avri Doria - NomCom council

Milton Mueller: Hello Philip?

Glen De Saint Gery: Have you received it, Milton?

Milton Mueller: Yes, I did. It was my username, my email address or just my name?

Glen De Saint Gery: You're - no, no, no. Your - just your name.

Milton Mueller: Just the name?

Glen De Saint Gery: Uh hmm.

Milton Mueller: My conference is currently unavailable at this…

Glen De Saint Gery: And the number is 7430930.

Milton Mueller: (Unintelligible) 093.

Glen De Saint Gery: Oh, sorry. 7430930.

Is that better?

Milton Mueller: Well, so I'm - username should be Milton Mueller?

Glen De Saint Gery: That’s right.

Milton Mueller: And the conference num…

Coordinator: Excuse me Mr. (Woutuno) now joins.

Milton Mueller: …to the type of it…

Glen De Saint Gery: 7430930.

Milton Mueller: I have 7403.

Glen De Saint Gery: 74 – sorry that should have been 7430930.

Coordinator: Excuse me, Mr. (Metalitz) now joins.

Woman: (Unintelligible).

Milton Mueller: Okay, I got it.

Glen De Saint Gery: Okay, then you see who's on.

Milton Mueller: Right. So, shall we get started?

Glen De Saint Gery: Will you ask the operator or shall I do the “Star 0” for you?

Milton Mueller: I can do the “Star 0”.

Glen De Saint Gery:Okay.

Milton Mueller: Okay. The conference is being recorded. We have about – do we need to go through the roll calls? There are people who can't (unintelligible)…

Coordinator: Excuse me, (Sir Isenberg) now joins.

Milton Mueller: Okay. Okay, we're getting some quick additions here. We have Palmer Hamilton, right?

Palmer Hamilton: Right.

Coordinator: Susan Kawaguchi now joins.

Milton Mueller: Patrick, are you here from the registry constituents?

(Patrick Cain): Pat from (Unintelligible) is here.

Wout de Natris: Wout de Natris of APTA is here.

Milton Mueller: We have Carole Bird. We have (ErickDierker). We have Dan Krimm, Maria Farrell is on from ICANN staff, Margie from the registrar constituency, Philip from business constituency, Melissa Rotunno, Melanie Holloway, David Fares, Steve Metalitz, Doug Isenberg, Michael Warnecke and John Levine, Susan Kawaguchi and Wout de Natris.

All right! So, you've all received the report that I've sent out. I kind of pushed forward basically I think have – supposed to have one more meeting. We could sort of the call for two by telephone.

And it's, you know, pretty apparent at this stage where the areas of diversity are. And I don't see a lot of convergence. So, I suggested the four propositions.

And two of those were a call for basically straw polls. It should probably best be conducted by email but we can discuss our opinions about what positions to take on this call.

Palmer Hamilton: Milton, can I ask a procedural question on the straw poll? Are you talking about by constituency or are you talking about a head count?

Glen De Saint Gery: Please identify yourself when you speak.

Palmer Hamilton: Surely, this is Palmer Hamilton.

Milton Mueller: I was talking more about a sense of how the constituencies are arrayed on that issue. Definitely not a head count. We're not supposed to be voting on this but I want to know very much where the different parties stand on those two issues.

Palmer Hamilton: Not a formal vote but still by constituency. A vote but not in terms of being a formal vote that…

Milton Mueller: Yeah not even a formal vote in the sense that we're counting numbers if more to – if basically we discover that nobody disagrees to something, it would be easy to go forward. If we discover that people are all over the path, then we pretty much know where we stand.

Steve Metalitz: Milton, this is Steve Metalitz. Can I get in the queue when you establish one?

Milton Mueller: Okay. So, anyway, we have the four propositions and I would propose as our agenda today that we simply go down the list of those propositions and discuss them and decide what we want to do on them.

Maria Farrell: Milton, it's - is Maria for the queue as well please.

Milton Mueller: All right. You have a procedural point about my suggestion?

Maria Farrell: I do. Yes.

Milton Mueller: Okay. Why don't you go first then?

Maria Farrell: Okay, sure. Briefly, just to remind people that within this entire working group, we really have tried to steer away from polling, on voting because it's been so divisive in the past.

And if, you know, if we are trying to measure around support and agreement, I mean I can give people a rundown of exactly what we mean by those terms again.

And, you know, personally, I would defer to Philip as well on this but I really think we should try to avoid mechanisms of and have the potential to be divisive within the group.

Milton Mueller: Well, that’s definitely true. And that’s why I'm not calling it a vote but if - I don't know where people actually come out on a particular issue. I'm not sure how we can move forward.

Maria Farrell: Yeah, sorry. The other point really was also that we've tried to make this script very much open to observers to be fully – be full participants in the group.

Moving back to a constituency voting just didn’t seem to be especially opened to the new people we have involved on it. You know, the fact that we're really trying to take a fresh look at this issues.

Milton Mueller: Right. I – again, I'm not calling for a vote but if there happened to be eight people from the noncommercial side of the fence on the call, that’s precisely what I mean by paying more attention to how the vote is distributed among various stakeholder groups then it then to the actual numbers.

Maria Farrell: Well, can I make suggestion then? What if we were – what if you were to look at the various options and ask is there agreement? Is (thick root) relatively unanimous or almost unanimous in its support for something.

Is there just simply support so that the gathering of opinion behind it but there are some dissenting voices or is it simply a question where what we call an alternative view where there many differing opinions and really no gathering of agreements.

What I'm really pushing out is, you know, given that we're trying to move away from constituency from voting, we can call it holding or straw polling, whatever we like.

But it really is what it is. And is there another way we can get at measuring support without going down the road of voting and also of excluding people in the group.

Milton Mueller: Right! That’s exactly what I want to do. Let's take for example the structural approach for banks. I just want to know who supports that. And I don't want to make it a head count.

And I don’t want to make it a constituency GNSO type vote. I just want to know who supports that. So, can we call it an expression of support instead of a straw poll? Will that make people happier?

Philip Sheppard: Milton, its Philip Sheppard. Just to help, the way we had set up the subgroups was, as you're aware, to discuss and list options and in the either being a group options that are similar so that we have a manageable set of things and to look at as a group as a whole.

And that was based on the fact that we had three questions and there was overlap in all of those. So, that’s at some point needs to go to the wider group for this sort of exercise.

I think it's clearly informative I think for the subgroup to – in the way that it listed its options in this sort of final vote or whatever the subgroup for perhaps, indication they're saying and answer that nobody disagreed with this but with option one, you know, there was mixed feeling about option two or something like that. I mean that sort of feeling would be fine.

And that that thing you need to be anymore definitive of that at this point because we'll be taking as best as we can gauging support in the bigger group subsequently based on the output for that you're producing.

Milton Mueller: Well, I understand that. But I think that we're simply – there's no way to avoid at some point asking people whether there's support for something or not.

Philip Sheppard: Uh hmm.

Milton Mueller: And we can save the larger group which is going to need all the help it can get - a lot of time by finding out things where there is substantial agreement and things where there is a – that can be taken pretty much off the table or at least identify those things that have a very limited amount of support.

Ross Rader: But Milton, it's Ross here. So, if I can jump into the queue on this question?

Milton Mueller: All right. Steve, you were in the queue. Would you address our same question?

Steve Metalitz: Yeah, I'll pass. Most of what I was going to say was raised by Maria and Philip.

Milton Mueller: All right. So, go ahead Ross.

Ross Rader: So, I joined this call late as well. So I only caught the last half of the discussion. But if I understand it right, it leads me to a question from Maria which is, in participating in the last call, I noticed that, that (Jon) has somehow captured feelings of those participating in that last subgroup. And how did he grow about measuring that, Maria?

Maria Farrell: He pretty much – a number of ways but mostly he really asked if there was support and then he himself - chair, made an assertion as to whether there was support for something or agreement on it and circulated it in the draft and people were then free to raise, you know, their objections to that which in fact I did on one of the cases and the things who create happy, you know, some pretty satisfied people that it did reflect what the group thought.

Milton Mueller: Well, then that's what we're going to do here. I'm going to eliminate the word straw poll and I'm going to ask how much support there is for the word of the various things. But then on two of the propositions I suggested the – the ones where I suggested a straw poll.

I really have no idea based on our discussions whether there's any preponderance of opinion in any particular direction. So, what I'll propose is that we discuss those propositions not that we hold straw polls, we'll have a discussion and we'll determine through that how much support there is and I'll draft the report which people can say whether it expresses their feeling as to how much support is out there or not. Okay?

Maria Farrell: Thanks Milton.

Milton Mueller: All right. So, I – on proposition A, I declared that there seemed to be consensus that law enforcement agency – public law enforcement agencies can be recognized categorically as a party with a legitimate need for access.

Now, based on Avri’s comments on the list, we're not saying anything that (unintelligible) about how they get that access. What kind of certification or procedure they go through but in principle, we're simply saying that nobody here can see those situations in which law enforcement agencies would never be granted access to the shielded OPAC – OPAC shielded data. And that they all can conceive a situation and there would a legitimate claim. And it's just a question of defining those procedures.

So, does anybody disagree with that?

Ross Rader: Can I ask you a question of definition, Milton?

Milton Mueller: Sure.

Ross Rader: When you refer – and this is going sound pedantic – but I think it’s an important question to ask. When you're referring to law enforcement agencies, you're referring to those agencies with the legislative mandate, is that correct?

Milton Mueller: Yes, I'm talking about governmental agencies that are empowered to enforce the law, to police the law.

Ross Rader: Okay. Thank you.

Milton Mueller: So, I – there's no, no disagreement on that proposition A that I'm hearing. Is that correct? Going once. All right, so that was easy, as I suspected.

Now, I made another statement. And this is a more controversial statement as it should be but it's also what logically precarious in the sense of disapproving a negative. But I found a great diversity and not much movement that's discernable on the issue of private party access.

And I proposed more of an operational thing. Maybe that kind of a proposition doesn't belong in the report. But since we do have about two weeks left, I thought it might be constructive to concentrate our time on LEA's.

But let's remove that from consideration for the moment and talk about private party access. Does anybody believe that there's some kind of a solution or a pro-(unintelligible) have been discussed or could be discussed that would achieve widespread agreement in this group?

Philip Sheppard: Philip here, Milton, just a clarifying question. Are you saying that you believe that's the case both for query based and bulk access and the case of a specific domain request that was even for that latter smaller case there was a chorus of voices saying no, never?

Milton Mueller: I think – I think you're identifying a good point which is that the proposition D, the last one about the type of – is my might be logically prior to the proposition B.

That is if there was widespread agreement that private party access would be limited to type one, that is access limited to the records of a particular domain or registrant suspected causing problems at a specific time. Then it might be possible for this group to reach agreement.

So, Philip, do you think we should consider proposition D now?

Philip Sheppard: Well, yeah. I mean just in terms of – I mean for me, as I say, we're listing options here and just making some comments about them. So, I said it's always easier to do the easier win first. And if that’s going to be one of them, then let’s give it a go.

Milton Mueller: Okay.

Wout de Natris: This is Wout from APTA, can I give comments?

Milton Mueller: Sure.

Wout de Natris: Okay. From what I know from the practice of private parties that are active in the anti-spam business so to say, is that they sometime litigate privately against spammers.

And that in able – to be able to do that, they will need some sort of access to the data. The question is whether that has great haste or it's something which is investigated over time.

And I think in the case of banks with phishing, then, there probably is a high speed need for four banks to close a phishing site as fast as possible. But as usually one data records and do the banks need to find that data themselves or do they have a good relationship with law enforcement that are able to do that for them?

And when they want to private – privately litigate a person, they can get that sort of information through the usual ways in which you get this sort of information, I think. Is that something which will make the discussion easier also?

Milton Mueller: I think it's a good point. In my mind it raises the question of whether we should add a type four access in which private parties obtain the information via the intermediation of law enforcement. And I'm not sure whether this idea makes any sense.

But if that’s an option, it seemed to me to be a distinctive type of access in which they don't have direct access to the shielded WHOIS data. They simply get it from law enforcement.

Carole Bird: Milton, can you add Carole to the queue on that particular point please.

Milton Mueller: Carole, there is no queue. So, you have the floor if you want.

Carole Bird: Thank you, just a quick point of observation here. I think that for certain – can I make the global statement that police or law enforcement agencies are allowed to give access to data in a database which is not their own.

That is to say that if police have access to a database, it doesn’t automatically allow police to give that information to somebody else even if the party providing access to the database.

So let's say, ICANN is allowing us to distribute the information. I'm not 100% convinced that we would actually have a lawful authority to provide that information to somebody else.

Now, having said that, I'm more than happy, Milton, to ask our access to information personnel if that is in fact an issue?

Wout de Natris: This is Wout from APTA, I could comment to that directly. We are by law, not even allowed to give this sort of information to a private party. And that could probably be so with the whole EU but I'm not sure of that. But I know it's a big discussion with spam databases around Europe.

John Levine: This is John Levine can I have the mic?

Milton Mueller: Go ahead, John.

John Levine: I actually was talking to (John Craig) does (does) exactly this could be the lawyer who works closely with law enforcement and (unintelligible) last year.

He tells me it works exactly the opposite from the way you're suggesting individual party does the research. And then it basically provides the law enforcement details and use to come to recollect this stuff in a way that it could use it in a court case.

So, for something that – for this to work, you have to flip it around and say that law enforcement could deputize people who they knew were working with legitimately on a case or something like that.

Milton Mueller: That’s exactly what's being suggested, John. This type four access should we decide to stick it in there is not a description of how things are now. It's a description of an option.

John Levine: Yeah, but I'm saying that the person doing the research would be the third party not law enforcement.

Milton Mueller: Well, again, the WHOIS information is out there. A lot of it (unintelligible) know, you have a name, you have a state, a country. And what we're talking about is getting the additional step, the street address and the other contact information.

And the question is whether we want to define as an option having the private party go to law enforcement for that which introduces some kind of filtering mechanism that might add legitimacy.

But as the law enforcement representative (unintelligible) pointed out, we make (unintelligible) obstacles to that in certain jurisdictions.

Philip Sheppard: Milton, this is Philip. I just have another perhaps like a naïve question. I'm also wondering if it's – if it actually matter to us if that’s the case or not.

Supposing with – supposing we end up with a conclusion, private parties (getting an) access to the information their law enforcement – and we give law enforcement some sort of access.

Well then, so what? Law enforcements going to make the decision regardless of our view.

Milton Mueller: Yes and that…

Philip Sheppard: I'm struggling a bit with believing that stuff that’s actually relevant for our discussion. I mean it's so much to saying as far as we're concerned, no private access, if law enforcement uses to do something of they assume allows them, so be it. But, you know, that’s outside of our box, isn’t it?

Milton Mueller: Right, so are you saying that’s not really a different of type of access for the purposes of this working group?

Philip Sheppard: I think, so, I mean I'm speculating just on the simple logical train of thought rather anything more technically related to WHOIS and maybe others who have a more expert view on that. But it just struck me that seemed to be the…

Steve Metalitz: I think it's a good analysis, Philip, Yeah.

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

Milton Mueller: Sure, go ahead.

Steve Metalitz: I assume we're now talking about this part of your paper - the degree of access granted part of your paper?

Milton Mueller: To agree of access (unintelligible)…

Steve Metalitz: And leading up to your proposition D.

Milton Mueller: Right.

Steve Metalitz: I was a little confused about exactly which proposals fell in which categories. Seems to me that type one, describes a lot of the proposals that have been made because – but it's also, they also have elements of type two.

For example, if you say that, let's just take the Bank One - the Bank one for example. If you say that – if you adopted Palmer’s proposal, then the bank would have query based access to any domain but limited in time.

But it would also, its access would be limited to the records of the particular domains or registrants suspected of causing problems at a specific time. They would not have the authority under their certificate or whatever, you know, under their terms of access to just access somebody’s WHOIS data that was not suspected of being involved in a problem at a specific time.

So, I'm not sure whether our number one - you're – whether number one is really directed to a proposal if we have any in front of us in which you have to get permission or you have to walk through the gateway each time and get your use approved.

Or whether it – I'm supposed to take it literally and say you have access to any domain that is suspected of causing problems at a specific time.

Dan Krimm: Milton, this is Dan, can I comment out of that?

Milton Mueller: Yeah, go ahead.

Dan Krimm: I think it's a good point. I think basically there are two different things going on here. One is the prescreening step does, you know - does the bank have to give a reason to access a particular domain? And then there is the questions of mechanics, how does that happen and if there are enforcement or violation or something like that.

But it seems to me that number two would imply that you don't have to have any specific reason to access protected data from a domain. So, you will just be able to get access to any domain for any reason.

Milton Mueller: That was my impression of for example, the ESA proposal and I think David Fares' proposal…

Dan Krimm: Right.

Milton Mueller: …was that you basically had a subscription to the WHOIS database, period. And once you were certified as – once you got that subscription through (unintelligible) of filing of an application and an affidavit, then you have the full run of the WHOIS database.

And I wonder (unintelligible) that the party – the private party is asking and saying the following domains are causing trouble. We want to know who's behind them.

Ross Rader: Milton, if I may on the subject.

Milton Mueller: You may.

Ross Rader: Thank you. I'm not commenting on any of these specific types that you've laid out here. But the first sense that you've, under degrees of access granted, you used the word can be granted.

I think this three – three or four degrees of access that we theorized would be useful to grant. But I question whether or not we can actually implement some of these types? So, we might want to be a little bit softer with our language, okay.

Milton Mueller: Okay.

Ross Rader: For instance, there is no mechanism right now to time limit query based access, not without replacing the entire WHOIS from itself.

Milton Mueller: Right.

Ross Rader: But it’s theoretically useful whether it's practically administratively possible is another story.

Milton Mueller: Yeah, you're – I mean, you're absolutely right. We have kind of deferred the practical and cost discussion but because we cannot confront it adequately until we know sort of what we want to do. But we may indeed discover that the kind of access we want to grant is either too costly or not technically possible.

I guess tech – you might say that anything is possible if you're willing to spend enough money on it. But yes, we might indeed find that. That’s a good warning to issue, Ross.

So, again, the proposition is if we can limit access to the records of particular domains and registrant suspected of causing problems, is that something everybody could agree that we should allow private parties to do?

Man: Say that again, Milton. I'm sorry.

Milton Mueller: If we can limit access to WHOIS – the shielded WHOIS elements to particular domains and and/or registrants suspected of causing problems at a particular time, is that something that everybody can agree private parties should be able to do?

Wout de Natris: How do you – Sorry, this is Wout from APTA, how do you determine who is giving trouble or is suspected of foul play?

Milton Mueller: That is a – that’s a practical question. And we are in the theoretical, right?

Wout de Natris: Okay.

Milton Mueller: Really…

Ross Rader: I was going to ask the same question.

Milton Mueller: But again, it's the type of access we're concerned about. If we don’t ever want to give private parties access, then somebody should speak up. If, you know, somebody believes that, should speak up.

So nobody objects, if it's possible, nobody objects to giving private parties access to particular domains and so on causing trouble?

Ross Rader: Yeah, I'm not sure I understand the question correctly, Milton. But there's way too many qualifications in front of that statement for me to be able to agree with it.

In other words, is it any private party - how is private party qualified. What are the odd? Like there's just way too many questions there for me to say yeah, that’s a great idea.

Milton Mueller: Okay. Well, yes.

Ross Rader: At least with law enforcement, the need is extremely clear. The stakeholders (unintelligible) is very, very clear and there's been several discussions around technology and applications that at least lead us to some faint glimmer of hope that the theoretical is practical. And I just don’t see it with this second set of question.

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

Milton Mueller: Go ahead.

Steve Metalitz: I think the – if I understand what you're covering by type one, there really are two different ways these could happen. It really boils down to who decides whether a query that’s made is limited to the record of particular domains suspected of causing problems.

I mean there are two ways you could do that. One is to say that every time, whatever the qualified private party is and leaving that aside, whenever they want access to a record they have to go to some gatekeeper and say, “well, I want this and here's why.” And the gate keeper says yes or no.

The other way is that they get some more general access under some – under a contract or a license that says you can only use it for these purposes. In other words, you can only make a query when you suspect a particular domain and or registrant of causing problems at a specific time.

And that’s the limit of your access and then the question is, what's the mechanism for enforcing that? But I think those are – those could both fit into the definition of number one as it stands now.

But I think, we would probably - most people will probably view those are rather different models. I'm just suggesting to maybe to unpack that.

Milton Mueller: I agree that that is a distinction that needs to be made. And I want to try to write that down. So…

David Fares: Milton if I – this is David – if I could just clarify, mine was meant - the five proposals was meant to include the latter.

Michael Warnecke: Mike Warnecke. Can I get in the queue please?

Milton Mueller: Go ahead, Mike.

Michael Warnecke: I'm sorry, I dropped out of the call a few moments ago so, I apologize. I just want a clarification on the type two access. Our proposal, the ESA proposal, I think it's too broad to say it's unlimited to access to all WHOIS records.

I mean we are limiting it to the third parties for specific purposes. So, I think that just needs to be clarified there. I don’t feel comfortable with the necessarily that characterization of our proposal.

Milton Mueller: Okay. But, basically, you agree that if you have the fact that you could make a request of any domain in the DNS?

Michael Warnecke: Well, to the extent it falls within the categories of purposes that are covered by a proposal. Yes.

Milton Mueller: So, that would mean that if you consider a, you know, just a complete data mining automated process of searching and scouring the entire WHOIS - a necessary part of doing your trade mark protection activity, then that would be legitimate under your view, right?

Michael Warnecke: Well, no. I mean, I – that’s not one of the purposes we identified and moreover, that’s not the way we go about using the WHOIS information for, you know, we – first there's a site that’s problematic and then we query the WHOIS database. We're not querying the WHOIS database at random looking for things.

Milton Mueller: But you would be able to with the kind of unlimited access that we're talking about under type two.

Michael Warnecke: Well, not under ESA’s proposal. I mean, and there would be the enforcement mechanism as well. But I realize, you know, you may not want to go into all that right now. But I just – I think it's important to clarify that, you know, it's not a rubber stamp, go get them, do whatever you want kind of proposal.

Dan Krimm: So, this is Dan again.

Milton Mueller: Yes.

Dan Krimm: Dan Krimm. It seems to me that a lot of the people that might have been suspected of being in favor of type two access are disavowing themselves of that.

And perhaps, the difference between type one and type two is really the breakout ahead just in previously suggested for type one which is really what the mechanics are. Is there a mechanical prescreening process or is there only post fact dealing enforcement.

Milton Mueller: Right. I think – and that's pretty much what I meant by type one and type two. Although I've put too much emphasis on limited and time and I should have been more specific. So, I think we can clarify that.

But the problem with type two, or not necessarily a problem, you may or may not consider it problem is that once that level of access is granted, it is the user of the WHOIS database who decides without any review who is a suspect and who is not.

And that could include quite literally, anybody for any reason. And the burden of proof has been shifted to somebody to prove that this is used for purposes, you know, that are wider than their claim to be.

So, I think that by granting type two access, you really are a pretty much - giving query based access to any domain. There may – unless you can – we don't want to get to the enforcement mechanism.

We want to really just talk about access now. But I think that there's a big, big difference between those two. And it really has to do with where the burdens lie.

We all know that that's, you know, what all these policy debates generally revolve around is who ends up suffering the burdens and bearing the cost of different kinds of policies.

So, of example if – I mean in my own – if taking my chairman's set off and talking as a, you know, constituency member and working group member, I think I could live with type one access granted to private parties, while recognizing that the cost of implement that are something that need to be looked at carefully.

Ross Rader: Actually Milton, it's – I'm sorry if there's a queue – I don't mean to jump it.

Milton Mueller: I don't think there is queue so go ahead.

Ross Rader: I'm going to re-raise this universe is practicing again, my understanding of the work that we're intended to do here is to build consensus around the areas where we can build consensus in terms of making the operational point of contact perform the more acceptable to a broader range of stakeholders.

And I bring up my previous concern again in a slightly different way by noting that that proposal is – it's most common denominator is port 43 access.

Until we hear a confident and concrete proposal that that is no longer an acceptable means of conducting a WHOIS service. I think we need to bound our discussion within the scope of the capabilities of that existing protocol or service. I don’t see any other way around it.

So, I hate to say that this is a, you know, just say it's theoretical issue let's keep talking until we can prove that we can't do it. The port 43 protocol is a very, very specific tool that can do very, very specific things.

So for us to go down the road any further of type one or type two access, it’s just not – the protocol will not permit that behavior.

Steve Metalitz: Milton, this is Steve. Can I ask Ross a question here?

Milton Mueller: Go ahead.

Steve Metalitz: Wouldn't that also be true of law enforcement access? I mean – I guess my question is how is law enforcement access differ from other third party access in terms of port 43?

Ross Rader: Well, the difference is that the law enforcement community is well bounded. It's identifiable and there – there's at least one proposal that I'm aware of that allows the port 43 service to be of service a slightly different data to the law enforcement community using encryption.

To the extent that private parties can be somehow qualified and accredited in the same way that law enforcement can, then it can be a (unintelligible). But I think we need to be explicit that that's the path we're going down.

Steve Metalitz: Okay. So, it's not as much a technical problem as a problem of is it practical to accredit and identify and bound if you will, the entities that have that access.

Ross Rader: What I'm commenting on, Steve, is that limiting access to the (unintelligible) of a particular domain or registrants, et cetera…

Steve Metalitz: Uh hmm.

Ross Rader: Type one access is not possible using port 43. Query-based access for a limited period of time is not possible using port 43.

Margie Milam: Milton, can I get in the queue, this is Margie.

Ross Rader: It's not possible to – unless people are limited to somehow – they can be a queries from a single IP address which I don't think anybody is proposing. There's no way to separate the wheat from the (chap) to the degree that type of differentiated access is required.

Milton Mueller: Okay, Margie.

Margie Milam: Yeah.

Philip Sheppard: Philip for the queue as well, please.

Margie Milam: Sure, I disagree with Ross. What's happening right now with the registrars is there is limitations on access on port 43. And it's done exactly as Ross indicated. It’s IP address based.

So, theoretically, we could have a white list of - with rate limits on, you know, depending upon the type of organization. And that is already done by the registrars today. So, there are limitation…

Ross Rader: Is that your legal opinion Margie, or is that a technical one?

Margie Milam: Oh, it's a technical one because we deal with it every day as a registrar. And in fact, ICANN has established a white list for registrars in order to do queries for registrar related business. And so, that compass is already in place.

Ross Rader: Okay, so, when you actually figure out the ways to keep (unintelligible) from scraping your WHOIS and reselling it, let me know.

Milton Mueller: Somebody else said they wanted to get on the queue but I…

Philip Sheppard: That was Philip. Thanks Milton. Just a question about – for the registrar in basically, I mean are you saying that despite our interesting discussion about one, two, three or even more type – degrees of access granted that in effect today, the only practical way is port 43 access.

Albeit, with limitation possibilities. And therefore, in terms of pragmatic implementation, we should only focus on thinking about that type of access and then decide who gets it?

Milton Mueller: That’s a question for Ross.

Ross Rader: I think what I'm saying there Philip is that port 43 is the lowest common denominator of access to the WHOIS data. It's a protocol with 20 years of history.

And it's nothing that can easily be thrown away. But to the extent that we're making propositions related to WHOIS services, it needs to be consistent with the realities of that protocol.

Certainly, the operational point of contact proposal was tabled within the late – our work is bounded by that council document at this point so I think it's only a natural extension that we take that into account.

Milton Mueller: I have a question Margie for you. And if (Jay Westerdal) is on, he might be interested in asking it. I know we've had some exchanges about this before.

But suppose that you are, you know, I know that you are a service provider. You do extensive analysis of the WHOIS database for anti-fraud clients and so on.

Suppose that you only had what the OPAC proposal publishes to work, wouldn't there be an extensive amount of analysis still be possible in terms of the, you know, analyzing patterns of the OPAC listed the names, the jurisdiction listed, the domain name, IP address and name servers and so on.

Could you still – how much would your work be hampered if you only had the - what the OPAC publishes – what the OPAC recommendation publishes to work with?

Margie Milam: I'm sure. If the OPAC becomes a proxy service, so in other words if the OPAC's information is not really the registrant's information, that's where the analysis - where it's difficult to have analysis – that kind of analysis that we currently have.

Milton Mueller: So, the name and the jurisdictional information and the OPAC itself is, you know, presumably something that would have to be invented or something by a fraud, fraudulent person. So, I'm sorry – go ahead.

Margie Milam: Okay. So, for example, to say for the sake of argument that the OPAC is participating a registrar's information or some sort of proxy type information. The information that's missing in the current OPAC's proposal is we wouldn't have access to the address and the email address of the registrant.

And that's very key in the analysis that we do for fraud related purposes because if it's – I send an email add to this effect that is if the domain name registered say, bank of America online or something and you look at the – and if you can look at the email address for the registrant, if it doesn't say, you know, some address @bankofAmerica.com and instead says, you know, Margie@aol.com, that's a red flag where we can identify that that's probably a fraudulent side. And, you know, the information, we need to dig further.

Milton Mueller: But wouldn't, you know, for example, couldn't you go to the legitimate bank of America site to see who the OPAC was and compare to that or look at the country and state information and see that that's not the name that's any way associated with bank of America?

Margie Milam: Yes, you could. You could certainly look at the OPAC information. But the reason why the registrant information is useful is because I believe that's the information that the registrar would use to provide information to that registrant.

And so, you know, I just don't know if we'll have a complete, you know, information to be able to make that leap. And fraudsters would, you know, they theoretically could mimic the information of the bank and the OPAC information.

Milton Mueller: Right.

Dan Krimm: Milton, this is Dan.

Milton Mueller: Dan, go ahead.

Dan Krimm It might be (as well) for us to consider the difference between direct access and indirect access because access in the general sense is a wider policy matter (unintelligible) access to port 43. It seems to me that's what type one might be about is the indirect kind of access.

Milton Mueller: I'm sorry. There was some noise in the middle of your talk. What could you…

Dan Krimm: I was suggesting that we distinguish indirect access from direct access with direct access being port 43 and indirect access being some kind tiered access or prescreened path along or something like that.

Milton Mueller: Okay, that’s a…

Dan Krimm: It seems to me that that’s kind of what we're aiming for with type one access.

Milton Mueller: And indirect means a technical process or a legal, social process?

Dan Krimm: A legal, social process but probably if it's going to be implemented on a timely basis, there would have to be a separate technical process constructed to assist that.

Milton Mueller: Okay. So, I think Margie made an important point that we are in fact limiting port 43 access of…

Ross Rader: Milton, it's a false – a completely bad bit of technical advice for Margie that why I'll be happy to walk you through why but it's not possible today to actually authenticate anyone using port 43. And given the degree to which IP addresses can be spoofed. The mechanism should just completely fall off.

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

Milton Mueller: Go ahead, Steve.

Steve Metalitz: Yeah, again I'm not sure I understand how port 43 impacts on this. My understanding, let's assume the OPAC proposal was adopted, then via port 43, you – anybody coming in via port 43 would have access to the data that’s public. It would be the name, province and country and the OPAC data. That’s all for port 43.

And the other data that’s collected, the other data about the registrant and presumably still they had been in tech contact data unless that’s changed. That would be in a – somewhere else.

And we're talking about who has access to that data and under what circumstances and how. But there's no presumption that they would be gaining access to that data via port 43, is there?

My understanding is that it might – it wouldn't necessarily be through port 43. But the question is who has access and under what conditions.

Ross Rader: I think it's a fair question, Steve. It's certainly been my assumption that it would happen via port 43. But it's a fair question.

Milton Mueller: So, as opposed to port 43, it might be you send the message to the registrar or the OPAC, right?

Steve Metalitz: Well, yeah. I mean there's a lot of ways it could happen. It could be web based access, it could – I mean, yeah. You might – it could through email exchange.

I mean it really gets to the question with distinction, I was trying to draw between type one and two or one-A and one-B which is, is there a gate keeper who says, “It's time, yes you can have access. No, you can't have access,” or do certain entities get more or less a subscription or some kind of access for certain purposes. And but either way, I don’t assume that it would be through port 43.

Milton Mueller: Well, that complicates things even more doesn’t it? I guess that’s email or OPAC falls then to the category of what Dan was calling indirect access, if you want to call it port 43 direct access.

But I think I agree with Ross that the established mechanism for providing WHOIS now is indeed port 43 and that’s the kind of rapid query based access and most people are interested in actually having. And the other kinds of access raise barriers that don’t exist on port 43.

Let me try to wrap up this discussion.

Ross Rader: You mean for now, right?

Milton Mueller: For now, we're going to have to reformulate our access options obviously. But in the most generally principal terms, then what I'm hearing is that we cannot come up with a complete report for the idea that access to private parties could be granted even if it is limited to particular domains and registrants and some of that like of support stems from questions about the technical viability and some of it stems from not enough knowledge about who is going to be granted this kind of access.

Is that correct?

Ross Rader: It certainly summarizes from my perspective, Milton.

Milton Mueller: Now, I would like to get – make some progress on the bank proposal if we could. Is there anybody who opposes other than me? I think I've made my opinion clear and that it has nothing to do with the merits of the bank proposal per se but with the idea of tackling the problem on a sectoral basis.

But is there anybody else who does not want to try to solve the problem at least for one sector, that is if you could make a case that we're not going to agree on much.

But we've taken law enforcement and agreed to do something about them. Should we also try to do something about banks or does anybody oppose that other than me?

Dan Krimm: Milton, this is Dan.

Milton Mueller: Yes.

Dan Krimm: I still am not quite sure why if we can come up with an effective solution for banks. It couldn't be extended to other sectors generally unless there's something really specific about the bank regulation, paradigm for law enforcement that it can't be extended. But I'm still – I solved questions about that. So, I probably would oppose it for that reason.

Philip Sheppard: Milton, Philip here. Just probably as a work around, I mean, I think what may be useful rather than promulgating bank as an option to go forward, but just using banks for now as a possible private sector model.

Given that there are some characteristics in terms of the regulator regimes surrounding banks. It might make it easier.

And therefore, that model could then be looked at it - at its robustness for other good it might have merit and might solve the concern you have which I share and that I don't think it's ultimately useful to have a sectoral approach. But if we can pursue an approach as a paradigm, that may be useful.

David Fares: Philip – sorry, this is David Fares. Can I just chime in on that?

Ross Rader: If you could put me in the queue as well please Milton.

Milton Mueller: Okay, David and then Ross.

David Fares: I think that that's interesting if we consider this as an example but I wouldn't want it to be qualified in such a way that banks have been highlighted because they are regulated.

Those of us that are not in regulated sectors still have – I would consider have legitimate needs for access to do it. But I would just one with that caveat included in it if this is going to be serving as an example.

Milton Mueller: Okay, Ross.

Ross Rader: I was only going to make the point that it maybe that the banking industry shares more similarities with law enforcement. It may be useful to frame up the question in terms of to the extent that those similarities existed maybe interesting for us - useful to open up that question at a future date.

And that can verily to the extent that there are other sectors that share those same characteristics we may wish to implement some sort of a – once we proved ourselves with the law enforcement access that maybe useful opening up to other sectors.

So, I don’t necessarily share the caution that the sectoral approach isn’t the way to go. But it – I believe that our first step with this is the law enforcement sector.

Milton Mueller: Ross, I can't – make a lot of sense out of the position in terms of preparing a report. Can you tell me when you talk about deferring…

Ross Rader: The question for me right now is whether or not we can get access right for law enforcement because it's a clear distinct group to the extent that there are other clear distinct groups. We may wish from a policy or from a procedural basis to roll this type of access out to those groups in the future.

In other words, I would – for not (unintelligible) something else. This is for banks right now until we actually understand what's going on with this first (unintelligible).

Does that make more sense?

Milton Mueller: Yes, it does. And so, that is basically a very soft no to the…

Ross Rader: I just don’t know enough about banks at this point. And I'm still trying to wrap my head around law enforcement. So it can't get much more…

Milton Mueller: Yeah, the key point…

Ross Rader: …complicated than that.

Milton Mueller: …you think that law enforcement should serve as a model for banks possibly in the future. And Philip is saying that banks might serve as model for other private sector actors. So Philip's position is again somewhat ambiguous in terms of how I draft it up and its operational implications.

And as far as I can tell, David Fares' concern is only that he doesn't want private sector to be categorized on the basis on regulated industries to get some privileges and others don't.

So, David, I – you know, what are you saying about going forward with the bank sectors specific proposal for banks?

David Fares: As I understood Philip's suggestion it was that we would use the bank right now as an example. But we would not determine whether or not it would be a sector specific or generic approach for private path. Is that correct?

Philip Sheppard: Yes, absolutely. I mean I think without making any value judgment, I mean my interest would be assessing its practicality. And once you've done that, that should help us assess the practicality for other groups.

Wout de Natris: This is Wout from APTA, can I get in the queue?

Milton Mueller: I wish you would. Yes.

Wout de Natris: Thank you.

David Fares: Do you want me to finish first, Milton, I'm not sure.

Wout de Natris: Oh, sorry.

Milton Mueller: I'm sorry if you were not finished.

David Fares: Yes. So, with that in mind, I just don’t want there to be a distinction that would be carried forward between regulated and non-regulated given that that is simply an example. That was my point.

Milton Mueller: Okay, so you're basically agreeing with Philip but you just don’t want that distinction to be based in any way on regulated versus unregulated.

David Fares: I would say if – if we proceed in the way Philip suggested, that’s my point.

Ross Rader: And sort of clarifying my point, Milton. I'm agreeing with Philip but I'm saying that banks are the wrong places to start.

Milton Mueller: You may be right.

Susan Kawaguchi: Philip -this is Susan Kawaguchi. Can I get in the queue?

Milton Mueller: Yes. Wout and then Susan.

Wout de Natris: Okay, thank you. What I think, from my perspective is that it should be clear why private parties want access. And what do they need access for? And only then we can determine whether they have to have generic access or whether individual access per case is sufficient and how much of the whole database they need to see? And I think only then if you identify that per private actor, I think you can proceed and on to see in which way they need access.

And by granting them generic access, you probably will give away too much from a privacy point of view. That's my point. And I'm sorry that I have to dial off now because I got another meeting. If there are any questions, please send an email and I'll be glad to answer them. So, bye-bye for me.

Milton Mueller: Thank you very much. Well, that's Wout's statement I would take as a statement of support for the idea that if we're going to get private parties access, it's going to be what we've been calling type one access.

Of course, that position has been complicated by our discussion of the types – type one by the complications of actually delivering that kind of access.

All right. So, Susan.

Susan Kawaguchi: I just don't think we should focus just on the banks. I think there's a lot of legitimate users out there and a lot of categories we could establish. And we should look at all legitimate users and then define their access instead of just focusing on banks.

And maybe down the line, focus on other groups. So, I would be very hesitant to agree to anything where we have to evaluate every legitimate group for access.

Woman: This is (unintelligible) we turn on (unintelligible). I agree with that because then of all legitimate (unintelligible) in bank (unintelligible) identifying (unintelligible) the legitimate stakeholders that need access.

Milton Mueller: I – am I the only one that could…

Ross Rader: No. I couldn't understand that.

Milton Mueller: There was a very static field intervention of – I could not even tell who it was.

Man: Milton, can I just ask a quick question? How much longer are we going to go? I have a 10:30 meeting.

Milton Mueller: Two minutes. I…

Man: Okay.

Milton Mueller: I do too. So, I think I have a pretty good sense of how we fall out on the bank. Is there anybody with a completely different position on the bank issue?

All right. So, I will revise the report based on this discussion. It's been I think a very beautiful one. And the report will be much more precise next time. And next week obviously the discussion will focus on access mechanisms. And thank you very much for participating.

Woman: Thank you.

Woman: Thanks (Susan).

Man: Good bye.

END