WHOIS Working Group B "Access"
Teleconference
TRANSCRIPTION
Wednesday 16 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 16, 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-20070516.mp3

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

Attendance:

Milton Mueller NCUC chair - wg chair

Yaovi Atohoun - observer

Carole Bird - observer

Patrick Cain - observer

Bertrand de la Chapelle -observer

Wout de Natris - observer

Avri Doria - NomCom council

David Fares - CBUC

Palmer Hamilton - CBUC

Doug Isenberg - IPC

Susan Kawaguchi - CBUC

Tom Keller - registrar

Ross Rader - registrar

Dan Krimm - NCUC

Shaundra Watson - observer

Steve Metalitz - IPC

Margie Milam - Registrar/IPC

Palmer Hamilton - observer

Melissa Rotunno - observer

Suzanne Sene - observer

David Maher - gTLD Registries

Michael Warnecke - observer

John Levine - observer

Ken Stubbs - registries

Wendy Seltzer - observer

ICANN Staff:

Maria Farrell - GNSO Policy Officer

Glen de Saint Géry - GNSO Secretariat

absent apologies:

Philip Sheppard - WHOIS wg chair

Glen de Saint Gery: I'll do the roll call for you Milton.

Milton Mueller: All right.

Glen de Saint Gery: We have on the call (Yaovi Atohoun), Palmer Hamilton, Dan Krimm, Avri Doria, Melanie Holloway who is from eNom, Susan Kawaguchi, yourself, Doug Isenberg, (Melissa Rotuna), Wendy Seltzer, Michael Warnecke, Thomas Keller, Carole Bird, Patrick Cain, Margie Milam, Wout de Natris, David Fares, David Maher, Shaundra Watson, Ross Rader, Bertrand de La Chapelle and Steve Metalitz. Have I missed anybody?

(Yaovi Atohoun): (Yaovi Atohoun).

Glen de Saint Gery Yaovi Atohoun yes, I mentioned you in the beginning. Thank you.

Yaovi Atohoun   Thank you.

Milton Mueller: All right everybody. Welcome! I have been a little unprepared this time. I'm actually on the road. I'm in Washington now. So, I did not send out an agenda. Let me suggest one to begin with.

We received the (fuming) proposals. Someone at the last minute, I guess it was yesterday they started coming in, maybe one the day before. What I've tried to do was prepare a framework that shows the sort of the similarities and differences among the proposals.

And I sent that to you last night, very late as I labored to handle this stuff. Is everybody familiar with that? Let's say, is anybody is not familiar with that, can they speak up? Okay, sounds like most people have received that framework.

What I'd like to do is explain how that framework provides the basis for comparing and contrasting proposals. To that first, then I would like to discuss the three new proposals I know about within that framework and that would be the Kawaguchi proposal, the ESA proposal and the Margie Milan's proposal.

Is there another proposal, another new proposal that I'm unaware of? Okay, sounds like there's not. Silence is golden. So, we would briefly discuss those proposals and then I think we need to start actually discussing what it is possible to agree on.

Going after the (loaning) and truth first and then getting to the more difficult issues either at the end of this call or next week. So, how does

that sound as the skeleton agenda? Anybody think we need to add anything?

I feel like I'm talking to myself. Is anybody there?

Woman: (Unintelligible).

Man: Yup. We're here.

Man: We're all here.

Milton Mueller: Okay. So, I take it that we are completely unified at least on our agenda. That's good. All right, let me go quickly through the framework. The idea was that we're basically talking about - I think the points of – key difference at this point breakdown into three areas which is which third parties are we talking about, what kind of access filtering mechanism is in place and then the type of access.

Now, in the third parties, I've basically broken it down into two options. One of them is law enforcement agencies and the other one is anyone with the legitimate interest.

I know that there are proposals that speak to the needs of specific third parties that are not law enforcement agencies. But – and somebody might want to challenge this but it's my opinion that those proposals and basically making a take for a particular group such as banks or service providers. But there's nothing inherent in those proposals that would not allow the same logic to be applied to any group.

So, basically, I'm lamping those proposals together under the idea that they're all saying that somebody other than the Law Enforcement Agency has a legitimate interest to access the data in some way.

And I find it difficult to conceive of how we could go forward with a – what I call last time a specific sector proposal. That it would be difficult to say we come up with a proposal, it applies only to, let say, banks. And then we would have potentially 15 or 20 other particular sectors that we - that might make similar claims. So I think we have to be more general than that.

So I'm framing that as LEA's versus anybody in society, any private actor who might think they have a legitimate interest.

Man: Milton, may I ask a mechanical question?

Milton Mueller: Sure.

Man: As I understood how charge as subgroup and - correct me if I'm wrong on this – what we're supposed to do is come up with various options or the full working group to consider and we're to refine those options so that they can be considered by the full group.

We're not going to win all options except to the extent we might massage them so that they can be more or less alike in terms of your template that you sent out a couple of weeks ago. I thought it was a very useful tool so that they could be compared and contrasted and refined. Dan, for example, has suggested some very useful ideas that we're working on to amend that proposal.

That's point one, if I'm wrong on that, how do we, I mean - well, first let me ask you if I'm right in my view of what it is that we're doing as a subgroups.

Milton Mueller: Yeah, I think that we are developing options, laying it out on the table as you've said. If we are able to win all them that is, if we're able to say, you know, "We don't want to go these groups." Is any particular approach to something gets a certain level of agreement. And of course that would be welcomed by the full group, I'm sure.

The full group is going to have a tough task at getting agreement as it is. So, if we can give them a smaller set of options than a bigger one, that's good. But fundamentally, I think you're correct that we are here to clarify and elaborate proposals. And then those people who are making proposals that are similar are basically going to be grouped together as much as possible.

Man: But if for example, on our bank proposal, if we wanted to have our proposals go forward, you're not suggesting we won't be able to, are you, unless we chose to combine something?

Milton Mueller: Right. I'm not suggesting that. I think the best way to handle that would be to simply enter into the record the caveat that I just mentioned about the sector's specific proposals.

In other words, if you found a generalized proposal about private party access that – in that your need, as the banking sector, I think you'd be happy to have that more general proposal pushed forward rather than the specific sectoral proposals?

Man: Well, I think we've, I would be inclined to leave both on the table for the working group as a whole to consider.

Milton Mueller: Okay! Well, I think that's something we can discuss when we're maybe at the next stage of the game?

Man: Sure.

Milton Mueller: But I have no intention, I mean it really doesn't do anything to take off things from what goes forward at this point if there's no agreement on that, you know. I mean I could possibly say, you know, its chair to somebody that I don't like this proposal or that proposal and I could may even - maybe get six to seven people to agree with me.

                 But if the people who don't agree with me aren't satisfied, they're going to bring up what they want in the final consolidated working group anyway. So, you know, the process here is designed to narrow options as much as possible on a consensual basis.

Man: I see. May I ask one more mechanical and then I'll be quiet?

                 The three different issues - would you want – one was which third party should have access, the second were filtering mechanisms and what did you say the third?

Milton Mueller: The types of access.

Man: Okay.

Milton Mueller: It's in that PowerPoint file. Did you get that?

Man: Is that the one you sent out last night?

Milton Mueller: Yes.

Man: Oh, okay. Yeah. Yeah, I don't have it now.

Milton Mueller: So those are the vertical dimensions, the columns.

Man: Okay. I've – I have it on my Blackberry so it's not…

Milton Mueller: Oh, okay.

Man: ...(unintelligible) yet, it probably makes more sense when I'm able to print it out.

Milton Mueller: Okay. Or view it on a bigger screen.

Man: Yeah. Yeah.

Milton Mueller: I'm paperless my self.

Man: Yeah.

Steve Metalitz: Milton, this is Steve Metalitz. Are you taking a queue at this point or did you want to go through your whole presentation?

Milton Mueller: I think it's – what you're saying is relevant to this discussion we just had, go ahead.

Steve Metalitz: Okay. Well, I just think that to - for your left hand column to consist only of LEA's and anyone is not really representative of what's in some of these proposals. And for example, Susan Kawaguchi's proposal as a multi-tier proposal was recognizes or it (pauses) there will be several different categories. And they might have different gateways and different types of access.

Of course, Palmer's proposal was not either an LEA proposal or and anyone proposal. In fact, it really combines elements of both. And I just think it's not realistic to say…

Operator: John Levine now joins.

Steve Metalitz: …that some proposals shouldn't be reflected here because they're too complicated. It maybe this is a complicated problem and the answer to it maybe complicated. And it may not be just one track for law enforcement and one track for everyone else. So, I think that – I guess I would object to the way it's been portrayed here, at least in the left hand column because I don't think it reflects proposals that are really in front of the groups.

Milton Mueller: That's funny. Again, I didn't have time to include Margie's proposal. But I do think Kawaguchi's proposal is the two-tier then I think it's very actively reflected in the second slide. In fact, it was her proposal that inspired this diagram because I was trying to relate its similarities and differences to others. And I came up with this model.

The problem is, yeah, you can come up with like the EFA proposals comes with a long list of parties. But basically, those parties are more

like criteria or a legitimate use. And those criteria could be asserted by anyone.

And I see the same with Kawaguchi's and I don't consider that a weakness of Kawaguchi's proposal. In fact, it's a straight in the sense that anyone can assert one of these lined affidavits. And under the Kawaguchi's proposal, they get a fairly limited type of access where the LEA's get the more extensive kind of access.

So, you know, I think it would just be confusing the issues to have a bunch of very idiosyncratic and multiplicative categories in this third parties thing. I really think we fundamentally are talking about new categories. We may disagree on that and that can be reflected in any ongoing reports that we forward. But I do think it's much more to think of it as – and let's say, the very clear, crisp operationalizable distinctions.

We're really talking about somebody asserting that they have a legitimate access need and we're talking about LEA's. I don't see…

Steve Metalitz: Are you drawing at distinction? I mean LEA's are certain they have a legitimate access need.

Milton Mueller: Because LEA's can be easily certified as the distinct category of actor.

Steve Metalitz: You're making an assumption there that I don't think is really justified by the discussion we've had at the proposals. It may be easier to certify for example, who's a bank than certify who's the Law Enforcement Agency. Certainly in United States that would be much easier to do.

Milton Mueller: But the category – they have no categorical difference. I've seen asserted between the needs of banks for that information and then in needs of trademark owners for example. It wasn't needs of…

Steve Metalitz: But those are different groups, I mean on the one hand, you're saying that these are simply different people asserting needs and the other hand you're saying they're different groups. I mean, and then you're saying your different groups. I mean there maybe a different path for a bank than for a trademark owner.

Milton Mueller: Yeah…

Man: Can I make a comment there?

Steve Metalitz: …commerce proposal, it goes through the national Bank Regulatory agency. There isn't a national trademark regulatory agency in the same sense, although perhaps we would incorporate that too. But these are two different groups that might have two different paths.

And it's not – I'm just concerned that people who aren't participating in this group and who see this PowerPoint are going to say, "What do you mean anyone can have access to this data?" The whole idea of the OPAC proposal was to deny almost everyone's access to this data. So, I think it's somewhat misleading.

Milton Mueller: No. I - well, it should say anyone of the legitimate need the, you know, the constraints of PowerPoint and diagrams. But we could turn it into public or private actors if that would be better. I think that maybe might reflect in some ways the distinction I'm drawing.

Susan Kawaguchi: Yup. This is Susan Kawaguchi. And I really think we need to get

                    sense of distinction between the different groups and the different

                    needs because I don't think that's been thought through. And I mean

                    that was one of the reasons I listed everybody we could just really

                    came out of a different working group I was on.

                    And we spent many weeks sort of figuring out what organizations. I

                    don't see and I'm sure we've missed some. But to just group those all,

                    as anyone, I think Steve's right. We're going to get back to, you know,

                    let's just make it all private. So…

Dan Krimm: No. This is Dan. I have a contrasting deal. It seems to me that the

                    grouping of which third party should follow how many different

                    categories of access gateways there are. So, if you will only have two

                    different kinds of access gateways, then that define two different

                    groups, it seems to me.

                    So, if you've got, you know, LEA's or national agencies and then

                    you've got an affidavit process to cover other legitimate third parties,

                    then if all of the other legitimate third parties are using affidavit

                    process, then there's no functional difference between them. That's –

                    as you say, its listed categories that would apply.

Susan Kawaguchi: I do see a difference in, you know, different organizations having

                    sort of a different level of access. I mean, I didn't, you know, outline it

                    completely in this proposal but I think if we thought it through, we

                    would come up with, you know, financial institutions maybe better

                    access and, you know, real time access compared to either a

                    registrant or an IP.

Man: If you put me in this queue too please don't miscount stuff.

Milton Mueller: Susan, let me just give you an example before I recognize Ken about what, you know, the reason I collapse your categories. You have fishing, takedown services, anti-parent services and brand monitoring services and then at the second one you have IP owners. And then you have consumers in the public.

                        Now, what really is the difference in the legitimate needs between those categories?

Susan Kawaguchi: Well, in some ways, you know, as eBay takes care of fraud issues, we need real time access and we need to have it, you know, we need full access to all the information out there.

                        From brand enforcement, maybe I don't need to see that information upfront. Maybe I can have a brand monitoring services out. And I wouldn't have access. I just need to – I just know that, you know, the domain name eBay whatever dot com is an issue for me. And I need supports upon that.

                        So, there are different – there are, you know, there's a lot of a different distinction on what these different legitimate users need and how and why they need it and how they need it.

                        Now, I didn't want to make a proposal that was two or three pages long but…

Milton Mueller: But I really - honestly I don't see the difference. In each case, you have somebody is using the domain name in a way that is in somehow is threatening presumably some right of the private parties.

And the private party wants to find out who is behind that domain name.

Susan Kawaguchi: Right. But it's the way that I need to see that WHOIS to be different. That's my (unintelligible)…

Milton Mueller: It might be but that's an accident question. Isn't it?

Susan Kawaguchi: Right. It is.

Milton Mueller: See, what I'm concerned about is – I think if you're concerned about sort of the propaganda value of the word anyone, we can fix that. That's just a label. Okay. Don't worry about that. If that raises bad overturns to you, we'll change that. The court – the (point) that I'm making is private actors of all categories.

Part of our own saying is a factual point. Part of it is a normative point related to what Dan was saying. The factual point is that it's very hard to distinguish and categorize private actor's need for this information in a way that really holds up. And you don't want to create a more (asset) of regulation that are different based on a bunch of arbitrary categories.

The normative point is I don't like the idea that certain groups in the society would assert a stronger need than other groups simply because that they are more prominent in a political process or a

lobbying process. It is not clear to me that the, you know, the needs of a brand owner or - are more important than needs in the individual who think they've been defrauded by a website.

Obviously, one group is more well-organize and has more resources than the other. But it doesn't necessarily mean they have more rights to be recognized as a legitimate third party.

But I think it's simpler and it's actually both just the case for certain kinds of institutionalized access if that party is defined as broadly as possible. So, they're talking about rights here, rights to access data. We're not talking about special needs yet.

((Crosstalk))

Milton Mueller: Anyway, was there anybody else in the queue? Ken Stubbs was and I forgot about him. Sorry Ken, go ahead.

Ken Stubbs: No problem Milton.

Bertrand de La Chapelle: I'm Bertrand, if can get in the queue.

Milton Mueller: Bertrand.

Wout de Natris: This is Wout I would like to get in the queue also please.

Milton Mueller: Okay. Let me just make sure I've got everybody. We have Ken Stubbs, Bertrand and what was the third person?

Wout de Natris: Wout de Natris from APTA.

Milton Mueller: Okay, (Wout de Natris from OPTA. You'll be third. Ken.

Ken Stubbs: Yeah. First of all, whether we like it or not, I think we all have to admit
this that a lot of the issues that are popping up tend to be the result of
distrust that the process maybe abused by a parties on both sides, you
know, and depending on which perspective you were looking out of
that. I'm afraid that is a legitimate concern that wraps in people's mind.

I have – I would say – I won't say serious issues but the overwhelming
majority of fishing I guess for my own personal email comes from
emails representing financial institution. I know based on discussions
I've had both with web hosting companies and with ISP's as well that
these are very short term deals and there needs to be an opportunity
for financial institutions to protect not only their own assets but
anybody who's even been the victim of identity knows it's an incredibly
honor risk task to clear your reputation up.

And my brother actually just has gotten going through it. So, from a
practical template, there has to be process that allows the opportunity
for financial institutions to get access to this information take it down as
quickly as possible.

It would be nice to assume that a financial institution could pick up a
phone call Law Enforcement Agency and that the Law Enforcement
Agency would act in the timely manner. But I'm inclined to think that
that's not necessarily going to happen.

So, I would hope that as we move on down the road and we start
setting up guidelines for access, we provide some sort of a stratified

system or a system that allows for accelerated access with people with legitimate needs.

Now, here's the problem. Legitimate needs are finally brand manager for fortune brands and somebody is selling fraudulent tireless golf clubs or Louis Vuitton handbags, I'm sorry folks. I know it's a serious – could do serious damage to your company but from a practical standpoint I don't consider that. And I'm speaking for myself personally to be as essential as somebody who's fishing for hundreds of thousands of names for bank of America or PayPal.

And I think that we have to realize that even though from their perspective, they considered to be incredibly important to get these issues done. You're dealing with different – you're different dealing with different impact.

And I think we have to recognize that is irritating is that maybe for the people who are responsible for brand enforcement and for protecting in for counterfeiting. And I recognize the public shirt when they purchase products that in fact are misrepresented and are not.

I just honestly believe that we need to be practical from that standpoint. If we can't get by this, then people on one side are going to assume that the essential need is going to be abused by either intellectual property or – and on the other side, the IP people are going to assume that people are going to be hiding behind who is for every welling nearly reasons.

So, I'm trying to take this up back up to a broader level. But if we aren't willing to acknowledge the impact on some of these things and if we

aren't wiling to accept the fact that we need to have access for – and it's – it'll probably get hang up as what's legitimate for one person is suspicious for another.

So, no matter on how they take this back up to another level and maybe on out of the line bringing it up at this point in time. Thanks for hearing me out.

Milton Mueller: Okay. I would summarize your statement is that different sectors have different impacts. So, you're arguing for some kind of recognition of sectoral differences across the access, right? Is that right?

Ken Stubbs: Right. But there has to be just because I am a brand – and responsible for intellectual property enforcement for City Corp or Chase, doesn't mean that I get the same access as to some pretty people who are dealing with their fishing issues.

Milton Mueller: Okay. Okay, we got that. All right, Bertrand.

Bertrand de La Chapelle: Thank you, Milton. Just to remarks (spiritly). The first one is that I'd pick in the previous discussion the expression access gateways, I think we need to put it in our mind somewhere because that might be something that we might like using in the future in the discussions as a concept. Nice word.

The second point I wanted to make relates archly to what was said. I think it's less that people have different impacts or different – only different needs is that different problems have different impacts.

And if I try to summarize what I've heard in the previous interventions, I would venture to suggest that actually, the legitimate needs of the private actors more or less seemed to resort to three different categories that are relatively simple.

One is prevention and monitoring of registration of domain names and, you know, in the preventive manner. Brand management is in one key illustration.

The second type of question is the urgent remediation particularly for fishing for taking down content or things that require the rapid actions.

And the third category is assignation – sorry for my broken English – assignation of liability for further legal processes like brand enforcement or fighting counterfeiting material and so on.

I'm wondering whether those three categories would help the different actors identify different modalities or different access modes as was mentioned earlier, in terms of urgency, in terms of nature of the data and maybe the type of intermediary or access gateway that they might choose. So prevention, monitoring, remediation and liability, assignation, I don't know if it helps but I just suggest it.

Milton Mueller: One quick question for you Bertrand, it seems to be frequent equation in these discussions about the linkage between urgent remediation and the access to the address, email and telephone number records at WHOIS. Did – are you asserting that there is such a connection because that connection is never been clear to me?

It seems that a website can be taken down without knowing anything about who the person is or where they are but simply knowing that it is a fishing side, for example. And then in fact, it seems that the most effective enforcement of anti-fishing has almost nothing to do with those missing data elements and everything to do with proper procedures to take things down.

So, are you disagreeing with that point or when you talk about urgent remediation?

Bertrand de La Chapelle: I see your point. I'm not – I must confess I'm not submitting here enough with the details of how this works. What I was just making is a connection also with the work in Subgroup A where this question of whether the OPAC for instance has some (unintelligible) need to be in charge or even responsible for taking down and whether he can act as a legal or proxy for the registrant was something that I kept in mind.

What I just wanted to make is a simple distinctions in the type of needs because it's probably easier to qualify those three needs than qualifying the category of actor.

Milton Mueller: Okay, I agree that those three needs are distinct. And I'm not sure what you mean by the third one. But if I do understand properly, then I think that we do need to keep those distinctions clear.

Bertrand de La Chapelle: Sorry, the third one is the distinction between - if another legal process is going to be made that will not – that will just go through the court, it shows the capacity to identify the person that will have the liability for this…

Milton Mueller: I see, okay. Right. And that would definitely be related to the WHOIS data, right?

Bertrand de La Chapelle: Yup.

Milton Mueller: Okay, great. Mr. (Dinatres).

Wout de Natris: Yes, thank you. Mr. Mueller. Most things I think it's just about being said because written down the board need also in my little scribble before I started. I think we need to identify what the third parties to call their need. And I think we've just heard a very, very good summary of that because what they need is to control the damages and the damages of the customers. And what kind of access do you need to achieve that? And I think it has to do with taking down something as fast as possible.

And I think if they can find who the hosting company of the damaging what site is, then that hosting company can be asked to shut the site off and then it can't do anything anymore. You can send their messages.

And of course it will be a new site and a new site but if you know where these sites are and maybe you need the data to the chain of sites because they were registered by the same company as the same person. Then that would prevent even more. So, I think that's one of the things that would need to be addressed for legitimate third access.

And on the other hand, what we also heard is about branding and ford and duplicates, Louis Vuitton handbags, these are all sense in spam messages usually. And I think what companies need to do is put more

pressure on local governments to start affecting their anti-spam laws because a lot of countries have this law but they don't credit any money and resources to the small dedicated team to start acting on this anti-spam law.

And bigger companies do have this source of lobbying possibilities. So, start there because a lot of countries have the laws in place but they just don't have the resources, they don't allocate the resources to do something about it. That's also an important message I think to a lot of companies. Thank you.

Milton Mueller: Thank you. All right! So, we've been having some discussions here of the framework. We have some discussion of the third parties categorization. Let me make a commitment that when we move forward, I will modify the classification of third parties in a way that takes into account the comments of Palmer and Steve and Ken Stubbs.

But let me take off my head as chair and express my own opinion here about what Ken said. I think I'm not convinced that you really – you've made the point that there is a difference in impact of various kinds. But I don't think that those differences in impact necessarily correspond to particular categories of sectors.

For example, it maybe that the brand manager, you know, could literally be put out of business by, you know, various kinds of counterfeiting activity. And obviously, from this point of view, it's very dangerous.

And I - while there maybe a greater social impact for the banking and financial sector stuff, to my mind, all that means is that the parties attacking the fraudsters would place a higher priority on it and develop more resources to tracking them down and fighting it, but not necessarily that the parties have different rights with respect to access to the data.

Obviously, that point is debatable but I think it's not clear again based on your statement that I would recognize the difference and rights to access to data as opposed to difference in the level of attention that law enforcement agencies and private actors would place on stopping certain kinds of things.

And I'm afraid, if we create a group – I'm not very familiar with Telecom regulation and what we're trying to categorize different kinds of services and then the technology changes and mid market changes and the categories turned out to be really stupid. They don't apply. They get in the way of doing things effectively. And I'm very concerned about that happening here.

All right, so…

Palmer Hamilton: Milton, can I comment?

Milton Mueller: Sure, go ahead.

Palmer Hamilton: The distinction that I see is that when you're dealing with financial institution, you're dealing with institutions who we're trying to protect third party rights in particular. And I did have what Ken just mentioned is a prime example. And so, it's a difference of kind as well as degree.

And secondly, as to your point about the ability to shut down and whether you need and address. Last week I've sent out an email and I can't find my email right now. There's been so many of them. But - in which I've sited the example for one of our banks that had fishing operation - forward operations going on the run.

And finally, we were able to close it down. We tried every means and including the ones you had suggested. The only one that finally worked was when we produced the street address for that local law enforcement agency in the run. And they were finally able to close it down.

Milton Mueller: And the local street address was in the WHOIS?

Palmer Hamilton: Right.

Milton Mueller: Uh hmm. Because if that message had said that you had provided them with the WHOIS records and that didn't prompt them to action…

Palmer Hamilton: It didn't in the prompt. The – we've provided everybody the WHOIS information didn't prompt. What finally prompted it was when we've provided the WHOIS information to local law enforcement and we got them back.

Milton Mueller: Okay.

Bertrand de La Chapelle: And the data was accurate? The address was accurate?

Palmer Hamilton: It was.

Milton Mueller: But again, in that site, the key – so that's the – actually an instance and possibly the only one we've heard of a connection between…

Palmer Hamilton: I can get you more but by the nature of this, it's going to be anecdotal. But I, you know, we can go to our banks and believe me we can get you rims of examples.

Milton Mueller: Yeah, yeah! So – but for example, under – let's say under the Kawaguchi proposal, maybe I classified it wrong here. But if you were and anyone and you produced the signed affidavit requesting the information on that particular domain, you would get the street address, right?

                    Palmer?

Palmer Hamilton: Yeah, I have not seen that proposal. So I can't speak to it. Sorry.

Milton Mueller: Okay. But just as a hypothetical. If you know there's somebody that's out there.

Palmer Hamilton: Yeah. As I've said earlier, I'm not suggesting that we wouldn't be in favor of other proposals. I'm just mentioning there is the distinction that can be made for the bank proposal because we're dealing with protections of third party. And back to Ken's point about a very fundamental interest third parties have. So, I think you can draw a public policy distinction.

Milton Mueller: Okay.

Margie Milam: This is Margie. May I ask?

Milton Mueller: Margie, you want to talk?

Margie Milam: Yeah. Unfortunately I'm (unintelligible)…

Wendy Seltzer: And Wendy, please.

Milton Mueller: And who else wants to be in?

(Yahuvi Atun):   (Yahuvi) please.

Milton Mueller: (Yahuvi)?

(Yahuvi Atun):   Yeah.

Milton Mueller: Okay. Margie, (Yahuvi) was there somebody else?

Wendy Seltzer: Yeah, Wendy.

Milton Mueller: Wendy.

Margie Milam: I'm actually at an airport. So I apologize for any background noise. I will have to sign off soon. But I think – just follow up on one of your questions of dealing about information in the WHOIS that's being currently used for anti-fishing. The email address particularly is one that's used fairly regularly in the anti-fishing arena and where it comes out is still be identification of a domain name that has a bank name and it say, you know, Bank of America Online.

And then what we'll typically do, if we look at the email addresses and try to correlate it with other email addresses for other known fishing site to determine whether, you know, this happens to be a fishing site or not. And use that to try to get the site down before it ever, you know, it ever goes live.

So, you know, the email address is useful and it's not something that, you know, would make sense to wait for and ask if, you know, seek an affidavit or submit an affidavit because fishing happens so fast. It's 24 by 7, seven days a week. And if you have to wait, you know, until a registrar of the business is open, you know, that fishing site will be a whole weekend long.

Ross Rader: That's just a small case to – Margie, I'm sorry to interrupt from on queue but, you know…

Milton Mueller: Ross, Ross, I'm going to have to ask you …

Ross Rader: Yeah.

Milton Mueller: …to come after Wendy. Okay? So we've got (Yahuvi)? Can you come in now?

(Yahuvi Atun): Yeah. Okay, I have a suggestion. Based on the last document you sent to the group compiled proposal. And they knew the command you send yesterday night, the PowerPoint document, I have it. I would suggest that we add on the third party sector specifics.

I'm not just referring to the banks. It can (beat and as well) company and put out people. So, my suggestion is that we have the law enforcement agencies sector specific and anyone. Thank you.

Milton Mueller: Okay, that's a nice concrete proposal. Wendy.

Wendy Seltzer: Yeah, I just wanted to suggest that – I thought your initial proposal was helpful and starting out by breaking it up into distinct categories between public sector law enforcements and private sector anyone else. And if the "anyone" else feels offended by or different and they don't want you to be lumped together, then I think it's entirely right for them to - within that subcategory proposed further specialization.

I will continue to propose the due process on specialization that every one of those sectors and every one of those individuals and everyone even in law enforcement should have to go through due process of law as relevant to the particular data they're seeking.

So we might determine that less process was required to gain access to less sensitive data. But I still think that the baseline should be due process meaning considered evaluation as that has been established through the about evolution of legal systems for a long time. It's not something that ICANN have to reinvent here and now.

Milton Mueller: So, Wendy, let me ask you a question. Would it be possible under your concept of the due process proposal for - let say, a bank to say, we have an ongoing problem with fishing, it's very serious from a public policy standpoint, we want to request ongoing very extensive access to WHOIS records?

Wendy Seltzer: It's possible to get forward-looking court orders, absolutely. I would again, want a public agency to be reviewing those requests and/or a court ideally or somebody in that sort of position to be determining independently whether the access that was being requested was necessary as long as we're going into the examples.

There are lots of times when we're told that immediate access is necessary when really it's a retrospective. They want a snapshot to be taken. But you don't need the WHOIS information in real time to shut down a fishing site. You need the WHOIS information if you needed at all perhaps to figure out who was behind that fishing site that you have shut down.

But it's quite easy to stop a domain name from resolving without knowing anything at all about who's behind this.

Milton Mueller: Okay, Ross?

Ross Rader: Yeah. I'm just – I'm listening to a lot of the examples that have been brought up and, you know, Margie kind of pushed the big button but it's – I figured a couple of times and that's fine – I want to caution against this optimizing around boundary cases.

You know, certainly fishing is bad. Fishing is irreparable. It hurt people, et cetera, et cetera, et cetera. But we can place in the status which will finally and hold up examples of fishing. For instance, that are completely not the mainstream case to, you know, and I just wrote an email on this so I won't go into detail.

But, you know, for us to kind of hold on to the fact that fishers are registering domain names for the purposes of fooling the public is generally not the main case that we're seeing.

So, let's just make sure that we're focusing on the majority of the issues through this discussion and not some sort of boundary cases that we will never agree on whether they're right or wrong.

Milton Mueller: All right.

(David): This is David. Can I get in queue?

Milton Mueller: You are the queue, David.

(David): Thanks. I just bring – I just want to reiterate a post that I've made yesterday. And I think it goes to Ross's point. But it slows that a lot of this discussion and that is, don't we need some empirical data about what the actual situation is? Not just from efficient perspective as Ross says but also from the actual privacy infringement that might take – that are alleged to have taken place as result of access to the WHOIS. I mean, we would ridicule a government if they made public policy or any type of policy without the date and necessary to make informed decision making.

And I know the GAC has requested that a study be undertaken. There was a response to my email that said that, you know, if the private sector did it, it would – numbers would be painted or they would hide the results if that weren't into industry is liking.

We – ICANN should do this. ICANN is responsible for the policy. And I just think it's something that we all need. And I'm not saying it needs to hold our ongoing discussions. But it's something that we should all want so we understand what we're grabbling with. And it will impact the types of access, I think, and the different solutions.

Ross Rader: Milton, if I can respond to that?

Milton Mueller: Go ahead.

Ross Rader: (David), I think you're mischaracterizing this thing asked for here. There is a number of – there are number of countries in the world that allow individuals not to publish this sort of information. What's being asked for is that we're allowed to abide by these laws essentially. As a Canadian company, I am not able to do that because of contract I've got with ICANN today.

So, for us to kind of go out and do this data gathering exercise on the premise of – so how am I going find out? There's always massive amount of infringement. And then we can create a policy framework that would then get us to the point where it allowed to offer at privacy completely goes against where the most of the world is already. These are laws that we're trying to deal with. So, I think that's just a big waste of time.

(David):   This is (David). I'd like to respond to that quickly. Privacy laws have exceptions in them all of the time. It's a standard. And there's also a policy adopted by the WHOIS. The last two is half forced to reconcile differences between ICANN WHOIS policy and national law. So there

is a way for that to be settled. But we're talking about something else. But I just want to respond to Ross's point.

Milton Mueller: Yeah. As you know, (Dave) and Ross, I'm kind of somewhat sympathetic to this whole line of discussion, not because, you know, as a social scientist, I'd certainly like to see empirical data. But I think that we're beyond that point in the processes.

The charge of this working group as I understand is just to come up with some kind of an access scheme which presumes that the data is shielded as proposed or recommended by the OPAC proposal. And our job is to fill out the OPAC proposal by saying given that many stakeholders strongly believe they need access to that data that would be shielded, how are we going to give it to them?

It is not helpful in that context to have a debate about whether the data should be shielded at all. I mean that was a debate we had for the last five years. And I just don't want this subgroup to become stock in that place.

All right! So, let's talk a bit about access gateway mechanism. We only have a few minutes. We're clearly not going to get the types of access.

If you take a particular proposal, you know, it's possible to have the different categories of third parties go through different access to gateways, which is what I understood the Kawaguchi proposal to be doing. And it's possible to have them all go through the same process.

And then, we have the issue of the encryption key problem. One of the – I think one of the big difference is let's say we're dealing with the EFA

proposal. We're dealing with self-certification. Basically, the default is you have access and you pretty much have to do something bad to have it withdrawn from you.

Whereas with the affidavit proposals or the more restrictive proposals that focused on law enforcement agencies used, the default is you don't have access to match. And then, the gateway defines a way of giving you access which could be of various types.

Do we have any ending? It seems to me that somewhere in this access gateway column, we should have this inscription key business in there but then I didn't really how to put it in.

Is anybody having any suggestion about that? Or do we think we've pretty much identified the options that we're dealing with properly.

(Ben Hong):   Milton this is (Ben Hong), just one quick remark on my – on the queue.

Milton Mueller: Go ahead.

(Ben Hong):   The question of having access is not only being given a key that give access to the whole data. The interest of the access gateway concept is that for instance, a service can be establish by either a category of actor or the certified actor that is accessible by other parties that it give access to.

But for instance, the service is done in a manner that allows somebody either to call or to access a secure website but through an access gateway. It doesn't mean that there is a key that is set related that give

access to the whole data. Maybe you can ask just one question each time.

Milton Mueller: Somebody ask to be recognized?

(Mike): Milton this is (Mike) from ASA.

Milton Mueller: Okay, yeah.

(Mike): I think that we can go through the proposals through these three steps process you have of the three categories that how are you handling it?

Milton Mueller: Yeah, uh hmm.

(Mike): Well, we do have a set – we do have an affidavit requirement. So I think your diagram needs to be updated to reflect that, I suppose a big call for that.

Milton Mueller: Okay.

(Mike): And – so, that – it's not simply a matter of someone saying, "Yeah, give it to me." and there's more way to it than that.

Milton Mueller: Okay, so what – why – how did I make that mistake? I got the impression that it was fundamentally – so do you think of any difference in access gateway between your proposal and Kawaguchi's?

(Mike): Well. The third party as I understand it in the Kawaguchi's proposal. The central authority would either grant a level of mutual one time or for keep on file and set on going.

Susan Kawaguchi: Right.

(Mike): So I mean, I guess phones are just different in the sense that we would - we perceive that for being something that's more of an ongoing of basis. But it does have a discipline in there which I'm sure we can address when get the type of access that access of break against abused.

Milton Mueller: And what is that discipline?

(Mike): Oh, that discipline is a pre-specific criteria we put forward. If those who materially misrepresent the nature of access or grossly abuse access privileges, would be subject to a complaint procedure. And could have their access privileges suspended to their subscription suspended.

Milton Mueller: So, how will that be monitored?

(Mike): Well, I – you know, what I'm not exactly sure the particulars how that will be monitored. It could either be the entity itself or could be perhaps outside actors. If they notice abuse could complain to the entity and move forward with the complaint procedure.

(Tom): Well, one question I would check. This is (Tom).

Milton Mueller: (Tom), go ahead.

(Tom):   Yeah, one question would have is how do you make sure that that person or that group of person does not wanted us kicked out because there was a complaint run against them don't come into (unintelligible) dictator.

(Mike):   Well, yeah, there would be still be it has to be something near as, something that have try and catch those who would abuse that. I – at least from our perspective, from our members, I don't see that being a (unintelligible).

                  But I suppose you could have people who might try to gain the system like that. And I think that level of particulars could be worked out. I mean obviously, I don't have the whole "she bang" here on the page. But…

Susan Kawaguchi: Yes.

(Mike):   …we're just trying to do it at a high level concept.

                  Certain thing I think though is that if there's a discipline in here with specific criteria is to catch bad actors. Maybe we're allowing for broad access but we're at proposal that also has a mechanism to catch those that might slip through.

Milton Mueller: Yeah, I think I ask this question on the list and I'm not sure whether you have the chance to answer it. But it some kind of disc junction in my mind between saying, I got a legitimate need to catch, you know, some brand counterfeiters let's say, but then as a respond to that need I got access to everybody, everything. What's the rationale there?

(Mike):   Well, I think it's truthful, you know, and I think the person from a
                practical basis - from an enforcement perspective if we have to go one
                off every time that we need to check a WHOIS. Administratively, that is
                – we're talking thousands and thousands and thousand of domain
                names and that just – it would be procedurally difficult to do that to say
                the least.

                And expensive and it would also add a lot of burden to whatever entity,
                be at ICANN or some third party that would have the ability of
                (feasting) through all these things.

                If we need to refine the purposes or categories of users who can
                access in a way that makes that a little bit more manageable from the
                perspective that some – in a group may happen, you know, maybe
                that's the discussion we can have.

                But I am concern about any proposal that would make it so limited that
                anyone who feels with this issues on a volume basis which would be
                inundated with paperwork.

((Crosstalk))

Susan Kawaguchi: Milton, this is Susan. Can I get in the queue?

Milton Mueller: Okay, but I'm going to have to leave in two or three minutes. So Susan
                you – there's nobody else waiting, go ahead.

Susan Kawaguchi: Okay. Well, my thought with affidavit was not really to slow down
                the process. It would initially maybe but at least we would have some

information on who is requesting the information and somebody just signed off.

Now, there's going to be bad players that will always, you know, take that information. But at least we would have some sort of idea if we needed to go back and identify this use of the WHOIS data.

And hopefully, you know, I do see it a need for a not just an affidavit for each WHOIS request. But maybe a bulk WHOIS request for – I mean for, eBay for example, you know, we – I look at the WHOIS all day long and we probably access it 2,000 to 3,000 times a week, you know, within the company maybe more.

So, I would not want a file 3,000 affidavit but maybe we could do one affidavit as that eBay is looking at this, you know, at every domain name that has - that contained eBay and (unintelligible). I mean that might be that broad. All of those details that have been worked out.

(Ralph): And this is (Ralph) from (unintelligible). Can I get into queue?

Milton Mueller: Well, go ahead.

(Ralph): Yeah, thanks. I've probably seeing it – it's probably will be somewhat so regulatory in (yen) because if somebody gets one of affidavit to seriously system and if it's proven that it abuses the system then it's kicked off.

So the discussion whether the brand manager or the bank is going to use all these WHOIS data, for instance, the security part of the bank which is going to shift through it. I think it would be so regulatory

because (pre) kick out of the system then there is no way you're going to protect your costumers anymore yourself.

So in that way, I think the one of affidavit should we save enough if there is somebody with the power to kick some – kick the bad guys off the system and keep them off.

What do you think of that?

Milton Mueller: I'm concern the – in my case about how do you know what these people are doing once you given them unlimited access? How would you possibly know what they've done?

(Ralph): Somebody would have – they would be have - there have to be somebody in the world that the gets complains about companies or LEAs for that part if their doing something which is not correct. If that's – if that institution in the world relevant would be get the power to say, "Okay, you're not going to get access to WHOIS anymore." Then the LEA or the company involve is in trouble.

Milton Mueller: Yeah, I understand that. But I think there's an issue here and sort of the distribution of cost and benefit. If you tell – if you say to me as the brand owner, "I've got unlimited access to every domain name in the world." And I can just do a simply string inquiry match search and send every body demand letters and (season) to just letters rather automatically then why the heck not do it.

I mean, it's cheap and it might produce benefits and whatever cost it are or whatever scared people there are or, you know, responses of

the recipient of these letters, those cost are all (going) by somebody else.

Now if you actually have to individually request a, you know, you have to – if there's some cost associated with making this request, then you're going to be a lot more careful about who you go after. So of course, from perspective of a brand owner, unlimited and unrestricted access is desirable. But it's not quoted as the proper public balance – balance of the public benefit.

Palmer Hamilton: Milton, can I get in the queue for just a moment.

Milton Mueller: Yes.

Palmer Hamilton: The point about the bank proposal is in relation to your last point what's to prevent abuse. In the bank proposal the regulators would monitor. The banks would have to certify. We're not using it as a marketing purpose. We're not using for this other purposes. We're going after efficient. We're going after ID theft.

And furthermore, the regulators would be charge with monitoring that going in and making sure that the banks are doing what we're proposing that they would do.

Milton Mueller: All right, good. It's almost – well, I'll tell you what I do is I will try to refine this model. I do think there's value in having the simplified template so that we can talk about generic approaches rather than 16 different approaches with each with 15 different categories as actor in them. So that we could possibly reach consensus or at least know where the parties fall on various kinds of approaches.

I'll try to prepare some kind of report in time for the next conference call. That it may make it possible to start discussing, you know, which – how much as part of these approaches has, part of that in the next step.

Woman: Sounds good.

Milton Mueller: All right. Thank you all.

Man: Thanks.

Palmer Hamilton: Good. Thanks.

Man: All right.

END