PRAGUE – Update on RAA Negotiations
Monday, June 25, 2012 – 11:00 to 12:30
ICANN - Prague, Czech Republic

Ladies and gentlemen, please welcome Senior Vice President ICANN Kurt Pritz.

KURT PRITZ: Thank you, Nancy.

[Applause]

Save your clap at the end. Thank you for taking some of your very important time to attend this session. Joining me on the stage from ICANN are Samantha Eisner and Margie Milam and from the registrar negotiating team Rob Hall of Momentous, Matt Serlin of MarkMonitor I know -- and is Volker coming? And if Volker comes he's from Key-Systems. So thanks very much. And the purpose of this session is to get your feedback on some very important issues in this registrar agreement negotiation. The results of the negotiation will change things for the better but may also change some fundamental ways about how we register and can utilize domain names. This has been very hard work, and while we've characterized it as a bilateral negotiation, we know that there are other very interested parties. And the foremost example, of course, we know are representatives of law enforcement who have made several very specific -- 12 very specific recommendations about improvements to the RAA. We also have the recommendations of a GNSO working group that's worked very hard on this. And so this is why it's hard. When we're sitting at the table we're looking at, for example, law enforcement organizations and those representatives have worked to really hone and make specific their

recommendations. When we're looking at them, we ask ourselves, you know, how -- in discussing the practicalities and the utility of these changes, to what extent are we empowered to depart from the law enforcement negotiations. If we work very hard and come back to you with a set of amendments that are different, would you see the wisdom in that? Here's Volker.

VOLKER GREIMANN: Sorry I'm late.

KURT PRITZ: It's okay. I'm still talking. Are we empowered to depart from those law enforcement recommendations? Or when we come back would that meet for disapproval. Or if we were to agree with law enforcement recommendations and come back to you with a set of agreements that changes how we register and use domain names or it changes in a large way the cost of a domain, how would the community react to that? And so we think on some of these issues it's very important to consult with the community at this point in the negotiations. And also why it's hard is that a negotiation is just that. There's give-and-take on each side. But these issues we're talking about right here are the core issues, the most important ones. WHOIS, verification of WHOIS data that this community has been debating a long time. Data retention and access to data so law enforcement can go after, you know, the bad guys. And so in this negotiation, this give-and-take, you know, everyone's kind of reticent to do much giving until they understand what the settlement on the big issues is. So there's been a long, long period, as you know, of negotiation and agreement on many issues and many improvements,

but we're also -- both sides I think are poised to like make final accommodations and move forward. But we think it's really important to get these real important things done first.

So without -- I probably talked through most of my slides. And what you're going to see here then, the best way we thought to do it is pass the microphone back and forth a little bit. There is some ICANN proposals, there's law enforcement proposals, GNSO proposals. We sit around this table and there's experts on each set of these. So to bring the most information to you, we want to give you -- give you the best input. Now that I've talked all this time I want to say that we want to reserve most of this time for you and getting your input on these very important issues. So this slide is about we've worked really hard, spent a lot of person hours, a lot of airfare, big phone bills. We've considered the proposals, all of them, from law enforcement. The GNSO and ALAC teams, registrars have certain improvements they'd like to see in the proposals, ICANN wants to see changes to the agreement to facilitate its compliance activities or how to terminate agreements. And so we've posted quite a bit of work. And because we're not done but we wanted to give you as much information as possible, what we did is ICANN posted an RAA draft. So this is not a negotiated agreement. This is ICANN's version of the agreement as we would like to see it. And the registrars who are going to do that. We thought it might be helpful because rather than say we're really close on some things, we'd like you to be able to stare at some real contract language too and then you can remark with specificity about what you think is a good change or where a change could be some improvement.

There's also summaries posted and a registrar statement. And the summaries identify that there's agreements in many areas and we want to talk about today the two areas where there's some disagreement. And so what we've honed in on really are what we think out of the 12 law enforcement recommendations and they overlap with GNSO and ALAC recommendations the four key areas, and the first two are the ones we want to talk about today and get input on, WHOIS validation and verification, improving the accuracy of WHOIS, and then the requirements for registrars to maintain certain data and for how long they have to retain it for to facilitate law enforcement and other recommendations. I'll tell you on the other two issue that is we've identified as key, we think we're kind of done. That is privacy and proxy provider obligations. We've agreed fundamentally to a proxy accreditation program and laid a good part of that out but also a registrar obligation to adopt the proxy accreditation program that's developed. And also with regard to abuse point of contact, the registrars have done a lot of work and detailed out the procedures by which each registrar would have to maintain a point of contact, how fast they would have to react, who they would have to react to and so on.

So in this session we're going to ask for input on those first two items and one other. So luckily for you I'm going to stop talking now and Margie, I think, is going to talk about key GNSO recommendations that are discussed in this negotiation.

MARGIE MILAM: Can you hear me? Is it on? Excellent. As Kurt indicated, the GNSO ALAC formed a drafting team that had made several recommendations and those have been evaluated in the negotiation process. As you look through the documents that we've posted, you'll see that a lot of the issues overlapped with the law enforcement recommendations. But there are some that were specific to the drafting team that have been evaluated and there's proposed language related to them. So for example, there's an enhanced collection of registrar and affiliate information. We heard the request that there needs to be more information gathered related to registrars and their affiliates and that's included in a proposed specification that deals with additional information on registrars and their affiliates and what types of privacy or proxy services they provide. There's also a request for a WHOIS SLA and that's one of the issues on the table in the negotiations. And a request that there be more specific language with respect to the prohibition against cybersquatting. And so if you take a look at the language in the ICANN draft you'll see that there's a proposal to deal with that issue specifically. And that's certainly something that's been -- in the negotiations. And there's also a notion that registrars need to be responsible for the acts of affiliates and their resellers and that's also something that's been discussed at length in the negotiations.

And so with that I'll turn it over to Matt that will talk about the registrar proposals.

MATT SERLIN: Yeah, thanks. Thanks, Margie. So next slide, please. So we just highlighted here four of the key registrar proposals that the registrars

have put forth in the negotiation. The first is to align the amendment and renewal process for the RAA with the new gTLD registry agreement that's part of the new gTLD program, to really bring our agreement in line with the process for amending and renewing the registry agreement. The second one is removal of port 43 WHOIS for thick gTLDs, and I just want to be clear here that what we're talking about is with a thick registry the registry operator actually holds and reports all of the WHOIS information. But as it stands today registrars still have the obligation to run the WHOIS server specifically for those TLDs as well. So it's really, in our opinion, duplicative and the registry operator should really be considered the authoritative source of that data.

Aligning the Consensus Policy section, this is defining what's within the picket fence. We feel very strongly as a contracted party that this needs to be very consistent with what's in place in the new gTLD registry agreement as it stands today and we've put forth our proposal and language in the information that we posted as Kurt alluded to. And then a sort of housekeeping item which really is this notion of automatic accreditation for all new gTLDs that come into the root and go live. For us that's really just increases our efficiencies operationally to be able to, you know, account for the hundreds of new gTLDs that registrars will be offering in the future.

So I think with that, I don't know if I'm turning it back to -- I'm turning it to Sam now.

SAM EISNER: So given that this is a negotiation, one of the things that ICANN did is ICANN came to the table with ideas of how ICANN wanted to improve

the contract for means of compliance, for means of achieving other improvements. And so one of the things that we have put on the table is requests for improved termination and compliance tools. So one of the things is a -- a request to have a termination provision based on repeated material breaches of the RAA. Currently that's a method of suspension. We've also heightened our ability to request suspension. And so these are ways that ICANN has considered that maybe we can make the contract a better tool for us to use through our compliance function.

We've also requested streamlined arbitration so that we don't experience the delays in selection of multiple arbitrators that we've experienced in some current arbitrations that ICANN is involved in. Also, we've put on the table some technical specs including requirements to support IPv6 DNSSEC as well as IDN protocols so that as the Internet community is moving to these new standards, that our registrars are able to support those standards.

In addition, there's a -- a provision in there that some have paid attention to, the sunset or revocation position. We find ourselves at the point of entering into the new gTLD program and we don't know exactly what the registrar/registry marketplace will look like after the new gTLD program is up and running with vertical integration of registry operators and registrars, and so in the event that the registry/registrar model needs to change, ICANN was considering some tools to help move the ICANN community to a model that better suits it. And so that's one of the purposes that we have that sunset revocation provision in there. Thanks.

KURT PRITZ: Thank you, Sam. So we would like to -- for you to contribute and get your input on three specific topics today. We know that there are other topics the community wants to discuss. And so -- and we encourage that. We encourage the reading of the poster materials and comments. There's a community wiki that is monitored and there's other -- there's other forums that can be made available for community input.

The three topics we want to discuss have to do with WHOIS data verification and how that should occur, data retention is the second, and the third is methods by which we can quickly make -- make enforceable the new agreement on all approximately 1,000 registrars. What incentives or methods can be used to ensure that all registrars adopt a new agreement immediately, anticipating a successful closure to the negotiations.

The first is the most complex and the most important and the one that could essentially affect the community the most, WHOIS data verification. There's several models for this that have been discussed. Law enforcement, during the last trimester, provided some very specific recommendations that ICANN's adopted as its primary negotiating position and we want to understand from you whether we should maintain that. What types of verification should occur and we're going to talk about e-mail and phone verification, and then what -- what should the timing of that verification -- what should be the timing of that verification and both of those things have implications for the current marketplace and user and registrant experiences. Should the verification take place prior to the name being resolved? That would

change how we register domain names. Today we register a domain name, it resolves right away. Should we have a waiting period while the verification takes place? These additional verification steps are manual. This will increase cost of a domain name. By how much, it's uncertain and it would vary from model to model.

And then finally, if we undertake these additional costs, and we might determine that they're really minor, waiting for a domain name to resolve and increasing costs in affecting the registrar marketplace, what benefits are we -- are we accruing, is WHOIS accuracy improved? Does that improvement improve the tools of law enforcement, actually reduce abuse? So those are very important and fundamental questions. And we want to flesh out the detail of this issue for a couple of slides and then invite you to come to the microphone and discuss this.

SAM EISNER: If you can move to the next slide, thanks. You're going to wrong way. One more. So we wanted to help frame out the issues relating to WHOIS data verification before we open the floor for questions. Many of these topics were laid out and these questions come out of the summary document that we posted in advance of this meeting. In relation to phone verification, this is where a registrar may have to have some obligation to contact a registrant by phone, either by SMS to a mobile phone or leave a voicemail or provide some sort of code that can be authenticated but it was transmitted by a -- via phone to have some assurance that the phone number that the registrant put into the WHOIS data is actually a phone number that the registrant can be reached at.

So the questions that we'd like you to consider and provide us some input on, what are the impacts to registrants by requiring this type of verification? Does this mean that all registrants are required to have phone numbers? Is this a barrier to certain parts of the world? Is there a language issue that registrars may face if they're using voicemail or code sent through e-mail that they have to be able to provide their registrants with instructions on how to return? Does this limit the ability for registrants to select their registrars based on that language issue? Does it create technical burdens for registrars? Will this encourage the use of proxy or privacy services so that the phone numbers that are associated with a registration are associated with a known proxy service instead of going back to your registrant? And what goals will be achieved through a phone or SMS verification?

If you can move to the next slide. On the timing of verification, you will hear it described as pre or post-resolution verification. So this would be mean currently in today's marketplace, to the extent that any information is validated or verified, it's done normally after the time that the domain name actually resolves in the DNS. So the person who registers the domain name already has the ability to use that domain name on the Internet prior to the verification or validation steps.

One of the things that we've seen in the law enforcement requests is to have certain items verified prior to the domain name resolving in the DNS. And so if it is done before domain name resolution instead of the post-resolution phase, should we be doing verification of both phone number and e-mail, one or the other? Is there an appropriate time for one to be done but the other to be done differently?

One of the things that it may result in is a change to registrant expectations. If you have the expectation as a registrant, the domain name will automatically resolve. But now you have to wait for a verification step. What will that do to the registrant experience? And is that something that we should be placing into the system today to achieve the goals of verification?

Next slide.

We also have an issue of annual reverification. One of the requests within law enforcement is -- or that we've seen from law enforcement is a request to have registrant information reverified on a regular basis. And so the questions we pose for you today are: Will this pose a burden on legitimate registrants? There is a possibility that if a -- if information is not timely reverified, that a domain name could expire or could be deleted based on the non-verification of it. So will it result in possible unintended consequences for people who have moved addresses, have some problem with an e-mail system? Will this pose new technical burdens for registrars? What additional goals will be achieved? And are the goals proportional to the burdens that may be imposed to registrants because of this?

Can you go to the next slide?

So we're about to take questions. But one of the things that I wanted to make sure we put back on the table -- I guess we deleted it from our slides -- is about e-mail verification.

If we are doing preresolution e-mail verification, what that means is when a registrant registers their domain name, they must provide a

working e-mail address with that registration. We've heard reports that many registrants have the expectation that the domain name -- or that the e-mail address that they'll have associated with their registration is actually the e-mail address associated with the domain they're seeking to register. So if I was going to register icann.org, I might want to put in my e-mail address as samanthaeisner@icann.org even though icann.org is not resolving yet in the DNS. So it is not an operable e-mail address at that point.

If we are looking for preresolution verification, registrants would then be expected to have an operating e-mail address at the time of registration which would not be the e-mail address associated with their new domains. That's another item that may have impact on registrant expectations and the current behavior in today's marketplace that we would like to have you discuss.

So at this point, we would like to hear your input.

KURT PRITZ: Just to put a point on it, these are essentially the questions we'd like your opinion on. What verification should occur? The law enforcement recommendation includes e-mail and phone. The timing of the verification, should it occur before the domain name starts to resolve? Should it be done annually? You might ask the registrars here their opinion on how the marketplace would change or how users or registrants might be affected.

We might -- we might ask questions of proponents of these models about what goals would be achieved. So I think -- you know, I'm gratified that people are coming to the microphone.

Sir?

JAMES BLADEL: Hi, James Bladel, GoDaddy, registrar, not a member of the negotiating team. A question more procedural, before we dive into this, because this is a fun topic, why did we decide -- are staff issues, staff requests in the new RAA draft not up for discussion today? And why did we decide that?

KURT PRITZ: Because we have an hour and half. We think that these areas are potentially of policy concern, but we want to listen to anybody's opinion on any of the very many negotiations.

JAMES BLADEL: I'll step aside for the queue. I just wanted to submit that those also affect the community, and I think it's probably not a good idea to leave them off the table. Thanks.

KURT PRITZ: Thanks, James.

STEVE METALITZ: Steve Metalitz. I'm the president of the intellectual property constituency, and I was chair of the GNSO-ALAC RAA drafting team that was referred to. Sometimes it is referred to as "GNSO," and I want to act knowledge our colleagues in ALAC who made a big contribution to that drafting team, and they shouldn't be left out in this.

I actually agree with the previous comment perhaps this has been defined a little bit too narrowly.

I want to start by saying I want to thank ICANN and the staff for putting forward a complete text that they had proposed. I think that's very helpful to have actual contract language -- proposed contract language to look at and, we're eager to see -- and maybe it's in the material that's been posted by the registrars, which I haven't had a chance to review. We're eager to see their contract language or their proposals for contract language so we can really respond to concrete proposals.

On this issue of verification of WHOIS data, we appreciate the progress that's been made on this. We think it is a very positive first step, and we would encourage the registrars to try to come on board with the proposal that ICANN has made. Our concern is really that we don't think -- you know, this is a big change in how business is done. And when you're trying to leap the Grand Canyon, it's sometimes not the best strategy to plan to do it in two steps.

Our concern that with the availability of temporary, free and disposable e-mail and phone numbers which are ubiquitous, it may not achieve as much as we hope in terms of verification. There are a lot of commercial address verification systems that cover many jurisdictions. And while

it's not a total answer, we were disappointed to see that there is no requirement that -- apparently that registrars make use of those.

We think they have a commercial incentive to make use of them anyway because presumably they are getting paid for these registrations, so I hope that that would be also be included. But what I really see as the biggest gap in this proposal -- and it was referenced in one of the slides -- is that the proxy system is a work-around for this. There is no requirement, as I understand it, for a proxy service provider to do any of this verification.

So they can take whatever bogus information they want and hold that as the contact information. And even if you succeed in getting the reveal of that information, it may not be useful.

So I understand that that's an issue that Kurt thinks is done as far as the proxy and privacy service accreditation. We disagree in the IPC, and we will be talking about that with you tomorrow, I hope, and with Sam.

This is a big gap here. And whatever verification requirements are imposed, they should apply not only to registrars but also to, first, registrar control proxy services and all proxy services that would be accredited. Otherwise, it is just too big of a loophole to drive through. Thank you.

SAMANTHA EISNER: Thanks, Steve, for your comment. Particularly in relation to the proxy services, we have all recognized that that is a potential fail point in this. And so you saw reference to the proxy accreditation service that Kurt talked about in one of the first slides. We think one of the key parts of

that would be the imposition of this type of requirement, that that would have to be part of any accreditation system to make it equal across.

STEVE METALITZ: My recommendation would be to put it in the contract now. And when the accreditation catches up with it, fine. Otherwise, we may be in a situation until the accreditation process occurs -- and we have a lot of questions about that, we'll have this giant loophole in existence.

ROBERT HALL: Steve, if I could follow up, by and large, I think registrars agree to it, what I will call the cross-field validation which goes to are we verifying e-mail addresses? Although we are not verifying the contactability of you at that mailing address -- not e-mail, I'm sorry, mailing address -- I think we have agreed to say, Look, if you are in the Canada, the postal code matches the format. So there are worldwide conventions for postal code and phone numbers and that type of thing, so we're not getting -- I live in Denver, California, Canada. And my postal code is one and my phone number is two . So I think we've kind of taken that off the table so that's not being discussed today.

But in terms of the cross-field and the interfield validation, I think, by and large, registrars agree there are international published standards for each country of this that we've said, Yes, we will follow that.

STEVE METALITZ: That's helpful but very basic. And as you know the commercial registration -- the commercial address validation, address verification services go well beyond that.

KURT PRITZ: Steve, is your recommendation to include the proxy accreditation detailed program as part of this?

STEVE METALITZ: Yes, if you're going with the accreditation approach, the requirement as of the time the new RAA goes into effect should be not to accept proxy registrations from services that don't do the data verification that's required, whatever that turns out to be.

MATT SERLIN: When Kurt said we have agreed to a program, that's we have agreed to that, is that any proxy registration that a registrar accepts must come through an accredited proxy provider. We haven't at all discussed -- And we won't because it is outside of our scope, at least on the RAA discussions. We haven't discussed what the parameters of the proxy program, accreditation program would be.

STEVE METALITZ: That's my concern. That discussion could go on for years. Let's get this in the contract now, this aspect of it at least.

KURT PRITZ: Thanks, Steve.

Hi, Avri.

AVRI DORIA: Hi, my name is Avri Doria. For the first time at an ICANN meeting, I'm actually speaking for a company and a community. In this case, I'm speaking for the gay community that would be represented by Dot Gay, LLC.

I want to go back a little on my concerns here. First of all, in terms of the input that has gone into this, in terms of the input that ICANN has gotten, it's been very one-sided in terms of the law enforcement agencies.

In none of the lead up to this discussion have we heard from your conversations with the data protection authorities, with the privacy authorities of many countries. And I think in many cases, you'll find that some of these requirements would run against national law, regional law, various other treaty law. I also -- in addition to that other half of the story, I want to also look at the fact that when we say "law enforcement agencies," we tend to think that we're always thinking about good guys. In terms of the ones you have been talking to from the U.K., from the U.S., from Canada, that's more or less the truth.

When you're talking about law enforcement agencies in Uganda, however, especially when looking at the gay community, you are not necessarily talking about good guys. You are talking about people who don't adhere to the universal Declaration of Human Rights. You are talking to people that if they do give this information, if they do have this verification of where they are, who they are, how they can be

reached, you are actually putting people in threat of imprisonment and sometimes even death.

So to look at it with the benign eye of a particular Western law enforcement that, first of all, doesn't even take its data protection into account and then doesn't look at the legal structures that people live under in various communities and it isn't just the gay community, it is all the freedom of expression communities around the world, you're setting up something where you are excluding a large part of the population.

You ask how will it effect the marketplace, the user and the registrant? It will exclude these people. And those that are brave enough to participate, it will endanger them. So, please, take those into account.

[Applause]

KURT PRITZ: Thank you, Avri. The next topic we're going to talk about is that of protection, where the effect of privacy laws has a very real effect and it's sort of a confusing area because we're not sure how privacy laws affect these things or not.

BILL SMITH: Bill Smith with PayPal. I'm also a retired member of the WHOIS review team. So looking at what verification should occur, suggestion that we look back to the slide that was offered by SOCA at the last meeting. There are various mechanisms that can be employed, using a risk-based analysis for registering a name. What is the timing? It should happen when the name is registered. Whether the name is immediately

registered or not should, in fact, be a determination based on whether a contact can be made.

With the suggestion on e-mail verification, I think it is perfectly reasonable to expect a registrant to supply a valid e-mail address at the time of registration. Personally, I think it's highly unlikely that someone will be registering for a domain name without some form of e-mail or some mode of communication via the Internet. We should expect to be able to contact that individual, and that information can easily be updated after the fact or at least I hope it can, otherwise we cannot have accurate information in the WHOIS system. And that is one of the goals of the Affirmation of Commitments.

On a larger level, though, I have to ask why is this contract and the contract of other parties being negotiated bilaterally? If an agreement is amended and to be entered into by the registrars in this case, or registries, but in the registrar case pursuant to Section 2.3 and 2.4, 2.3 deals mostly with competition, 2.4 is community policy, to my knowledge, private bilateral non-community-based negotiations are not part of any policy at ICANN.

So I believe this entire negotiation is operating outside of the policy. Any contract that would come out of it could not, therefore, be recognized, if executed.

In addition, registrants are required to submit to requirements that's established by ICANN in its sole discretion or between ICANN and the registrars because they are engaged in bilateral negotiations. And that is in section -- current 2009 Section 3.7.7.

We have no right to negotiation. We are not a contracted party. But we are subject to the terms that are unilaterally applied to us. That is not fair.

So this entire system, in my opinion -- I'm not speaking as PayPal currently. That is unfair and needs -- Would you like me to speak as PayPal? If you would, I would like to speak as PayPal. PayPal sees this as unfair. Okay? This is not fair. It's not equitable. The registrants are paying the fees that get submitted through registrars and ICANN receives them.

This is an industry that is funded by registrants, and we have no voice in the terms that we are subject to. I believe this is a flawed process.

And at this stage of the evolution of the DNS in this organization, we can do better. And I suggest that the board, staff, registrars, registries and registrants seek to come up with a better mechanism. This process has been going on, as best I can tell, about nine months now. And as far as I can tell, we've made virtually no progress on issues that are of import to the community. Thank you.

KURT PRITZ: Don't go away, Bill.

[Applause]

So what is that alternative mechanism? And the reason for these negotiations and the reason why -- my understanding, and the reason why the ICANN board requested these negotiations is they were identified as a way to make real progress since there were 12 specific

law enforcement recommendations as a way to make real progress on those because two parties -- and, you know, it's ICANN and a thousand registrars, or their representatives -- two parties can make real progress sitting at a table.

That doesn't mean whatever is decided at that table is adopted. The results of those talks have to have the review and imprimatur of some sort of bottom-up discussion, which is what this is.

The ICANN board listens very carefully to the community, and it will take the output of these negotiations, listen to the people in the room, and listen to the people in the community and go back and say, You guys have not succeeded in making substantial improvements or meeting the expectations of law enforcement in the community.

So it's seen as a way -- as a mechanism for moving this forward in an expeditious fashion but also one that has real bottom-up input into it. And the other processes that we've used haven't moved the process forward, so this is one attempt by the board to move the process forward.

The board has also asked the community through the GNSO to undertake a PDP on any aspects of this that be don't address the need or to take up a PDP now.

So the board is asking for a dual prosecution of this effort, to run through this negotiation and through a formal PDP. Those are the mechanisms that are available.

At the end of the day, whatever we do has to be reviewed by everybody. And the board is not going to approve recommendations

that they don't think have real effect or support of those that are affected, which are the registrants and users you're talking about.

ROBERT HALL: Can I just ask for clarity, Bill? To get back to the topic, I think you said yes, e-mail verification should happen. I wasn't clear on whether you think phone or not. And on timing, you said sometimes yes, sometimes no before it goes in the zone. Could you maybe clarify? Are you saying yes, we should verify before it goes in the zone or not?

BILL SMITH: I believe we should attempt to do verification, okay? In real-time. And if we look at the SOCA proposal, the slide that was presented was, in my opinion, the first clear presentation on how we could do a variety of ways -- or have a variety of ways of doing verification. And if we cannot verify, my suggestion is to not put it in the zone.

ROBERT HALL: Perfect. Thank you.

BILL SMITH: We delay.

If I could respond to Kurt, PayPal actually submitted a set of proposals for how this negotiation should proceed.

And as an example, one of the things we believe is that the DNS system -- that's the entire community here -- is supported by some service

providers, registrars and registries, and a contract should be executed with those parties.

In such an environment, the party requesting the services pretty much dictates the terms, and that's not what we see here. Okay?

We see the two parties, the service provider and the party requesting the services, or its adjunct -- okay? -- doing the negotiations.

And the terms aren't being clearly specified and saying, "This is what we expect. These are the levels of service that we must have in these areas, and you must deliver if you wish to be a party to this contract and provide services for this community."

So that's what we would like to see is something that is much more clearly within the control of ICANN, the corporation, with input from the -- with ICANN, the organization.

Take the input from us, have a negotiating -- or not a negotiating team, a contracting team, a drafting team, that produces a contract with policies that are separate from the contract, clear separation, so that the contracts can remain relatively stable but the policies are the things that will change over time.

And as it currently stands, there's policy in the contract, policies outside that are in conflict. It's difficult -- as you point out, it is difficult to get all the registrars onto the same set of policies at the same time. What are mechanisms to do that? We laid that out in our proposal.

KURT PRITZ: Thank you, Bill. Hi, Wendy.

WENDY SELTZER: Thanks. Wendy Seltzer here from the noncommercial stakeholders group.

I first want to frame my comments by saying that, you know, domain names provide a user-controlled location and stable location pointer for online speech.

So we're talking about speech at the user's control.

And I think as an industry and as a community, we should be thrilled that one of the first things that people do when they think about launching a political campaign or a protest or a new enterprise, they go and register a domain name, so that they can independently control this pointer to their activity. So as participants in a protest in real-time tweeting, they want a way to refer back to that, they register a domain name. And so I think as we look down these questions, we have to ask: How does -- how would these changes impact the registrant trying to make that immediate use of a domain name to locate and center a campaign. Verification that requires them to have access to a phone that may not be with them, to have an e-mail address that's controlled by a third party because they haven't yet registered their own domain name then subjects them to interception of communications that I -- if somebody is in the middle of a political protest trying to house their dissident speech and they give a Gmail address but Gmail -- access to Gmail is compromised in their country -- and we know that, in fact, serious attacks have been launched with fraudulent certificates and middleman attacks -- forcing people to go through verification to receive the confirmation that would allow them to launch their speech

online is a serious barrier to that important political, civic, social, or business activity.

So I would argue that the system that we have now of no verification required is a proper system.

If -- because all of these -- so many of these questions presume that we're moving toward a verification system, I want to add some comments on those.

I think if verification were to be required, it should absolutely be only after the domain name is permitted to resolve and not before. It shouldn't be that one is required to wait before obtaining this location pointer. We shouldn't require somebody to get back to an e-mail address when they're standing in the square protesting. We shouldn't hold up the -- the launch of their campaign while they wait for a domain name to resolve.

And we should consider the costs that this imposes.

Of course it's not a cost that's significant to a multimillion dollar business if they have to pay $5 extra for a domain name, but for the individual who is just moving from the free services that have offered blogging and tweeting and other kinds of communications to something that's a little bit more stable and a little bit more permanent, adding even $5 to the cost of a domain name registration is a serious barrier. It causes them to think twice. And we don't know, I think, what the costs -- what the economic costs would be, how much of those would be passed on to registrants, but I think for the individual end user and for

the small nonprofit organization, we need to be concerned about even small increases in those costs.

And then the noneconomic costs of being forced to provide additional information, potentially being forced to wait for resolution, are serious.

So I think we will be gathering and submitting further commentary around the serious privacy issues that these raise and the serious concerns these raise for anonymous speech and I think it's important to -- along with law enforcement, that you are -- along with the types of law enforcement that you're currently hearing from, it's important that you also hear from those in charge of enforcing privacy and data protection law, which is another component of many national laws which would come into direct conflict with some of the requirements that I've seen proposed.

I'll move to the back of the line to add further comments.

KURT PRITZ: Well, actually, Wendy, I think we're going to cut this topic off at Mike. You're in the back, right? And then -- but we're going to have another topic after that about data retention and you can bring up sort of related --

WENDY SELTZER: Well, then 30 more seconds.

KURT PRITZ: I'll give you 20.

[Laughter]

WENDY SELTZER: s I've said at other times, I think that anonymous speech is protected under the First Amendment in the United States and an important component of the speech right as a human right, and so any verification requirement that would force people to be tied to an offline identity, as telephone often would be, as any heightened authentication of identity would be, would be a serious violation of those speech and human rights as well.

KURT PRITZ: I guess you couldn't rejoin the line as Anne Nonymous, another person.

>> She's one of the masks, maybe.

KURT PRITZ: Yeah. Benedict?

BENEDICT ADDIS: My name is Benedict Addis and I'm on the law enforcement team that's lead by Bobby Flaim of the FBI.

I think the first thing I'd like to say is that -- and I don't think it's been said properly in public yet, is how much things have moved on since I think Bobby started this process and since I've been involved.

I think it's an absolute credit to everybody involved that whereas before, I think we simply weren't in the same place, law enforcement and registrars weren't even speaking the same language, and I think it's a credit to ICANN staff Margie and (indiscernible) on the registrar side everybody is, I think, evidencing an immense amount of good faith.

So at least whilst we're still arguing over a couple of points, we both understand where we are on both sides. So I think that's -- I think that hasn't been mentioned enough and I think we need to credit everyone.

One of the points I'd like to highlight -- and it's in response to Wendy's concerns about privacy and anonymity online -- is that one of the major changes in the law enforcement position has been, albeit grudging, acceptance of privacy and proxy services, and I feel that that's a major shift that -- in supporting this, and understanding that in fact that might be a way -- as Rob, I think, made the point at the last meeting in Costa Rica, if you allow people to protect themselves and not have their personal information splashed online, then they will naturally give you better information. And I think that's a really important point to make.

One thing I also wanted to clarify is really -- I wanted to make -- explain why law enforcement cares about WHOIS, and again, I don't think that's been clarified enough.

So we know already, and anecdotally from registrars -- and it's kind of business practice. We know that you validate and you verify your customers because you want to get paid. So you check that the payment card matches the country. You check that the address matches out. And there's plenty and plenty of commercial services that

do that for you on the customer data side, on the billing side, on the transactional side.

Now, I think the law enforcement point is that we'd like some of the same courtesy extended to the data that you put into the public domain, the WHOIS data, and I guess there are -- there are three reasons for that that I can think of, but I'm sure my colleagues can think of plenty more.

The first of those is really the simplest one, that we'd like to be able to contact the registrant. And that sounds incredibly dumb, but actually, some of the people that are either doing bad things on the Internet or that have had bad things happen to them on the Internet need to be contacted, so it's the very basic one.

And a slightly more -- and a slightly more complex version of that, about we'd like to be able to contact the registrant, is even where false or partially false details have been given, that often gives us what we call a "lead," so -- and they might have registered with a throw-away e-mail address. But hey, do you know what? Google log IP addresses, that might give us something. Not everybody is careful and people slip up. So that's a lead.

And again, leads, if even they've been careful, allow us to correlate bad stuff together, so we can group, we can look at maybe we can identify a gang who is registering bots for botnet, so command and control for botnet.

So that's the simple point about there is a value in WHOIS, and I think I need to praise the findings of the WHOIS review team who have made

some very clear statements and I think that hasn't been mentioned enough about how they'd like to see the WHOIS improved.

The second point is because everybody else does it.

We know when we register for a Gmail account, that we're expected to put a -- you know, to do an SMS validation, so we're expected to provide a telephone number and have an SMS come back, and I think one of the points that Bill from Paypal was kind enough to raise was the matrix that I presented in Costa Rica which allows some flexibility around how this is done.

So a scoring system gives flexibility for the cases where people do not have a mobile telephone number or do not have an existing e-mail address.

So there are -- we can be sophisticated about this. We can -- we can have a risk model, as Bill so clearly highlighted.

And the third point about why we need to improve this, this figure of 28% bad -- completely bad WHOIS, is a more subtle point and it's an economic point.

If we elevate the whole community, if we ask everybody to pick up their practices, then we let the bad guys stand out. So it marginalizes the bad guys and they show up more easily. If we (audio problem) to a corner, we can all, together, solve this problem. And I'm not talking about solving crime but marginalizing it.

One last point. Validation/verification leads to some metrics. We get some really rich metrics out of it. And this is a big "ask," but if we can

publish those metrics so we get a number -- how many points did you score on the model -- then we get really good things emerge out of that for free.

A better compliance process, one. So you can start to address the problem of bad registrars, the guys that cause all of you problems, and we know who we're talking about. They're not in this room. Okay?

We get -- we can inform the security folks so people like Rod can make better decisions about domains.

And the most important thing is that actually at the moment -- I've heard from the security folks is that at the moment, new domains are now considered so bad, so toxic, that a lot of folks won't route e-mails from them, for example.

So one of the main reasons for a domain to appear on a black list is because it's new.

Well, that sucks for everyone. The system is already broken because folks have taken decisions already to block domains that just happen to be new.

So by publishing scores and by allowing people to make a more granular decision, a more informed decision about whether a domain is good or not for a new customer, we can improve the way this works and not harm it.

Thank you so much.

KURT PRITZ: Yeah. Thanks, Benedict.

Kathy?

Oh, Volker wants to make a comment and then I'm going to rise to a point of order.

VOLKER GREIMANN: Is this on? Yeah.

Benedict, thank you for making the comments and bringing the scoring back as well, because we were under the impression that had been taken off the table with the latest set of recommendations, so it's good to see that it's still an option that law enforcement is also considering as valid.

KURT PRITZ: Thanks, Volker.

So Kathy, I'm going to rise to a point of order so you'll have to bear with me -- and it's because other people got in line behind Mike and disrespected my authority here.

BENEDICT ADDIS: I need to just clarify that there is a certain minimum requirement on scoring, as I think we've discussed, so that's -- we still very much need -- and it's pretty basic stuff.

I would need to remind everyone that all we're talking about is that there should be something in the fields. Like it's really simple stuff. It

shouldn't be blank; it should be "1." And I'll -- I will say that we've just been able to register a domain in the name of MI6, Number 1, Iran in Iraq, I think was the line, so this still isn't being done particularly well.

And that those e-mails -- e-mail and address match in those international formats. That's a check that can be done with no cost with a bit of code. Okay?

KURT PRITZ: Thanks. So what I would recommend, because we're still on the first topic, is that everybody stay in line. We have one slide on data -- data retention issues which are somewhat related to some of the issues that have already been brought up in this line, and then everyone can comment on both WHOIS verification and data retention and at least we'll get to those issues.

But even with that, we have a little less than half an hour to go, so if you could keep your comments to a couple minutes, it would be great.

KATHRYN KLEIMAN: What if I forget all my points, Kurt?

KURT PRITZ: Nah. You've got a short-term memory. I don't. So Margie, could you -- we're just going to spend a couple minutes and talk to the other set of questions we want to ask about, and that's about the data retention requests.

MARGIE MILAM: Sure. And can you hear me okay?

The other issues that -- we were talking just now about the WHOIS validation, but the other aspect of the law enforcement recommendations that we wanted to get your input on is the issue of data retention, because the law enforcement recommendations made a recommendation that there be collection of information related to registrants and that be retained for a period of two years after the life of the registration.

And so that is something that we've been grappling with with the negotiating teams and would like to get input from you all as to whether you think that duration is proportionate with the law enforcement objectives that have been at the forefront of these recommendations.

And also, too, a question of whether that would put a burden on registrants' privacy rights or a burden on registrars. We think that that's something that needs to be explored and we'd like to get input from you all about that.

Another aspect of it which you maybe haven't thought so much about is the compliance issue. As we think about different international regimes where some of the laws may not allow for the retention of that information for that period, the question is, is it fair for registrars to have different obligations if, in certain jurisdictions, they can't keep the information for two years. Maybe they can keep it for a shorter amount of time. And so that's one of the issues that we've been trying to explore in our negotiations, to see whether there's a way to deal with that and whether this concept of having a uniform contract across

registrars is an important concept to, you know, think about when we're dealing with compliance issues.

And the other area we'd like to hear from you all is whether there's been any GAC input on the latest law enforcement clarifications. It would be important for us to know whether the GAC was supportive of the -- of the clarifications that have been made and been received in the last trimester.

And then the question I think Wendy raised was one that we would like to explore. How do you think we could get input from data privacy authorities? That is something that, you know, we've heard loud and clear from you all and we'd like to see whether any of you have recommendations on how we could bring them into this discussion, so that we can make sure that the requirements that get written into the contract, you know, are consistent with some of these data protection laws.

So with that, I think we'll go back to the queue, and you can address either the WHOIS issues or the data retention issues.

KATHRYN KLEIMAN: And could we go back to the previous slide, please.

KURT PRITZ: Sure, Kathy.

KATHY KLEIMAN: Thanks. Kathy Kleiman, also a retired WHOIS review team member and a co-founder of the non-commercial users' constituency. And first I want to say, thank you. Immense amounts of time, energy expertise have been devoted to this from all sides. And so thank you, thank you very much and thank you for listening to our input and soliciting it. I will try to cover my points quickly, without talking too quickly, as I'm well-known for doing.

Regarding WHOIS data verification. What verification should occur? Let me address that. I would say e-mail or telephone. And the reason why is in some of the outreach on this issue we found that in different countries, actually different continents, there's different sensitivity on this. Because remember, whatever is verified is going directly into the WHOIS. It will be publicly accessible all the time. So in the United States our private telephone numbers, even our cell phone numbers are considered personal data and people are very protective of them, especially with cell phones. We don't have directories of these things.

But in Europe it's the e-mail address. People I've talked to don't seem to have the same sensitivity about their cell phone numbers but they are very sensitive about their e-mail whereas in the US we probably publish that much more quickly. So I would say one or the other. If you verify one or the other, you've reached the standard set by the WHOIS review team which is contactability. It was the unreachable domain names that we had recommended that ICANN work very aggressively to get rid of. So if you register one or the other you've got reachability, you've got contactability in case of problems.

On the timing of the verification, I would say post resolution. And here I would echo what you've heard from Avri and Wendy so I won't repeat it, but we have speech issues here, we have human rights issues, we have timeliness issues, we've got some kind of dangerous product or service or very timely issue. So do it afterwards. Don't hold it up, especially if there's some kind of problem. And it could be technical. I send e-mails all the time around the world and often they bounce back. There's a server problem. I don't think you want to hold the domain name and I think that would totally change the user experience in the domain name system. Get those up and pull them down if necessary but get that speech up and those -- that freedom of expression up as quickly as possible.

On the issue of input, which is -- which I'm glad you covered the next slide, I would urge outreach, I have ideas on how to reach data protection commissioners but know that they've already participated in the -- in the process. We've had four or five data protection commissioners and associations over the years write to us, but normally when they were pinged and told what was going on, they don't participate as actively. But they really should. And I just wanted to say for balance purposes in every community I know law enforcement requests are always balanced with what the court is saying, what the community is saying, what other data protection commissioners and consumer groups, it's a big conversation. And here we need to have that conversation. So outreach and quickly, and we'll work with you on that.

The last thing is, as I hear about accreditation of proxy privacy providers, let me add I'm not sure that should be a bilateral negotiation.

I would like -- this is going to be the first time that we're setting a common set of standards for reveal and relay of proxy and privacy service providers, and I would love to see that as a consensus process because I think you'll get great input. And notice and comment isn't enough. I think you should bring everybody in to the discussion of that one. It's new, it's groundbreaking and users really want to be involved. Thank you.

KURT PRITZ: Thank you, Kathy.

ROB HALL: Kathy, if I could just follow up on your announcement. I think all that is being proposed in the RAA contract is that if ICANN ever does accredit privacy and proxy providers that we as accredited registrars will only use them then as opposed to anyone else. So I don't think at this point in the RAA negotiations we're negotiating the details of what that accreditation will be. I assume that will come back to a more public process.

KURT PRITZ: But we did hear from Steve that he would like to see that included in this round of negotiations. And if we were, you know, we would want to talk about how to do that in the bottom-up fashion you spoke about but in some sort of quick way.

So I really appreciate the speed with which Kathy spoke, and I admire the scribe who kept up with her. So try to speak more slowly for the scribe but keeping to a narrow time frame, if you could.

JOY LIDDICOAT: Thank you. Joy Liddicoat from a non-commercial stakeholder group. And I will speak slowly for the scribe because the New Zealand accent is always a little tricky to catch. Firstly I just wanted to reiterate in terms of the ICANN board and the ICANN staff, you know, on this issue, please be a human rights defender. The Human Rights Council and United Nations has recently said that where any Internet public policy is being undertaken human rights analysis must take place. And just because this is a private contractual arrangement between registrants and ICANN doesn't change the fact that this is in relation to global public resources and that registrants have rights and these must be respected and upheld, and this is partly why the noncommercial stakeholder group is encouraging ICANN to join the global network initiative. So that's the first thing.

The second thing is registrars please hold the line on those rights. Please don't cave in just because the negotiations have been going on for some time. It's really critical, for example, that (indiscernible) verification is not required. And that's for some really practical reasons. Subject to court orders, for example, many people are not -- are subject to witness protection programs, they're subject to non-harassment orders against other people and requiring them to disclose their telephone numbers publicly and have those verified can actually put

them at risk. And also result in registrars violating court orders. So please, I think minimum verification.

And in terms of law enforcement officers, you know, from a registrant's perspective it would seem entirely unfair if registrants accredited at country level, registering domain names as registrars at country level face different standards than they do from registrars at global -- the gTLD level. And we would say, you know, bring -- if you're asking how to get data protection officers here, bring them here. And it's unbelievable this is the 18th -- you know, you've had 18 meetings and ICANN is still wondering how to get data protection officers involved.

[Applause]

I mean, the -- it would be great, for example, to invite the privacy commissioners from the United Kingdom, from Canada, the European Union to participate on the panel and to give their views. And I would encourage and really insist that ICANN do that.

In relation to annual verification is also a major concern. You know, and this is a burden for registrars as well. It's not only from the registrant's perspective. And, you know, requiring positive verification annually seems disproportionate to the objective that law enforcement is trying to -- trying to achieve.

In terms of privacy and proxy, I would just echo the comments on that. I know it's a separate discussion. But it's vital that there be community input on that.

And finally, just in relation to, you know, developing country perspectives. Bear in mind that many people in various parts of the

world, for them using phones and so on is not an accessible way or a safe way to verify data. So I just really want to emphasize those points. Thank you.

[Applause]

PAVEL: Hi. I'm Pavel (saying name) from Global Sign. And I would like to ask the question why we should list data that is false anyway. If we -- the question is, do we need to verify data? Yes. If we want to list data, we should verify it, else don't list it. And it's also the question then, should it be publicly or not. If it is publicly, it should be verified. If it's not publicly, it should also be verified because data that isn't verified is useless. Then there has been questions around, how should we verify this data? Maybe we should look into the industry that's already there. We have the certification authorities. The CA industry, an industry that's all about digital identities. Identities on the Internet and how we verify that we are sure you are who you say that you are. The CA industry has its forum, the CA/B forum that defines guidelines. We have the extended validation guidelines. Guidelines where all defend -- define how data should be validated to be able to trust it. That was my question.

KURT PRITZ: Thank you.

ROB HALL: Can I just touch on that briefly. We are widely divergent, as you can well imagine, within the registrar community on should we verify or not. The one thing that I think we're probably pretty unanimous on is, please don't tell us how to. So we are the competitive level of ICANN. We are the entrepreneurs on the innovative level. So tell us what you want us to do and I think you'll find that the thousand of us do it all very differently. So I don't think any of us are looking for the one unique Holy Grail solution. We're looking for the policy and then let us go and innovate and figure out how to verify. But I thank you for your comments, but I think that's one of the factors that registrars are pretty united on is we'll figure it out, just tell us what you want us to do cause --

>> Yeah, I can agree with that but the only thing I would like to say is why should we try to invent the wheel again while industry is working on it 15 years, over 15 years and has learned a lot of how to do it. How to do it in several countries. And those industries, they can work together. That doesn't say that you have to follow their rules. But talk to them.

ROB HALL: Oh, and I -- I imagine the day after the RAA was published for comment every single registrar got e-mails from companies such as yourself. It's not your company specifically saying we have a solution. We can do this for you. I think we are probably the most diverse group within ICANN with representatives and resellers and more regions than any other group in ICANN. We understand the global nature of this. We will figure it out. We may use already existing solutions, but I don't think

we're look for the community to prescribe this is the one size that fits all.

KURT PRITZ: Hi, Jeff.

JEFF NEUMAN: My name is Jeff Neuman, excuse me, and I'm up here as someone who has previously negotiated contracts with ICANN, which is always an interesting experience. There's very few of us that have but soon there will be 1,400 more so I welcome people to the club.

The first thing I want to point out is kind of joining on what James Bladel said at the very beginning, I think in setting up this agenda, it's my understanding that the registrars were not consulted. And I think when you set up an agenda for this instead of dictating how we should comment and what order you should probably let people just come up to the mic and give their comments.

[Applause]

So my first substantive comment is something that actually wasn't mentioned by Samantha that was something that ICANN had asked for in the drafts and I find it very interesting that it wasn't mentioned but it was basically changing the definition of Consensus Policies. It's always been my view, and I've said it for the last three years or four years now in the last set of contracts, that the definition of Consensus Policy should be exactly the same for registries and registrars. Avoid confusion. Especially in this time when there's vertical integration,

there's going to be registries that are registrars, registrars that are registries, et cetera. But interestingly enough, ICANN added a provision in there that basically says the Consensus Policy is now defined as the entire agreement. Everything now falls within the scope of Consensus Policies according to the changes by ICANN. I'm not aware of any requests by law enforcement or anyone else that had made that request, but it's not appropriate at all. It shouldn't be in there. And I ask that ICANN staff please remove it or explain in detail why there's a need to change it.

The second thing is on the revocation concept. Basically if you read the definition, it says to a certain extent that in the event that business models change over time ICANN has the unilateral right to terminate the agreement. Seriously. If ICANN determines that these business models are no longer acceptable to Joichi Ito could basically tell these large corporations and people that have made their entire businesses, millions and millions of dollars, some public companies that we can now destroy that model. Of course they do say that a registrar is free to apply to be an entity under this new model, whatever that is. So I think this is something that was tried with the registry agreements, the new gTLD registry agreements, and was obliterated after a little bit of time when they realized it didn't make any sense. But if we can't get rid of it, I would ask for the power to be mutual. So in the event the community determines that ICANN is no longer the appropriate entity to handle accreditation of registrars that the registrars could then revoke the agreement. Of course, ICANN would be able to apply to be that next entity. Thanks.

[Applause]

ROB HALL: Jeff, just one minor knit with what you said and I'll defend ICANN a little bit on this. We absolutely were consulted. We spent two sessions yesterday going through these slides on what we were going to talk about and there was no intent on either of our parts to limit discussion but rather try and get answers to the two questions we think are the biggest differences between us and we think a lot of the other stuff will fall out if we can solve some of these major issues. But there certainly wasn't agenda setting by ICANN and the registrars weren't consulted. Matt and I spent a few hours with them yesterday going over the slides. So I don't want to portray ICANN as ramrodding this by any means. We were both involved.

MATT SERLIN: Yeah, I -- sorry, just one second. I'd echo what Rob said and I'd also say what we started off with at the beginning is that -- what ICANN -- is a proposed draft. It is our hope and anticipation that some language, some of which you highlighted, will come out of that draft when we get to a final negotiated agreement.

KURT PRITZ: And I think, too, because I've been thinking about your comment and James Bladel's also, and the reason we chose these topics is that the negotiations are kind of at a holding point pending the resolution on these issues and then once we get past them there will be a full opportunity for comments on all of the rest of the aspects of the agreement as negotiated. So we're not seeking to foreclose that. We're

seeking to get some of the roadblocks out of the way so then we can have a public discussion on the rest of it. Hi, Judith.

JUDITH VAZQUEZ: Yes, Judith Vazquez. I speak as a registrant. Any new domain name that I have created requires pre-verification prior to domain resolution. And Benedict, I'm sorry to say this, but I do have a serious issue about putting my contact information on the public Internet. If you called me, I wouldn't believe you. There's a trust issue here. But I would trust my registrar. So which brings me to the importance of the RAA, of our contract. Any good contract focuses on trust and best business practice, but operational procedures follow as addendums which change over time. So to quote Bill, let's get this going. Thank you.

[Applause]

KURT PRITZ: Thanks, Judith. Hi, Mike.

MIKE PALAGE: Hi, Kurt. Mike Palage, Farris Global. First point, with regard to the issues of e-mail verification, phone verification and verification before resolution, when you were going through those slides I found it a little ironic because there is a gTLD registry right now and I created a gTLD registry doing all those things and it's ICM registry. And it's somewhat ironic that this particular registry that's been often demonized, villainized, it's been a hot topic over the years, they are actually the gold standard of what you're looking for. Not only do they do those three

standards, they actually do what Mr. Metalitz wants. They actually do address verification. So I think that that's important. You know, let's not discuss this in a vacuum. Let's look at what is currently being done in the marketplace. So this leads to point two. Over the last 12 years I've worked with over half of ICANN's new gTLD registries and in this last round I was involved in about 100 or 150, 160 applications. What I am encouraged to see is that a lot of the applicants that I was involved in want to do these things, right? They want to go above and beyond what is currently being done in the marketplace. So to me that is a validation of what ICANN is supposed to be about. The private sector, innovation, trying new things. And I -- the word of caution that I'd like to say here is we're kind of at a crossroads here. We could tackle this problem, right? And it is a problem and it's a problem that I support the IPC, I support law enforcement. But there's two ways we could sort of tackle this problem. One is we could sit there and get additional facts, try different models, let the private sector work. Right? That's option one. Option two is we can come up with a top-down solution in which we do not have all the facts. Which is perhaps being created in a vacuum. And I submit to you, if we go down with the top-down solution in which we do not have all the facts and this is being developed in a vacuum, we are going to have Digital Archery 2. Okay? So again, let's get facts, let's not develop this in a vacuum.

The third point, again, as I touched on previously, I think the concerns of law enforcement and the IPC are totally valid. This industry is not -- the domain name industry as a whole is not one of saints but it's not one of all sinners. I think it's a mixture. People trying to do better things. The point I would like to raise here is, about five years ago one of the

scourges of the domain name industry was domain name testing, testing. There was a problem. It really was a problem. And one of the interesting things that happened is a group of registries, particularly myself and Jeff Neuman, we got together and we proposed an RSEP that was supported by Afilias and Neustar to tackle the problem and what was ironic was when we put forth that RSEP proposal both by Afilias and Neustar, it was demonized by the IPC. We were told that we were somehow going to be legitimizing domain name testing and they opposed it. But guess what, a beautiful thing happened. It worked. Domain name testing went away. Those RSEP proposals were later adopted by the GNSO as Consensus Policies. So again, give the model a chance to work. It does work. It's not perfect, but it does work.

KURT PRITZ: Thank you, Mike.

>> Am I allowed to speak? I was told that he was the last one.

KURT PRITZ: Well --

[Laughter]

JOYCE LYNN: I am going to make it quick, short. Joyce Lynn, from 007Ms.com (phonetic). I'm concerned about the waiting period for the newly registered domain name to resolve because I think that you consider

domain name as a freedom of speech, freedom of commerce; that we are depriving those good players. And I would think that the bad players in the domain name industry is a very small percentage. So we are depriving them of the opportunity to express their opinions and everything. So, in other words, we are -- if we do that, then we are proving everybody is guilty before we can say you are innocent.

So I don't think that's a right approach. And besides, you don't really know what this domain name is going to do because I'm pretty sure the law enforcement officers, they are concerned about all the bad domain names. So I'm very, very concerned about this resolution waiting period.

Secondly, I would like to hear more about the difficulties that the law enforcement officers face when they are trying to chase those bad actors. I'm pretty sure the original reason that this whole thing is coming to a picture is because they had trouble. We really have not heard much about what kind of troubles, what kind of difficulties they have.

To me, okay, as my very limited knowledge about law enforcement, they have so much tools, they have so much time chasing the bad actors, they could have gone to the registries and say, This site is illegal. It is engaging in phishing or any other illegal activity. They should just suspend the domain names right away until they prove they are innocent.

It is a very effective tool to do that instead of casting a net and catch every fish just trying to look for a couple rotten ones. That's my comment.

[Applause]

KURT PRITZ: Thanks for being so patient to talk. We only have a couple minutes.

ROB GOLDING: I will be as quick as I can.

KURT PRITZ: Thank you.

ROB GOLDING: Rob Golding, Othello Technology Systems. I represent an ICANN accredited registrar, and we have to start from the position of why are we doing any of this? We know who our customers are. We know who the registrants are. They are the one that pay the registry fees. They are the ones that pay the ICANN fees. They are the ones that are paying for this conference. Yet, we are trying to make them all criminals. We are trying to screw them over or restrict who they can be.

Not one of the people we speak to who run or pay for the Internet care about WHOIS. The days of needing to call up the tech contact to get them to fix a typo in their DNS zone are long, long gone.

Registries don't seem to care. More and more of them don't publish information. And with thick WHOIS mandating across all new TLDs, I can see that extended.

Registrars don't care. The contractual requirement to run a WHOIS server to illegally display private information of individuals is specifically in contravention of a lot of EU country privacy laws.

Registrants don't care whilst the business may want a detail shown for security or trust reasons, individuals don't.

The only people who seem to care are spammers and scammers, the perpetual interfering committee members and law enforcement who seem to go to extreme lengths to bypass due process.

As a contracted party to the RAA, our standing position has to be to take the 2009 and discuss what we want taken out, not to discuss what non-contracted parties want to stick in.

Law enforcement will tell you all these things are to protect people. They won't mention that in 30 years of me receiving e-mail, not once have they managed to stop the king of Ongo Bongo offering me $100 million into my bank account. They won't mention the fact that the majority of online scams are from exploited Web sites and have got nothing to do with domain names. They won't tell you if they had any evidence of wrongdoing, that they can already obtain whatever information they need from the registrar.

My personal opinion is it is time to decommission WHOIS. It's had its day. It's outdated. It's not needed. We get rid of WHOIS, we reduce the cost to registrants. We reduce the cost to registrars. We reduce the cost of registries and we reduce the costs to ICANN.

[Applause]

KURT PRITZ: So, Bill, a closing word but not much more than the word.

BILL SMITH: Understand. I'm Bill Smith from PayPal. I can stand here and tell you that I'm not here from law enforcement but PayPal and eBay do use information from WHOIS, and we use it in ways to protect our customers and consumers at-large.

So I appreciate the comments from the last speaker. I side with him in many ways. If we could do away with WHOIS and allow our researchers and our people to conduct investigations, et cetera, to protect consumers, we would be happy to jump on board with it.

I would like -- the last comment was I wanted to respond to a comment made by Jeff Neuman regarding the proposal that ICANN put in to be able to terminate the contract with registrars, that's a good thing to have that out in full disclosure.

I would point out sections 5.2 and 5.3 from the current 2009 RAA. 5.is 2 regarding termination of agreement by registrar. That is three lines long. Section 5.3, termination of agreement by ICANN, ten times longer, 30 lines, specifically limiting how ICANN can currently terminate the agreement. Registrars can terminate their agreement. These are the large public corporations that Jeff spoke of who have a significant interest in a large number of the registrants or the registrants have a significant interest in their continuing to operate. They can terminate the agreement in 30 days' notice, period.

The only thing that the registrar must give up is any funds that they have already transmitted to ICANN. That's a very low bar. It is very lopsided in terms of the termination ability of either side. It is another example in my opinion, PayPal's opinion, why this contract needs to be negotiated and bring balance back into the equation. Thank you.

KURT PRITZ: So I would like to thank everyone for their contribution. We have just a few closing words. So if you could stay in your seats so everybody can hear.

Volker, did you have a few words you wanted to say?

VOLKER GREIMANN: Okay. I wanted to just briefly touch upon the topic of universal adoption of these new amendments. And this is one that the registrar community cares very deeply about because as it stands now, we have registrars under the 2009 agreement. We have registrars under the 2001 agreement. And once a lot of the proposed amendments that have been discussed here and some of them -- some very much more that haven't been discussed here come into the new agreement, we feel that going to marketplace in the way that there are three different registrar agreements out there, or even two, with different obligations for registrars, depending on the random chance when they renewed or signed their original agreements, does not really make sense or achieve any of the purposes of the amendments. So what we're looking for is for a method or a way to ensure that all registrars would be required to follow these new policies, once they become a part of the new RAA or

delay the release of the new RAA once -- to the point where every registrar becomes available.

We have a list of a couple of options there. I think one of the most valid ones is limitation of terms of new accreditations or renewal terms once we have new agreement to ensure that when the new agreement is signed, it has to be signed by all registrars without shortening, of course, the terms of the current agreement.

Another one would be creating milestones for phasing in of certain terms. Not sure how that would work, but we would certainly be open to discussions about that.

We have talked about incentivizing registrars to adopt the new RAA early. However, that would also lead to a situation where different policies are provided by different registrars and different registration policies would follow.

A registrar code of conduct process has been proposed. There is a lot of pushback on that from the registrar community because it is felt that this would be out of contract, out of compliance, out of policy way to implement new requirements. Some registrars are very worried about that.

And there has been a proposal that all registrars who want to be registrars under the new gTLDs would be required to follow this agreement. Now this would also create an imbalance between the old gTLDs and the new gTLDs. Not sure if that would be to the benefit of the new gTLDs in any way. So we are just putting these options out there and ask you to think of other options that would ensure that

registrars come under the new regime of the new RAA, whatever that may look like, we are not talking about any content here at roughly the same time.

KURT PRITZ: So one of our parties that's not sitting up here on the stage is Becky Burr, she would like to make a comment before we close, if you could all hang on one more minute.

BECKY BURR: Sorry, I just want to clarify one thing. There are -- I think we all would agree that the draft issued by ICANN probably overstates the ways in which we are apart. But with respect to Jeff's comment about consensus policy, I think that is a new provision. And I don't think that that's an over -- that his comment was -- I don't think I have any reason at least to believe that that's one of the things that falls away.

So I do want to make sure people pay attention to that provision, which is a very serious provision, in my view.

KURT PRITZ: Thank you, Becky.

So thank you very much. And thanks for staying a little bit late. These negotiations will continue. We encourage additional comments, especially on the issues discussed here on the community Wiki. We intend to close. We intend to publish a negotiated agreement for additional sessions like this and public comment so we can put a new, improved agreement in front of the ICANN board for approval.

You also know as another next step is that there's a GNSO PDP pending to discuss issues that aren't addressed here or any new issues. So, again, thank you very much. Thanks to our panelists for investing the time here. Everybody's really busy. So, thanks. Have a great meeting.

[Applause]