LOS ANGELES – At-Large Policy Roundtable
Wednesday, October 15, 2014 – 10:00 to 11:30
ICANN – Los Angeles, USA

HOLLY RAICHE: This is the At-Large Policy Roundtable on – is it Wednesday? It's Wednesday. First of all, thank you all for coming. I think we might have a very, very quick whip-around. Could people just say their name and, with about one second, their affiliation, and then we'll start on the first part of the session, which will be on the privacy proxy service. Well, actually on much larger issues, but we'll first hear everybody, and, Eduardo, you're going to have to stop reading and tell us what your name is. Thank you. Eduardo? Hello?

EDUARDO DIAZ: Eduardo Diaz, ALAC.

MOHAMED EL BASHIER: Mohamed El Bashir, AFRALO.

STEPHANIE PERRIN: Stephanie Perrin, NCSG.

GRAEME BUNTON: Graeme Bunton from Tucows for Registrar.

TOM MACKENZIE: Tom Mackenzie from the OP3FT. I shall be giving a short presentation of the Frogans project during this session.

STEPHANE VAN GELDER: Stephane Van Gelder. I'm with Tom on the OP3FT.

SARAH BOCKEY: Sarah Bockey, Go Daddy.

JAMES BLADEL: And James Bladel, Go Daddy.

EVAN LEIBOVITCH: Evan Leibovitch, moderator of the second session, filling in for Garth Bruen. Vice Chair of ALAC. I'd be here anyway.

HOLLY RAICHE: Holly Raiche, Internet Society of Australia and ALAC.

HEIDI ULLRICH: Heidi Ullrich, ICANN staff.

SILVIA VIVANCO: Silvia Vivanco, ICANN staff.

GISELLA GRUBER-WHITE: Gisella Gruber, ICANN staff.

DAVID SOLOMONOFF: David Solomonoff, Internet Society of New York.

[YASUICHI KITAMURA]: [Yasuichi Kitamura] from APRALO.

JOHN LAPRISE: John Laprise, NARALO.

DAVE PISCITELLO: Dave Piscitello, ICANN staff.

HOLLY RAICHE: Thanks. Gisella, can we start with the slides, and can we have a full screen?

EVA OLSSON: Oh, hi! Eva Olsson, Lawrence Berkeley Lab.

CAROLYN [WYNNE]: Carolyn [Wynne], Microsoft.

UNIDENTIFIED SPEAKER: [inaudible], Indiana University.

HOLLY RAICHE: Thanks. First slide, please.

FATIMATA SEYE SYLLA: [inaudible], can I introduce myself?

HOLLY RAICHE: Could I have that bigger? Because right now you can't read it. Go ahead.

FATIMATA SEYE SYLLA: Fatimata Seye Sylla, AFRALO.

HOLLY RAICHE: Thank you. I don't want to see a picture of me. I don't. Anthony, you're almost too late. Okay, thank you, everybody. What this is about is – for some of you, this is very, very old territory. Please do try and stay awake. For some of you, this is not old territory, but it's important background to understand where we are in terms of both the issue of proxy services, which is part of a larger issue of WHOIS, and for those of you who went to the actual WHOIS session, you will have heard at least a little bit of this anyway, but probably not the full background.

That's the order in which I'm going to talk, and some of you, as I say, will know this anyway, but just to keep you all...to bring everybody up to speed at the same time. Could I have the next slide? Thank you.

This is all about WHOIS, and what we really mean, and what was said yesterday by the guy from SSAC was to point out actually the registration data is probably a better name, but WHOIS is the term we use really shorthand for a bunch of information that is required to be made publicly available. I'll stop here, and say the issue behind all of this is a fundamental tension between, historically, the requirement to make WHOIS information publicly available, and the way that it's run right up against privacy laws about 30 or 40 years later.

WHOIS data used to be, when a bunch of geeks were the only ones who were on the Internet, and they wanted to talk to each other, they wanted to know how to get a hold of each other. That was fine, but that was a long time ago, and the requirement for people to identify who they are and where they are, and a lot of information about themselves, which was written into some pretty fundamental documentation a long time ago, is now in clear violation of what is a growing body of privacy law.

So we'll go back and say, "What is WHOIS data, or what is the requirement?" The requirement is now in the registrar's accreditation agreement. That's the agreement between ICANN and the registrar. I think it's clause 3.1.8. We've all memorized it.

Essentially it says this is what must be made publicly available as part of the WHOIS data: The names of primary/secondary name services; the identity of the registrar; the dates; the name/postal address of – sorry, the registered name-holder is another name holder for "registrant." That's the person who actually has got the domain name and the use of the domain name, doesn't own it. Their name, postal address, e-mail address, etc., and the name, postal address, e-mail address, etc. You can read it. But that it is what is included in the WHOIS data that, under the RAA, must be publicly available. Next slide. Thank you. I'll say, "Next slide, please." I'm being rude.

The issue of WHOIS data, by the way, has been around for a very long time. I was a latecomer in that in 2009 I was involved in the beginnings of negotiation on what to do about WHOIS requirements. At the time, there was a growing concern about the actual accuracy of the data that

was held in the WHOIS database, and there are probably two basic reasons why there is inaccuracy.

One probably has to do with the fact that the person doesn't necessarily want to be identified because they're a miscreant, and they want to cause mischief. The other is a range of quite legitimate reasons why someone doesn't want to be identified, starting with they don't want to be identified, but there are a range of reasons why not, not the least may be that people don't wish to have accurate information about them. James?

JAMES BLADEL: I didn't know if you wanted to take questions or comments as we go along, but as a member of the WHOIS review team – and I don't know if there are other members here – I just want to point out that the first bullet point saying that only 23% of WHOIS records are accurate maybe isn't telling the entire story.

HOLLY RAICHE: I'm absolutely aware of that. That was why they said the level was inaccurate. Now, I know there are levels of inaccuracy there.

JAMES BLADEL: Right, it was not a black-and-white line. It was very much shades of gray, and I think what we found was that only 23% of WHOIS data records were perfectly accurate. Some – a vast majority, in fact – had some inaccuracies, but still functionally contactable, and then there was a

small percentage that was so inaccurate that it was useless as a point of contact. There was this spectrum.

I'm just pointing this out because I think the bullet point, as it reads in this slide, is very damning.

HOLLY RAICHE: James is right. I do remember the review team saying, "We have to do something about accuracy," but the review team, in the final, then said – this is, by the way, NORC team, and you can read this report still. Actually, there is a link there to the final NORC results, if like.

Oops, I've lost my next slide. That's okay, Kathy. That's fine. You can't read that too well, but what the report pointed out was that, in fact, there are a number of quite legitimate reasons why somebody would use a privacy proxy service. For individuals, they just might want to protect their privacy. There are a number of organizations, things like women's refuges, that certainly don't want their contact information available – religious groups, political groups, ethnic minorities, and companies as well that are about to introduce new products or services, and don't want the information made available for quite sensible corporate reasons.

So there are a number of reasons why, in fact, people do not want information about themselves and their names published. But there are also concerns, and it's clear that there has been an abuse by some of privacy proxy services simply to hide who they are.

So it's not that everything and everyone who actually uses one is wrong or bad. There is a recognition that the final report made: There is a

whole range of reasons why people use privacy proxy services, and many of them are sensible, so perhaps we actually have to deal with the issue of what a privacy proxy service is, when one is, when one isn't, where they are accredited, and who can use them. Next slide.

This is what the final review team recommended, that there should be some kind of consistent and enforceable requirement for the privacy proxy services that are – and this is important – consistent with national laws, because increasingly, national laws include laws about privacy, and to strike an appropriate balance, which is what we're trying to do throughout. Could I have the next slide?

In the 2013 RAA, as a consequence, there was a new clause, Clause 3.14, which actually said registrars have to comply with a specification. I'll tell you what's in the specification. The specification for privacy proxy services was drafted. It was part of the actual agreement of 2013, but it looked forward to the development through the GNSO PDP process of developing actually a specification.

So there is something that registrars have to comply with until the Privacy Proxy Working Group – and I'm not going to go into that history – comes up with a specification for privacy proxy registrars. Next slide – oh, James wants to – okay.

JAMES BLADEL: Just one note on that temporary specification for privacy proxy services. That does have a sunset date.

HOLLY RAICHE: I know.

JAMES BLADEL: Oh, is it in there?

HOLLY RAICHE: No.

JAMES BLADEL: Okay. The sunset date is, I believe, January 1, 2017, and that was done deliberately to ensure that the effort to develop a full privacy proxy accreditation service did not go on the pile of "someday" projects for ICANN, that it got moving and got formed. One of our co-Vice Chairs of that effort, Graeme Bunton, is here, and that PDP is well underway to develop that program. I have to believe that having an expiration date attached to a policy helped move that successor effort along.

HOLLY RAICHE: I remember, when first joining the working group, thinking, "2017? Am I going to be involved in [inaudible] until that time?" I'm optimistic we meet the date.

Okay. This is what registrars must comply with now until the working group comes up with a final specification. First of all, basic thing: Compliance is required, and then there is a range of existing requirements, and they are: The terms of the privacy proxy service must be publicly available, the identity of the provider, the prices that are charged, how data will be requested, when it will be revealed – and, by

the way, these are terms I will talk about – how to transfer from one registrar to another if you are using a privacy proxy service; how disputes are handled; things about points of conduct; where data is stored, the fact that is should be stored, and then allegations of misconduct – and, again, we're dealing with what that term is – have to be relayed.

So that's what now is in place until such time as the specification that is now being drafted by the GNSO Privacy Proxy Working Group that's working through what the final specifications look like. Until we've completed our task, that's what has to be complied with. Next slide. Thank you.

A working group is always started with a charter. The list of questions that had to be answered was very long, and actually not necessarily in a logical order, so the first thing we did was to say, "Let's group all of the charter questions that we have to answer into some groupings that are manageable." This is the way we're actually, as a working group, working through all of the issues involved in privacy proxy specification; things like, first of all, what the tests for accreditation are going to be; who is going to do the accreditation; how it will be done; what happens if somebody doesn't comply; what the sanctions are; what non-compliance is. That's before you start.

Then you have a lot of issues about if there is a different between a privacy service and a proxy service. Then you have what information is revealed or not, and, by the way, we had to come up with some very clear terminology.

In the context of data from a privacy proxy service, relay simply means that the privacy proxy service provider will get a request from someone that information the requester has should be relayed to the customer. It's a request for relay.

"Reveal" is different. It is that data that is concerning the customer of the privacy proxy service is revealed to a requester, not generally, and then the term "publication" means information is available generally.

So we had to actually agree to use those kinds of terms to understand what we're talking about, and we have to go through the circumstances in which all apply, and there are lots of questions in each of those. We have to deal with issues of transfer, and I'll get to that.

Finally, who accredits, who checks or terminates, and we haven't even got to those issues you. We've got a lot of work in front of them, but we're actually making some good progress. Next slide, please. James?

JAMES BLADEL: Just through the course of the working group, I think one of the things that we've addressed is the idea that this distinction between reveal and publish, particularly reveal to a single requester. From a consumer perspective, it makes more sense, certainly, if you feel I'm doing something wrong and reveal it to the complainant as opposed to publishing in the public WHOIS. But from a provider perspective – and actually something we hadn't considered – it makes more sense to perhaps expose it publicly, so as not to assume exclusive liability for anything that might be done or misused on the part of that knowledge. It's an interesting discussion that we can have.

Also, it's just one of my little quirks or something, but that says GNSO-zero, not GNSO, the letter O. If somebody could fix that, that's a splinter in my brain right now.

HOLLY RAICHE: My apologies!

JAMES BLADEL: It's almost like an IDN homographic attack.

HOLLY RAICHE: Think of it as IDN variant. It will be changed. Could somebody make a note that I should change it? Thank you. James, I promise it will be fixed. Next slide, please.

We have already come to some early conclusions by the working group. Some of this may seem obvious, but that's okay. It's all been discussed. You would say, "The existing specification requires this anyway; why are we repeating it?" But, in fact, in the specification, that will be the product of this group. We need to actually be very clear about what is or isn't going to be required. Yes, we say the obvious, but that's okay. It remains a requirement.

Privacy proxy services must relay to their customers any notices required under the registrar accreditation agreement or consensus policies. Sound obvious, but that's fine. It's one of the things that we will put in there.

Again, transparency in terms of, if you want to be a customer of a privacy proxy service, you ought to be able to have full knowledge of your rights, your obligations, particularly the details about when information will be passed on to you, when it will be revealed, the circumstances under which both will happen, as well as information about transfers. So, in fact, the stuff that's important for a potential customer of a privacy proxy service – they should have some transparency about what they're getting themselves into.

Some of the things we've said are best practice, and I will get into more detail, because we've discussed this more fully. I'll talk about transfer in a coming slide, and we're still dealing with this privacy proxy service issue. Should you use commercially reasonable efforts to avoid the need to disclose any customer data in the process of renewing, transferring, or restoring? Now, that is the intention, and we're still working through what that means. Next slide, please.

I think we've gone backwards. Dave?

DAVE PISCITELLO: Before you leave this, I just wanted to... Can we go back to that?

HOLLY RAICHE: Can we go back? Early conclusions, yes.

DAVE PISCITELLO: Just as an observation, when you say that privacy proxy service must relay to the customer a notice or an action, in the case of a criminal domain – for example, a domain that's algorithmically generated on a

daily basis for a botnet – would that mean that if the domain is actually privacy-protected, that the privacy protection service operator is obliged to contact the criminal if he has the ability to say, "We're taking down your DGA?"

HOLLY RAICHE: I think if you're talking about one, it's to relay to their customer. Did I say a requirement to tell the customer that their information –

DAVE PISCITELLO: I'm just trying to get a clarification on that, because I don't quite understand the consequence to a criminal investigation.

HOLLY RAICHE: What number are you referring to on that slide?

DAVE PISCITELLO: Number one, on the top.

HOLLY RAICHE: “Must relay to their customers any notices." Let me back up and probably go a little bit further, because in subsequent discussions, we have actually started to distinguish between requirements that are from law enforcement agencies, and trying to work out the context and definition of law enforcement agencies, versus other things that perhaps are not criminal in nature. What we have heard from our own Chair of the Working Group is that law enforcement agencies are never

going to ask for a relay. They're going to go straight for "tell me who it is." I suspect that's right.

Now, in practice, I would imagine, Graeme or James, that would be what you'd expect to happen. I don't expect that the law enforcement agencies are going to say, "Pass on..."

DAVE PISCITELLO: Just bear in mind that not all criminal activities and takedowns are performed by law enforcement. In fact, that's actually the minority of suspensions, especially in cases of things like algorithmically generated domains for botnets.

HOLLY RAICHE: I think we're taking questions now. Stephanie first and then Kathy.

STEPHANIE PERRIN: I just thought that I would jump in here at some point and interject that some of the procedures that have developed at ICANN over the years do not necessarily reflect human rights law. For instance, in Canada, it's taken us quite a long time to get a case through the Supreme Court that what is required for law enforcement when accessing telecommunications providers to get my name and address and who I really am. In that judgment, we have strong language on the right to anonymity.

Now, from the human rights perspective, there is a discussion going on at ICANN at 1:15 on the Council of Europe's report on ICANN activity with respect to human rights, notably freedom of expression and

privacy, freedom of association as well, and I think we're going to have to retrofit some of the legal framework onto practice.

Now, law enforcement has no problem getting a warrant. They have problems with time delays, they have problems with the fact that the Budapest Convention doesn't work, but they're not the ones that are going to have issues with this. It will be the private sector security guys and the intellectual property guys, who claim, of course, that they're enforcing criminal law, because violation of copyright has criminal – But we can all go there. There are criminal penalties in data protection law.

I expect maybe we'll hit our deadline for this, but I wouldn't be surprised if we have to do a little retrofitting.

HOLLY RAICHE: Thanks. Kathy?

KATHY CLYMAN: My name is Kathy Clyman. I'm with the Non-Commercial Stakeholders Group, and I'm very pleased to be here today. Holly, the explanation is great. Dave, to your point, I don't think number one hits what you're concerned that it hits. Let me give you the background, and then if you have any wording changes, we should do that so that we can focus on we intend number one to focus on, because we didn't think there was ambiguity.

All proxy privacy services must relay to their customer any notices required under the RAA or ICANN consensus policy. What was happening, apparently, is that some proxy privacy providers allowed

you to check a box that said "Don't forward anything," but in the process, you didn't get your renewal notices. You didn't get your notices that say, "Keep your information up-to-date and accurate, even behind the screen," so things were getting lost because people didn't get the right information. This is just saying if it's official, and it comes from ICANN, and you'd have to get it as a registrant or you'd have the right to get it as a registrant, you have the right to get it as the customer of a proxy privacy provider. That's the whole idea, just to take that small set of official notices, and push it down all the way.

DAVE PISCITELLO: I just asked the question. I'm not going to go close to trying to sort out the policy in a short period of time. The only thing I'm concerned about with the way that we currently have privacy and proxy protection is that, from a pursuit of criminal or malicious registrations perspective, the presence of privacy proxy is one more delay in trying to accelerate a suspension of criminal activity. So I just want that to be very much in the mindset of the people who are on the committee.

We all don't want to be phished. If the ideal takedown time is two to four hours, so that we minimize the harm of a domain, then adding a pass-through or some other request to privacy proxy to get some information can be troublesome. We all know how problematic botnets are, and if I could be in automation, I would probably be supporting dozens of other security researchers that come to me on a daily basis, and say, "Can you help us with the registrar" – not the people in this room, because they're all actually really good at this, by the way, but there are others who are not – and say, "How do I do this? How do I get

through here? I have 24 hours. If I don't suspend this within 24 hours, tomorrow the botnet is live again."

I know that law enforcement get court orders. Unfortunately, most of the response to criminal activity and malicious registrations is not done through court orders. We have a tension in time, because I don't know that we'll ever get to a point where we'll have a court order that can be issued in four hours.

HOLLY RAICHE: Thank you for the contribution. I think one of the reasons for this forum is to actually flesh out the sorts of responses we need as we move along. So that's very useful to the way we talk about law enforcement and criminal activity. Can I have the next slide? I'm hoping we get through. I'll get through these very quickly.

Those are some of the early conclusions. I'm not going to go into them. Could I have the next slide, please?

We all met on this Friday and reached some – I will call them tentative – conclusions. Terms of transfer – what James and Graeme and others told us is that it's very difficult to actually transfer. If you are a customer of a privacy proxy service, the situation in which there is very real difficulty in transferring is, if you are a privacy proxy service customer and you want to maintain your privacy, can you transfer? And there is difficulty.

One of the issues that we're working through is how you transfer from one privacy proxy service to another without revealing your details, and some of that answer may be in the fact that a privacy proxy service is

accredited, and going to another accredited one, but we haven't actually locked that down. Can I have the next slide?

Another issue is the whole issue of reveal, both in terms of what it means and what it requires. First of all, what details are actually revealed, and then under what circumstances? We're working through this now, but it seems to be the case that when registrars receive a request, it's dealt with on a case by case basis, and they usually require – we're just calling it prima facie evidence – some kind of information that indicates that the person requesting the reveal is bona fide, and that there's a genuine cause for this. Can't do any better language than that. We tried; we're working on the language, and we're also working through whether or not the customer should be told and given some kind of time in which to respond or not. These are issues in front of us. Next slide. Thank you.

Now, we're moving to the EWG, and I thought we'd have time to do this. When the Board decided in 2013 to move with a specification for privacy proxy services, what they also did is say, "We need to think about another way of dealing with the requirement for that kind of contact information to be held, and should we actually rethink the whole structure of WHOIS?"

That was their characterization, or, rather, this is Carlton Samuels's characterization of what they said. Could I have the next slide? Thank you.

They recommended a completely different model. Now, in the discussion on WHOIS, there was a lot of discussion not only on where we're up to with privacy proxy services, but also where we're up to with

Expert Working Group recommendations, and whether the two fit, whether we should move on both, and whether, in fact, you're going to be asking registrars at some point to change their systems to deal with a new specification, and then very closely after that, change the systems again radically to deal with the concept of what the Expert Working Group came up with, which is essentially a very large database in which there will be very real efforts for verification of all the data, and then a characterization of what data is made public, what isn't, when it's revealed, and so there is consistency.

So we in the Privacy Proxy Services Working Group are coming up with one solution, thinking that there may be a different solution down the track, and how these two fit. It was the subject of a lot of discussion in the final stages of the WHOIS sessions. I think it was Monday. With that, and almost no time for discussion, I would love discussion. James, have you got anything further?

JAMES BLADEL: No, but thank you for putting me on the spot. Actually, I think probably, as far as this issue, it's one of the jokes I made – maybe Kathy remembers – going back to 2009. There have been problems with WHOIS since I've been in high school, and they're still ongoing. I don't know if you guys know, I'm not high school-aged any more, but I think that you could always– What's that?

DAVE PISCITELLO: Since I've been in high school.

JAMES BLADEL: Since Dave's been in high school, which is two years after I got there, right? Yeah, at least.

It's the joke, too, that you can always spot the newcomers to ICANN because they've got a great idea to fix WHOIS. I think it's only through an understanding of all the complexities that WHOIS is the intersection, not only of privacy issues and accountability issues and – now let's put the elephant on the table – surveillance issues as well as some of the other social issues that bubble up into the Internet. They weren't born in the Internet, but they're spilling over into this online ecosystem.

And I think, from a service provider's perspective, we don't want to be harboring bad actors. We don't want that junk on our network, but on the other hand, there seems to a desire and in fact a demand from other segments of the community to infuse some degree of omniscience into WHOIS, that we know who they are even if they're criminals, and we can tell when they're lying, and we understand their intention before they do something bad.

I think it gets us into a very weird space, and of course we're all trying to do this and still make a couple of dollars or euros, or whatever. That becomes very challenging whenever you get outside of an automated environment, and start having human beings inspect and put all of these systems under a microscope.

I think the work is going in the right direction. I think, initially, I was very concerned, not just as a service provider that's watch-dogging some products, but as a consumer. I use our privacy proxy service. I tell the story of the Buenos Aires meeting a year ago. I just registered a domain name, couldn't believe it wasn't registered, and it was a controversial

issue in the US at the time. I couldn't believe that word wasn't taken in dot-com, and during the Buenos Aires meeting, I received no less than 18 telephone calls on my cell phone within 48 hours after registering it, asking me what I was going to do, if I wanted a web service, if I wanted to sell it. I said, "That's it." I went and activated Domains By Proxy, and it went away.

There's the answer to "I don't want to receive these communications, these unwanted messages." How does that correspond to a relay, which is someone like Dave? "I have to get this message to the person on the other end; I know that it's unsolicited, and they have chosen not to receive unsolicited messages." Dave's a good guy, and the message he has has a good intention and will better the operation of the Internet and the DNS, versus the army of people who may not be so well-intentioned.

I think that one of the ideas we have floated in the Privacy Proxy Group that's surprisingly enjoying broad support is the idea that requesters of these systems should be authenticated. They should have to create an account, say who they are, and if they abuse that privilege, it should be revoked and they should be banned from accessing those tools again. That's just one way to try and curb the potential for abuse while still leaving it available for legitimate purposes.

I think there was earlier talk that only natural persons, not businesses, should have access to these services. We've explored, both in the context of the WHOIS review team and in this working group, that's not a good idea. Businesses have mergers, and new products, and all kinds of reasons they don't want to -- anyone who knows when Apple

releases a new product, and all the "domain-ers" are cruising WHOIS to see if Apple registered iPad or iSlate or iTablet, and they were trying to figure out what they were going to name it so they could register all the domain names that were associated with it.

These are real-world considerations that are a factor, and I think that we're making progress, but I'm not yet ready to say that we have a good idea to fix WHOIS. Holly?

HOLLY RAICHE: Thanks, James. We've got in the queue Evan, we've got Stephanie, and we've got Dave, and our time is up in about how long? I'll have to cut it off after Stephanie and Dave, but, first of all, thank you, everybody for being here, and to say this is a very live issue. We are still grappling with a lot of the issues, so any and all contributions are welcome now. Stephanie, then Dave, then over to the next session.

STEPHANIE PERRIN: Just a few comments on the Expert Working Group report. I was on the Expert Working Group. It's a massive report which I encourage you read. It was a rough consensus, from which I dissented on a couple of key points, but let's not kid ourselves. As a privacy advocate and someone who's worked in risk, there are a lot of things in there that I certainly don't agree with, one thing being, of course, right off the top, you have to apply data protection law that exists already, and we're doing it in a backwards way.

The risk for the end-user has not, in my view, been properly assessed across the board, and we have a public responsibility at ICANN to do that.

The work on the implementation of the Experts Working Group report is going to start soon. Figuring out what pieces still need a lot more homework, I think, is important. We had an all things WHOIS session the other day, but what we don't have is an all things WHOIS that looks at end-users and what their issues are, because I think James hit the nail on the head. Now we're talking about risk analysis, and projection and surveillance for market purposes, personality profile purposes, for surveillance in terms of limiting free speech and freedom of association. And of course lots of people want richer data in there, and they certainly want it accurate.

From a perspective of Big Data, we have to watch what we're putting out there. Thank you.

HOLLY RAICHE: Dave?

DAVE PISCITELLO; Just quickly, James mentioned the need for vetting, and the Anti-Phishing Working Group has begun a program, and is in its pilot stages with about 15 to 18 ccTLD and other TLD registrars or registries, and we're actually talking with the registrars about the program. It's a voluntary program where there will be a vetted intervener program, and right now we're starting with APWG members, but one of the goals

we'd have in the future is to bring in people from civil society and from other realms to help us with the vetting process.

The goal is to a trusted intermediary, where we'd be able to submit attestations about a malicious registration; the registrar would be able to say, "I have high confidence with this reporter because he's been vetted by parties that I trust," and will be able to act on that.

I think this is a really, really interesting model. If you haven't seen it before, please try to get in touch with me, and I'll share a presentation that I gave on it at an APWG meeting recently. It's a very exciting process, because all over I see the need for vetted intervention, and if we can come up with a good model for the vetting and credentialing people, so to speak, who are going to actually do it, I think that this has a lot of merit, not only in Anti-Phishing, but in other aspects of WHOIS, WHOIS access, and the like. Thank you.

HOLLY RAICHE: That is fantastic, and I'm sure we will all bring that back into the discussions of the privacy proxy and maybe even EWG.

With that, Heidi's at my shoulder, telling me I'm way over time, and Evan's antsy. So, thank you, everybody, for this session, and over to you, Evan.

EVAN LEIBOVITCH: Thanks. Not quite antsy, but that's okay. All right, so we're going to switch gears a bit, and talk about something quite a bit different, and it

has to do with alternatives and innovations in the realm of DNS. Could you switch the slides, please? Also, could you scroll the – thank you.

I'm working at a little bit of a disadvantage. I'm filling in for Garth Bruen, who can't be in Los Angeles, unfortunately, for personal reasons, so in addition to the bits and pieces of this I know myself, I will try and work to Garth's introduction, and Dave has graciously offered to assist me in filling in the many blanks in what I have to offer to this. So I hope to be spending a very little amount of time talking myself about this, and encouraging folks at the table to contribute.

Personally for myself, this has been an issue that's very near and dear to me. I participate in the Metrics Group dealing with the new gTLDs, and one of the things that is recurring when they talk about the metrics is they talk about the competition between the new gTLDs, between the new registrars and registries and business models. One of the things At-Large has been quick to point out is that the competition is not just between the registrars and registries, but between the DNS itself and alternate ways for end-users to find the information they want over the Internet. DNS is one way to do it. Things like QR codes and search engines and social media are other ways to do it, but today we're going to discuss actual alternatives to the DNS.

Could I get up Garth's slides?

Okay, the whole issue of "to DNS or not to DNS," the chart up there essentially says, out of all the sites that are using IP addresses, DNS points to a subset of them, and the number of DNS-pointed sites that are web-enabled is even smaller yet. The question is, if you're not using DNS to get to web content, what else are you using? Next slide, please.

What we're going to try and talk about today is alternative roots, dotless domains, the concept of Tor, DNS substructures, and other innovations in gTLD such as creative uses of second-level domains, which I personally am very interested in. Next.

The questions that we're going to try and raise, and hopefully have a little bit of discussion around the table, time allowing, is where ICANN comes into this. There have been all sorts of root systems. ICANN manages the canonical one that most of the world uses, but there certainly have been many other attempts. How does the consumer deal with it, and so on. These are, essentially, some of the questions. One of them is if other countries will reach a split from the single root. A couple of them already have, or have created their own duplicate systems. The issue of whether domains will even matter eventually – obviously up in the air. Certainly I'm not going to answer that now, but certainly I think it's worth noting, and it's worth ICANN being aware of the fact that the Internet has a way of working around obstacles, and if the DNS turns out to be an obstacle for the general public, there are going to be different ways to do this. Next slide. Okay.

At this point, talking about other structures, I'm going to turn it over to Dave, who can give a little bit of historical perspective to an idea of the many attempts made to try and do parallel ICANNs, if you would.

Dave?

DAVE PISCITELLO: Thank you, Evan. This is not a new topic. In fact, when I was the fellow for SSAC back in 2006, I wrote about this, and you can tell how old the

report is, because it's SAC document number 009, and I think we're in the sixties.

I'm going to try to be relatively brief, because I know we're behind, and I know that there are lots of other things to talk about. The concept of an alternative root is that instead of going to the authoritative root that IANA publishes, along with VeriSign and NTIA, and serves as the first query in the public DNS, you go somewhere else. Where else you go depends on the motivation of the operator of this so-called alternative root, and the purpose of most of the alternative roots is to provide something outside of the normal list of top-level domains.

In the report that I'll just have Holly circulate to you, what I did was I went and I did a lot of study back then, and it seems like it's actually still relevant, because some of these people seem to be still be in operation, but I classified alternative roots into five major groups. One is private name systems, and lots of you may be familiar with the whole name collision issue. Private name systems actually attempted to create roots within organizations, and then you would literally run your own DNS right from the root within your own organization. If you didn't want to use any of the public DNS, you could do this, and it was supposed to be completely separate and distinct from the public DNS. The reason why we have these name collision issues now is because now some of the names that used to be "private names" for these organizations are no longer private.

There are also experimental names systems. People wanted to throw up a TLD and to use it for a very short period of time for experimental

purposes. It was impossible to get that into the process of actually publishing in the ICANN or the authoritative root.

Another was commercial competitors, people who could not, back in the earlier days, especially in the 2006 timeframe, hope or imagine to apply for and receive a new TLD application that you might be able to do today, and so they simply set up their own structures.

Then there were also protest TLDs. There were groups of people who said, "I don't trust ICANN, I don't trust the US government, I don't want to have anything to do with the authoritative root, so we're going to create our own," and the politically motivated TLDs – as Evan said, there are reasons for certain countries to feel like they need control over the root so that they can actually control the content and any other communication of their citizenry.

There are lots of issues for these, and I'm not going to go through many of them, but from the ALAC or the typical user perspective, the complication of these things is the inability to disambiguate between the public and any of these alternative roots. Lots of these alternative routes, if you go and actually look at their root zone, have names that are in the list of new TLD applicants. They have names that people wanted to use and couldn't get from ICANN, and they said, "Well, fine. I'm going to use it myself." So there are a lot of – I'll use the term "adolescents" – in some of the alternative root. "I couldn't get it my way with you; I'm going to get it my way with me."

The biggest problem with users is that you have to have, typically, some additional software or file in your computer to get you to the alternate root instead of the conventional root, because most modern day

operating systems, whether it's on traditional laptops and computers or on mobile devices, has a DNS agent, something called a stub resolver. That stub resolver gets what's called priming information when the information system starts, and it says, "Here's where all the root servers are." When it says "all the root servers," it means all the IANA-assigned root servers, not all these alternative root servers. So you have to wedge something in as one of these alternative providers so that their root service is either embedded and replaces the ICANN root, or somehow operates with the ICANN root in a non-interfering fashion. Through all my research back then, I could not find any that could operate unequivocally with the ICANN root.

So the concern back in 2006 was fragmentation of the root, because there people at the time who, for mostly political reasons, looking to basically be able to have a root that was distinguished from the root that is published by IANA.

Let me just end there, and say that it's complicated to go into this space. It's not a space that I see, even today, being particularly large, having a particular strong influence in fragmenting except for the politically motivated roots.

But even then, the complexity for political entities that want to separate the root, is increased by the presence of a signed zone, a DNS- signed root zone. It's very hard to actually put any– well, it's impossible to make a change to the root zone and have the signature not fail, so you have to do a lot of interesting "widging" and controlling of anything that your citizens would use in order for the root not to misbehave, or to always return unvalidated responses.

That's just not going to work, especially if you ever expect anyone outside of your own controlled citizenry to be able to just come in with their own devices and behave the way they did before they crossed your border.

So I don't actually see this as a particular problem, and it never manifested as a particularly large enough problem to do much more than write a report, explain what it was, and just move on. Thank you.

EVAN LEIBOVITCH: Thanks, Dave. Could you go on to the next slide, please? I'm not going to spend much time on dotless domains. About a year ago, this was a source of – oh, Olivier, you have the floor.

OLIVIER CREPIN-LEBLOND: Thank you very much. Evan. Are we allowed questions at some point, or at the end?

EVAN LEIBOVITCH: If you have some questions of Dave, please go ahead.

OLIVIER CREPIN-LEBLOND: Thank you. I've noticed a number of examples. What about dot-onion?

EVAN LEIBOVITCH: Actually, Olivier, I can answer that, because we haven't done that yet. We're about to get to it. We haven't done Tor.

As said, the issue of dotless domains was extremely contentious within ICANN about a year ago, so I'm not going to rehash it. Just, suffice it to say, pretty well every constituency within ICANN came to the conclusion that this was a really bad idea, and so we've essentially moved on.

Olivier, this is to answer your question. At this point, I'm going to hand the floor over to the folks that can talk about Tor and similar technologies. So, Tom, would you like to go ahead?

TOM MACKENZIE: Hi. Thanks. My name is Tom Mackenzie, and I work as stakeholder relations for the OP3FT, which is the Organization for the Protection, Promotion, and Progress of the Frogans Technology. I'm hoping to tell you a little bit about this technology. I can't tell you very much about Tor, as I think our technologies are very different. In any case, I can't claim to know anything about how Tor functions.

EVAN LEIBOVITCH: My apologies. I didn't mean to mix the two together. I guess Garth was hoping to talk more about Tor and did not have this opportunity, so we'll basically skip over this for now, ask you to talk about Frogans, and, Olivier, if you can talk a little bit later about Tor?

OLIVIER LEBLOND-CREPIN: Thank you very much, Evan. Just to say maybe, because Tor is hidden, maybe there is someone from Tor, but they're just hidden.

No, just kidding. I'm not going to be able to speak about Tor. I don't really know much about it, so back to Tom.

EVAN LEIBOVITCH: Okay. We've already dealt with Tor at a previous roundtable of this kind, sp, Tom, please introduce us to Frogans.

TOM MACKENZIE: Okay. Do I have ten, 15 minutes, something like that? Ten? Ten minutes. All right.

Some of you may have heard of this Frogans project. In fact, I'd be curious to know, in this room, has anybody has heard of this project? Frogans? One, two. That's actually not bad.

Others may have heard of it. When going around the conference this week, I've come across people who have heard of it but really don't understand what it's about exactly, and they're wondering what this strange French creature with a reptilian-sounding name is doing in the middle of the gTLD program. Others, of course, have never heard of the project at all.

My aim this morning is just to really tell you a little bit about what it's all about, and to explain to you why we're here in L.A., and why I'm here sitting at this table with you this morning.

The first question – why in L.A.? That's the easy one to answer. We're in L.A. at the ICANN meeting because the Frogans project includes a new top-level domain: Dot-Frogans. In that sense, we're here taking part in the discussions. We're a member of the Registry Stakeholder Group, and we're interested in following the whole process around the

delegation of the gTLD. The dot-Frogans was delegated in April this year.

The second question – why I'm here, sitting around this table – is the more interesting question, and I'll tell you a little bit more about that.

To begin at the beginning, and understand this Frogans project, what you have to get is we are a top-level domain. We've got this dot-Frogans top-level domain, but the most important thing to understand is that we will not be selling or exploiting in any way domain names under the dot-Frogans. The only purpose for which the dot-Frogans was acquired was to secure the name servers and infrastructure on which the technology, which is the Frogans technology, will be rolled out and built.

This Frogans technology is a technology which will allow the publication of a new kind of site, Frogans sites, which will be small sites, something quite distinct from web pages. They will be small, little sites which will have their own addressing system, so that's why we're here. It's a different addressing system, and the other feature is it will require a separate browser called the Frogans player in order to show and navigate these Frogans sites.

I was interested to hear the presentation just earlier about alternative roots, and to clear up that the OP3FT in no sense sees itself as an alternative root, there will be no conflict at any stage with the Domain Name System. The Frogans technology is bootstrapped to the DNS, and it is in some ways like a kind of meta addressing system, a technology which will be above the existing DNS.

I do have some slides – here we go – and I can quickly run through these with you. This first slide is just really to show you where in the Internet ecosystem the OP3FT sees the Frogans technology as the position. On the bottom, you have the infrastructure; in the middle you have ICANN and the DNS. This is obviously a simplified breakdown of the layers of the Internet, and more often you have seven layers. It's been narrowed down to three, and we see ourselves at the top as a new application layer alongside the web and e-mail. It will be up at that level, and it will be bootstrapped, if you like, down to the ICANN level by means of the dot-Frogans gTLD.

Next slide, please. I can go over this quickly. It's just to say that the dot-Frogans will serve for the naming of the databases on which the Frogans technology will depend. It was delegated by ICANN, a community in which we fully intend to play our part.

When you were saying that there is hostility or distrust with some of these new naming systems with the ICANN system, that is really not the case for the OP3FT. We intend to be part of the ongoing discussions of the multistakeholder model of Internet governance as far as ICANN is concerned.

As far as AFNIC is concerned, which is the French registry for the dot-FR, they are the back-end technical registry for the dot-FR, not that they're going to have very much work, because there are only going to be five or six addresses delegated onto the dot-Frogans.

Next slide, please. This is a slide that was given to me by my technical colleagues this morning, so I haven't really had time to prepare any

notes on it. In fact, I won't go into now, because I'll be just inventing as I go along. Next slide.

This slide is just to give you a sense – it's not a very graphic sense yet – of what you will be able to do with Frogans sites. They will be whatever shape you want them to be. They will be simple. That's a very important feature of these sites. They will be ultra-light and ultra-simple to design and develop, and the other thing about them is, for developers, they will only have to develop their site once, and then it will be accessible across all platforms, all device types, and all operating systems without any need for redevelopment. We have developed a special simplified markup language which will allow them to do this. Next slide, please.

This just shows more or less what the Frogans sites will look like. You see that they are absolutely identical, whether you're on a mobile phone, a tablet, or a desktop computer. There will be a little bit of a zooming-in feature, so if you're on a desktop, for example, and want to minimize the size of that screen, you can squeeze it right down to something very small, and the content will adjust accordingly.

Next slide. This is what may be of most interest to you this morning, which is the addressing system. I'm here at this meeting this week with one of my colleagues who has been working on the technical specifications for this addressing system, the Frogans addressing system. It's a Unicode-based addressing system, which means to say that we've got the ten most used languages in the world, which you'll be able to use to address Frogans sites.

Just the structure of the address is somewhat similar to the Domain Name System. If you look at the top Latin one, you've got network name

and then a site name, the network name, and then you've got the same thing, actually, for all the other languages, except in the case of Arabic and Hebrew, where it's the same thing but written from right to left.

If you compare to the Domain Name System, the network name is the same thing as the top-level domain, and the site names are the second-level domains. I suppose one major difference is that we won't have infinitely extendable addresses, so you won't be able to have second-, third-, fourth-level domains. You won't be able to go any further than just the site name.

The technical specification for this is all ready. We've been here this week, discussing with the IDN groups and exchanging with them.

I think I'm pretty much done, so I can just go through the remaining slides. That's a slide in ten seconds just to tell you those are the main principles on which the OP3FT, which is the organization that has put this all together, uses. It's a model that's a bit inspired by the ICANN model, and if we go to the end of the slide, this is something which we have been discussing in other forums. As part of the roll-out of the project, we will be establishing communities around the world to give us feedback on the technology and how to improve it. We've started to establish those communities, and they will be based in universities.

This is just to show you that we have a few players in the Internet ecosystem who have started to get interested in the technology. We have on the left some domain name registrars who have become early adopters of the technology, and they are starting not to sell site names or Frogans addresses yet, but at least to inform their clients that this technology is about to be rolled out.

In the middle you have the dispute resolution centers. Those two dispute resolution centers there are the same as the ICANN-accredited resolution centers, the ADNDRC for Asia and Forum in the United States, and we hope to get more as we go along. I think we're getting pretty much towards the end. Okay, that's just a summary of the technology, we can go over that.

Thank you very much. That's it from me, and if you've got the slides, those are references of the technology.

DAVID SOLOMONOFF: Really fast question. Is there length limit to the site name? Because you mentioned that there's only one level. You don't have second- and third-level.

TOM MACKENZIE: That's right. There is a limit. I can't remember exactly what that limit is, but it's something like 30 characters, or something like that, for the network name, and I think it's the same number for the site name, perhaps less. I'll have to check that, but there is a limit, yes. I can give you that figure. I can look it up.

EVAN LEIBOVITCH: Dave, go ahead.

DAVE PISCITELLO: This is very interesting. I can't help but draw a comparison between this and apps. You have a specific client that actually enables your

participation in the Frogan network. The only thing that the DNS does in this case is get you to that environment, which then has its own naming convention to go through the Frogans world, so to speak. These are not connected to a browser. This software is just going to be software that everyone will have? You'll have one for every operating system for the client ? Is that correct?

TOM MACKENZIE: Yes, that's right.

DAVE PISCITELLO: So that's the distinguishing feature.

TOM MACKENZIE: That's right. It's a self-contained kind of universe which will function on the different devices, so there will be our own browser, this Frogans browser, in order for the Frogans site to be navigated.

EVAN LEIBOVITCH: Thanks. Next up, we have tentatively to speak Ken– sorry? Oh, Olivier, go ahead. Keep in mind our time constraints.

OLIVIER CREPIN-LEBLOND: Okay. I'll be very quick then. You touched on multilingualism, and what I see as an extension, I guess, to IDNs. Are the label generation rules for IDNs going to be carried into the Frogans as well, or are you going to [inaudible]? For variants, for example – are you going to have your own rules for variants?

TOM MACKENZIE: That's a very interesting question which we're thrashing out this week with, in fact, in discussions with the IDN groups. We have been attending all the different panels. In fact, it's my colleague, Benjamin Phister, who's here this week.

We have developed our own rules, actually, for this multilingual addressing system. They're not exactly the same by any means as the rules developed by ICANN, although we have been very inspired by the work carried out here. As a small organization, we don't have the resources that ICANN has to form groups with large numbers of linguists, but we are very interested to take part in those groups, and so far the exchanges have been very positive in both directions, I think.

One of our hopes at the OP3FT is that some of the R&D that we've been doing on the addressing system may be useful. Who knows? In all modesty, we would like to be able to contribute if we can to the ongoing work at ICANN, and would be very happy to share any findings that we have in that area.

EVAN LEIBOVITCH: I have Holly in the queue, but just before that, I don't see Ken Hanson here. Is anyone here either interested or capable of taking his place and talking about the co.com? If not, we'll give more time to talking about Frogans.

Okay, having seen not, I have Holly first, and then Gisella has an online question. Holly, go ahead.

HOLLY RAICHE: I think I share Dave Piscitello's idea that you're almost talking about an app, aren't you, or are you? From your diagram, it looked like you've got your basic infrastructure, then you've got your Internet protocols and so forth. From your diagram, you're sitting on top. Does that –

TOM MACKENZIE: It's a bit like an app. I think it will look very like an app.

HOLLY RAICHE: Why is it, and why is it not? That's what I'm asking.

TOM MACKENZIE: Right, good question. I might have to think about that. I don't know if I'll be able to give you a good enough answer just like that, but it would look very much like an app on mobile devices. What you will have is in the first stage of getting towards Frogans, you will look up the Frogans app. Yes, it will be an app, I guess, on the Apple store or the –

HOLLY RAICHE: [inaudible] carry it?

TOM MACKENZIE: No, of course, but part of the roll-out of the project has been discussions with Apple and Google and all the stores who will carry the browser. On mobile devices, it will look very much like an app. You will

go to Frogans, and once you've got Frogans, you will be able to open it and then access all the different sites within that universe.

On a desktop, you will have to download a special player. Will that look like an app? Yes, I guess it will be a bit like an app. It's a piece of software that you will have to –

HOLLY RAICHE: [inaudible]?

TOM MACKENZIE: Yes.

EVAN LEIBOVITCH: Actually, there's a part of this that's really fascinating, but in a certain sense then, how different is it from the alternate roots that force you to have to get a browser plugin in order to recognize them? It still requires some extra work on behalf of the end-user.

TOM MACKENZIE: From my understanding of the functioning of alternative roots, the problem with them is that they were essentially competing for the same IP resources underneath. The addresses were resolving to the same sort of IP addresses, and creating a potential for conflict with the official ICANN structure. That's why we need one system of ICANN, whereas within the Frogans universe we're not competing. The addresses are resolving down. They're not resolving to an IP number. We're resolving,

in fact, in the first stage of this project, down to a URL. It's in that sense that we're above, if you like.

We're not resolving down to IPs. We want to make it clear that we're not one of those alternative roots that conflicting with ICANN directly.

EVAN LEIBOVITCH: Gisella, we have an online, and then I have Jimmy next in the queue. Gisella, go ahead.

GISELLA GRUBER-WHITE: Thank you. We have a question from John McCormack, host of Stats.com. The question is to Tom. "Is Frogans a solution looking for a problem?"

TOM MACKENZIE: No, I think Frogans is providing a solution to a real opportunity out there, and a need even for a new kind of site. The calculation has been made during the process of developing this project that there are today hundreds of millions of people who are online with a website. In some sense, why create anything different, you might ask?

But what we have calculated or estimated at Frogans is there are a hell of a lot of people who aren't online, and included in those people are small- and medium-sized businesses who may just simply not have the time or the resources. Perhaps they consider that they just don't need to be online.

If you think of a guy who's renting bicycles in a seaside resort, he might just consider that he's doing his business perfectly well, and that actually having a website is something that is too complicated to maintain and too expensive. What the Frogans proposition is going to be to someone like that is, "Look, for six euros" – because that's going to be the cost of getting one of these addresses – "you can very quickly, very simply get your Frogans site out there, and before the end of the day you will have your little thing that looks like an app on mobile phones across Apple phones, the Android systems, on desktop computers, and tablets. It'll be out there."

Our hope is that there is a genuine market out there for this kind of technology. We don't think we're creating a new problem.

EVAN LEIBOVITCH: Okay, next in the queue is Jimmy. Go ahead.

JIMMY SCHULZ: Jimmy Schulz from ALAC. Just to get it right, where is that data stored, [inaudible] content stored when you receive a Frogan site, whatever it is?

TOM MACKENZIE: Yes, right. Tt's hosted under a URL necessarily.

JIMMY SCHULZ: So it's somewhere on some server you are running. Is that correct?

TOM MACKENZIE: Not necessarily. The user could have it somewhere. It could be hosted somewhere else, but it's identified under a URL.

JIMMY SCHULZ: Then I really don't get what's the point here. I could add to that question – I don't see the problem why we need new protocols, new client software, everything new for something that's already there in place. I don't see it, but everyone can do what you want.

TOM MACKENZIE: Hopefully next time we'll be able to come back at a future ICANN meeting. Hopefully in the not-too-distant future I can give you a demonstration. That would be probably helpful to you to see exactly how this system will function.

JOHN LAPRISE: I was in the same boat. You still haven't told us what the problem is that you're trying to solve. You're talking marketing opportunity. We don't care about the marketing opportunity, we care about solving problems, and I just didn't hear that in your statement about what problem you're actually solving clearly. You're talking about meeting opportunities. That's a different thing.

EVAN LEIBOVITCH: If I can expand on that, to use the entrepreneur parlance, what's the pain point you're trying to address, that you're trying to fix?

DAVID SOLOMONOFF: But what pain point does any app in a mobile device actually try to fix? To me, this is no different from Twitter, or from Vine, or from any other play to come up with some other kind of disruptive or different environment for users to correspond and communicate.

Instead of having to launch a browser all the time, I could have this tiny, little footprint, and, yes, I can imagine a lot of different use cases for this, anything from notifications... I could see banks using this for notifications. Today, for example, banks are looking for relief from robo-text calling in cases of breach. Maybe this is a more secure way to do it. I don't know what your model is, but that's one example I could see of this being used right away.

I could see other scenarios where it just becomes another social success, another way to do things, publish things, provide coupons for people. It's just another delivery mechanism.

EVAN LEIBOVITCH: But let me ask both of you then: What is about this that could not have been done in, say, Frogans-dot-something as opposed to having this as a TLD?

DAVID SOLOMONOFF: Are you talking technically? Technically, absolutely nothing, but marketing-wise, why are 2000 people getting TLDs?

TOM MACKENZIE: Right, that's it. Technically, we didn't absolutely need to have the dot-Frogans to address the name servers, the technical infrastructure on

which this technology is being built. However, a decision was taken at the board level at the OP3FT that they wanted to have this TLD because it would send out a signal that we were really in control of the entire system right down, including the addressing of the server infrastructure.

EVAN LEIBOVITCH: Okay, thanks. On that, Tom, you have the last word. We had hoped to have a bit more here on Tor and on co.com, but the people talking about that were not able to come. But I think this has been very instructive on Frogans as an alternative. This is one of the things that we've been doing at these roundtables: trying to introduce alternative ways. I'm sorry if it sounded a little rough, but I guess any time you try and introduce something new, that's going to happen.

TOM MACKENZIE: No, I'm very grateful. Thank you very much for this opportunity.

EVAN LEIBOVITH: Thank you for coming. We are five minutes over time, which by At-Large standards is early. On that note, I leave you to your other meetings or the rest of the week. The NARALO meeting starts immediately two floors up, and thank you very much.

[END OF TRANSCRIPTION]