SINGAPORE - All Things WHOIS
Monday, February 9, 2015 – 14:00 to 15:15
ICANN – Singapore, Singapore

MARGIE MILAM: Next slide, please.

And so where we are in the development. As many of you remember from Los Angeles meeting, we actually conducted a pilot study in conjunction with the NORC research organization out of the University of Chicago where they actually tested a methodology to examine WHOIS records for accuracy using live data. We actually looked at 100,000 records in that sample and produced some results that have been published for public comment. And we're looking for feedback from the community on the pilot and the methodology to help inform the final design of the system.

Essentially the findings reflect some improvements in WHOIS as we looked at different aspects of WHOIS; in particular, looking at registrars that are under the new 2013 RAA obligations, and we saw a difference in accuracy rates depending upon whether they were under the new obligations versus the old ones.

We also kicked off a compliance related pilot to take a look at the findings from the pilot study to see if there were any areas that reflected contractual issues and the compliance department will be following up on some of those activities.

And as I mentioned the next steps are there will be a public comment period that closes in February -- end of February. We'll use that feedback to develop the final system. And the question for today's

panel is really, you know, how far should we go in the development of that system, and whether the system should actually take a look at identity validation checks. And we'll explore that a little more in the next slide.

So the timeline. As I mentioned this has been an ongoing activity, starting with an RFP back in May of last year.

We published the preliminary findings prior to Los Angeles, and the full report is now open for public comment.

When we get the information back from the public comment and synthesize it, we'll roll out the system in phases. Phase one being a look at the syntactical element of a WHOIS record. In other words, is the syntax correct for an address, a telephone number, an email address. And that's expected to be rolled out in mid-2015.

Phase two will be later in the year. That will look at the operational aspects of a WHOIS record; in other words, is an email address operational, does the phone number work, is it a real postal address.

And then as we continue learning from that experience, we'll take a look at whether the system should also incorporate identity validation checks. And that's something that's being discussed right now. There's no decision made on whether that will happen. And we'll go into a little more detail on the complexity associated with doing that.

Next slide, please.

So as I mentioned, the pilot report was conducted with NORC in conjunction with a number of service providers that use their

automated systems, and the pilot looked at WHOIS records from a syntactic and operational point of view.

We did not attempt identity validation checks because of the cost and the complexity. And we have questions for the community to discussion in this session as to whether or not we should try to explore identity validation, whether it's feasible or even acceptable to go to that level.

When we talk about identity validation, we're looking at the recommendations from the SSAC where they examined different types of validation, and essentially it's trying to match a registrant with real-world information and real-world identity of the registrant to see if it matches. And so that involves a layer of complexity that we haven't explored yet.

Next slide, please.

So as I mentioned, we did an RFP to take a look at what was out there. We did receive six responses from organizations that were willing to try to help us do identity validation services. As you can see, they came from different backgrounds. We received research organizations that were interested, a credit bureau, standards body, and they all gave us different perspectives on how you might look at a WHOIS record from an identity perspective.

Next slide, please.

I think when we summarized and took a look at it we found there's really no consistency or standard for doing this. Most of it involves manual processes, and that's part of the problem when we're trying to

build out an accuracy reporting system. If we're trying to look at a significant sample size, there's a lot of cost and time involved in trying to identify whether someone is, you know, who they say they are in a WHOIS record.

There's different approaches that were suggested. Some of them involve third-party database checks, like doing a LexisNexis search checking a postal address database. Some of them involve actually contacting the registrant and seeing if they'll confirm that they are who they say they are. There's a question of whether registrants will even respond to those kind of inquiries, but there's definitely different ways of trying to determine if the person is who they say they are.

We received responses, for example, that someone might want to send a postcard to the person at the address listed in the WHOIS record to see whether or not they acknowledged that that was them, maybe via certified mail or something like that. So there were definitely different approaches that were suggested. They all seemed pretty costly and complex, and so, you know, that's really the discussion for this group, as to what is the feasibility of this and what are the different perspectives on whether this should be attempted.

Next slide, please.

So I have a number of questions for the panel. We'll open it up to any panelist who would like to comment on whether or not identity validation checks should be explored as part of the development of the accuracy reporting system.

Avri.

AVRI DORIA: I have a first question. After I stop sort of giggling at the absurdity of doing identification verification and sort of the whole line of -- The first image I had was of a hundred million people standing in line to have their fingerprints taken and going on from there.

But when you asked the first question, what is required to manufacture around it, I would think some sort of policy that mandated it. We already have a couple of policies, verification processes, that got put into the RAA without the community's approval, and now we sort of -- sort of, well, we've got that. Let's go to this next level.

And actually, my hundred million people standing in line is the mildest of the funny images one can have in terms of identity verification.

So in terms of this first question, what is required, I would assume it would be a policy process where we actually had people say something like that was reasonable, something like that was warranted, something like that was permissible.

Thanks.

MARGIE MILAM : James.

JAMES BLADEL: Hi, James speaking, and well said, Avri. I think when this first was circulated, a lot of registrars, the first question I put out for feedback

was where did this come from, and, you know, this is the first we're hearing about it or seeing it.

But stepping back from that, let's take maybe a more pragmatic look at this. I think there's a concern that WHOIS is not about identities. WHOIS is about managing points of contact.

If we get into and we start to expand upon that and get into the concept that WHOIS is about preserving or managing identities, then I think it takes us down a number of roads that are very concerning and, I think, problematic, the first one being what are we checking against? There are a number of -- well, I would say there are a number of scenarios where we would have to examine the edge cases as to why this could leave a large swath of potential registrants out in the old because they were unable to satisfactorily validate or verify their identity versus -- versus what was contained in WHOIS.

MARGIE MILAM : Chris, you wanted to jump in?

CHRIS DISSPAIN: Yes, thanks, Margie. Speaking entirely as a ccTLD manager for dot AU, it strikes me as being -- this is something which I find -- I must admit, I find that the mere suggestion extraordinary. I don't know what countries there are that require you to validate for your own ccTLD. I know that in Australia, we don't. And I would argue that people who believe that this is important should first tackle their own governments and suggest that each of their own governments introduce the necessary legislation that requires their citizens in their territory to identify -- identity

validate themselves to get hold of a ccTLD in that country before trying to leapfrog and suggest that an organization like ICANN, which is not a lawmaker, should create laws that would, in fact, be quite possibly illegal in some territories where ccTLDs operate.

Thanks.

SUSAN KAWAGUCHI: So in reference to your ccTLD comment, I manage a somewhat large portfolio of domain names for our company, and I have submitted my passport and driver's license in multiple countries to -- which does not apply. It says Susan Kawaguchi. The applicant is really, for domain registration, Facebook, Inc., but they want something to know. I'm not advocating we go there, but that has been and was, early on, fairly universal in a lot of ccTLDs. That's the way it worked. You hand over that critical information or you would not get a registration.

So -- But -- And to take a step back here, if we're going to go through and validate the information in a domain name registration, but there's no bar and there's no way of telling that the person providing that information, that is really their information, then we've -- oh, yes, Facebook, Inc., is at 1601 Willow Road, Menlo Park. Yes, this is a validated information. And Facebook, Inc., is an entity. But I didn't register that domain name. And actually the craziness part of it, I'm probably the only person in the world who would know is that really a Facebook domain registration or not? Oftentimes it will have -- it always has different servers than what servers we use, but we do use a wide variety of servers. And, you know, in most times, the email address is not domain@FB, which is our standard email address.

So you've gone through the whole practice of validating information, but you still cannot contact the person or hold responsible the person or entity that registered that domain name. So do I think it's feasible that we identify each and every registrant? No. But there should be some sort of practice in place that when I attest to the fact that this is not my domain registration, I have not used -- put my information and paid for this domain name, that Facebook, Inc. is not responsible for the domain and that someone should be responsible for the bad behavior. Because they're not doing -- using my information, our information for good purposes, usually.

A couple years ago, I -- I just ran a search on President Obama. You wouldn't believe how many domain names the President of the United States owns from a Chinese registrar with a yahoo.CN email address. Those are the issues we need to address. Do I think we need to hunt down every single person who registers a domain name? No. But we have to have a way and a practice that prevents fraud.

MARGIE MILAM: James, and then we'll open the floor for a few minutes of Q&A before we move to the next topic.

JAMES BLADEL: I wasn't sure how to tee this up, but I think my friend Susan did a really good job, is that -- with raising President Obama, because I was curious as to whether or not he had to show his birth certificate perhaps to get some of those domain names. And for those of you that understand the humor there is there's still a very vocal segment of the population that

believes that the President is not who he says he is. And I guess I'm using that as an example of an -- an extreme example, perhaps, and maybe a funny example that you can never definitively demonstrate that someone is who they say they are with 100% ironclad confidence, particularly if you're doing it on the scale of domain names, 284 million as of fourth quarter of last year, and also on the speed of one per second that we're talking about for registration.

So we have to think in terms of how we can manage those scales, those sizes and those speeds with a reasonable degree of certainty, and also allowing for an acceptable level of false positives. And I think when you put all of that into a pot, that starts to look like a very difficult, if not impossible, lift.

MARGIE MILAM: We have five minutes for Q&A from anyone on the floor. CHARLA has got the mic.

KATHY KLEIMAN: Kathy Kleiman. Thank you for the discussion.

The question is where did the standard come from? The standard appears to be evolving to all accurate all the time, whereas where I think the standard is supposed to be is contactability. That was the standard the WHOIS review team recommended is that the registrant be contactable, and that seems to also be where the 2013 RAA is as well. An email address that is accurate or a telephone number that's accurate. The ability to reach the registrant. So that they can solve problems.

So how did the standard change? Why did it change? How do we go back to contactability?

And just noting that after -- after what's been going on in France, addresses are really dangerous things.

Thank you.

MARGIE MILAM: Do you want to respond?

UNKNOWN SPEAKER: Yeah, and also to the question earlier about where this issue came from, and just it's my understanding it came from the GAC. The GAC advised for WHOIS related safeguards for the new gTLD program that there be a phase three identification verification.

CHRIS DISSPAIN: So just -- Can I -- May I? Thanks.

So just to be clear, my understanding is exactly that; that there was a -- whatever the correct description of GAC -- a lump of GAC advice that included in it a phased -- suggested phased approach for dealing with WHOIS. And I think from memory, the changes that were agreed eventually into the 2013 RAA was like the first phase of that and second phase and third phase.

So I want to be very clearly, certainly, from my perspective that this is an open discussion about a topic. It's abundantly clear to me that's it's policy, massively policy and so nobody should be imagining for a

moment that this is suddenly going to appear and we're going to insist on seeing everybody -- although we are thinking for the next meeting we'll take everybody's DNA as a right to be in a room because we can build up a database that can come in handy.

So I think that's where it is. So I don't think people should get too concerned about it's going to happen, et cetera, but I am very interested in hearing what the room has to say about the thoughts. Thanks.

AVRI DORIA: But can I add one thing? To say that the GAC requested it, the GAC has no --

CHRIS DISSPAIN: Yes.

AVRI DORIA: -- policy-making authority. They can perhaps recommend that a policy process start, but the notion that the GAC requested something and, therefore, it's on a schedule TBD is a process error.

Now, I get accused very often of only being a process junky, but the notion that the GAC can request something in their advice and therefore it's a TBD for something, it's difficult to accept.

UNKNOWN SPEAKER: And going back to Chris's earlier statement about using the ccTLDs as perhaps a pilot program for that, I think there's a natural synergy if this

idea originated from the GAC that they go to their sovereign ccTLD and perhaps lead the way, lead the way by implementing it there and show us how this can be done on a larger scale in the G's.

VOLKER GREIMANN: Volker Greimann speaking, Key-Systems registrar.

Two brief statements and a question. First to Kathy. This is not a standard. This has not been a standard. This is not a standard now. There's no corresponding RAA requirement for entity validation. And to Margie's comment, if the cost is too high, why do you expect -- for ICANN, why do you expect to be more reasonable to perform this for registrars or registries?

Second statement, to Chris's question and to what Susan said, there are countries that require identity verification today. China, Russia come to mind. If you want to align with them, good luck.

In Germany and Italy and many other European countries it's illegal to ask for a personal ID, for a copy of personal ID because that can be abused in a whole number of ways.

And the question, may be rhetorical but I'll ask it anyway, WHOIS data collection and publication has no purpose, no purpose for 99% of the registrations because nobody will ever contact them or try to contact them through the WHOIS data. Does that not mean that the collection is in itself unreasonable from data protection and privacy perspectives?

MARGIE MILAM: So I think we're now moving on to the next topic. We're out of time on this one. I'll introduce Mike Zupke, who is going to introduce the next topic.

MIKE ZUPKE: Great. Thank you, Margie.

Mike Zupke. I'm the director of registrar services for ICANN. And so I think this topic is actually apropo. I think the question now is what exactly does the 2013 RAA require of registrars?

So can we go to that slide, please.

Thank you.

So, in the 2013 registrar accreditation agreement or RAA, there are a number of new requirements for registrars. And among those there is a specification called the WHOIS accuracy program specification.

And that requires registrars to do certain things, some of them easier than others. So, for example, registrars are required to make sure that registrants are populating all required fields. They're required to validate that email addresses are in the proper format so they conform with the applicable RFC. Telephone numbers need to meet with the ITU's notation. Similarly, postal addresses need to fit into the EPU formats for the respective country.

There's an additional requirement that has not been fully implemented yet. And that is that registrars will be required to perform what we call cross field validation of addresses. And what this means is that a house number exists on the respective street; the street exists in the city, the

city in the province, the province in the country. And this is the extent that this is commercially and technically feasible in that country. So we're aware that in some nations this data is not very well commercially available where in others it's pretty commonplace or maybe even free to get this.

So these are some things that that registrars are required to do. And the question is when exactly do they have to do them? And there are certain triggers. So, for example, if a new domain name is registered, a registrar has 15 days to perform this series of validation. If a domain name is transferred in, if a registrant identity is changed or, if one of these particular fields is changed, that field would need to be revalidated.

Additionally, the RAA requires that registrars perform verification of either the telephone number or the email address for the registered name holder and the account holder. And the account holder's information is typically not what's published in WHOIS, but it may something different. It's the person with whom the registrar may have the sort of commercial account, so to speak, or may be the credit cardholder, for example.

In this case the registrar is required to validate the email address or phone number by affirmatively reaching out to the registered name holder or account holder. And they would do that by transmitting a unique code or URL that the registrant would need to click on. And this would allow then for the verification of one of those contact details. And, again, there's a 15-day requirement for registrars to do this. If this

process fails, the registration would either be suspended or the registrar can perform a manual verification of the domain name.

If it's just the account holder data, the registrar is not required to do a suspension if the process fails for verification.

So this is what's currently in the registrar accreditation agreement.

As I mentioned, the cross field requirement is still -- has not been fully operationalized. And that's because this idea of technical and commercial feasibility is something that is subject to further definition. And so there's a registrar working group -- and this is spelled out in the RAA in more detail. But there's a registrar working group which is working with staff to define what it means to be technically and commercially feasible and to determine whether there are indeed solutions out there that would allow registrars to do this in this technically and commercially feasible way. So that work is underway. This is what's required of registrars.

The specification also requires ICANN to perform a review of the specification with the registrar stakeholder group. And what the language in the RAA says is that we should perform this review approximately one year after the first RAA is signed with registrars, which would have happened around the Durban ICANN meeting. But, interestingly, most of these requirements were actually phased in for registrars. So they did not begin implementing these requirements, for the most part, until January of 2014. Sorry. I'm losing track of the year here. So it's been about a year's experience for the registrars. We are initiating the review of this specification. So, although the agreement specifies that ICANN will conduct a review with the registrar stakeholder

group, we, obviously, envision there should be a strong community input component to this. So what we're envisioning is that ICANN staff and the registrar stakeholder group will sort of compile our own wish list based on our experience with the specification and simultaneously announce this review for public comment and allow the community stakeholders who have had experience with the use of these processes or with the specification to provide input. And then, at that time, staff and the stakeholder group will come together, take a look at the complete list of inputs and feedback that was received, sort of come up with a proposed roadmap of addressing those different topics to the extent there are topics that are raised for possible change and then post that roadmap for community comment, too. So not to get too much into the weeds here, but the way this could unfold, depending on, you know, the sort of input we get, is there could be some suggestions that are made that are completely non-contentious. ICANN and the registry stakeholder group are in full agreement. Those wouldn't take a lot of work for us to amend the specification and make those chances. To the extent we think that there are changes that require a more deliberate process, we can go through the full RAA amendment process that has different community input pieces. There's also the potential to defer work to the policy development process. Or there's also the potential that we may just completely disagree with registrars and say we think this is unworkable. So there's different paths that the different inputs may sort of go through in order to get implemented or not.

So that's sort of where we are. We're in the beginning of the process. We've had some informal discussions with the registrar stakeholder groups executive committee.

We're having discussions with the registrar stakeholder group tomorrow. And the public comment process, although we had anticipated kicking that off in January, that's probably going to happen shortly after this ICANN meeting. So that's where we are. And I think I'll stop talking and turn this over to the panel.

And I think, if you want to go to the next slide, we've got some sort of suggested questions. But I have a feeling that possibly James and Brad might have some thoughts already on this that won't require prompting. So I don't know, James or Brad, if you'd like to kick this off.

JAMES BLADEL: Sure. Thanks, Mike. Good overview. And I'll take a look at the questions.

It has been about a year since we've been living under the new 2014 RAA. And some of this came up earlier in a meeting between registrars and some folks from law enforcement. That was a closed meeting. And I didn't like that, so I'm going to tell you what we said.

But, primarily, we identified at least I think, at least from my perspective, two areas where we dropped the ball on the 2013 RAA. The first one is that we did not establish at the outset what an acceptable level of -- what do we want to call it? False positives, false negatives, collateral damage -- of people who were being impacted by these or tripped up by these new requirements that were otherwise innocent registrants. I think that we've seen and we've presented some figures establishing that those are, in fact, non-trivial numbers of folks. You know, if we were able to get something in the 99.9% accuracy

range, that still leaves approximately a million and a half, I believe, gTLDs at risk of being suspended.

And we didn't present any other sanction for failing this validation except for suspension. So it's kind of an all-or-nothing proposition, which is particularly concerning when you consider that this is not just for new registrations but also for incoming transfers or renewals or other sort of material update changes to contact information for domain names and Web sites that may have been functioning perfectly for years or decades are now suddenly being tripped up by these processes.

So I think we need to have a dialogue or discussion within the community of what sort of false positives are we willing to live with. And I think that segues into the conversation we're having on cross field validation and the recognition that, again, on the size, scale, and speed of this industry, there is a significant challenge there.

We can talk to other industries, credit cards or shipping firms or online retailers that, you know, will probably give us their success rates of validating online addresses. And I can feel very confident in telling you that they fall very, very short of 99.9% accuracy. And so, again, what is the threshold that we're willing to accept? What is the sanction that we must impose? Is it suspension? Is it automatic suspension, or is there something short of that would come into play? So I think from a registrar perspective, this has been very disruptive to our industry. It has been very disruptive to our customers. We are looking for ways to either position it to the community that it needs to get better, it needs to be a more -- not such a blunt instrument. And, if we can't make it

work or we're unable to come to terms with what the acceptable level of fallout from these policies are, then maybe we ought to look at rolling them back.

MARGIE MILAM: So I think Brad and then Chris.

BRAD MARDEN: Thank you, James. I totally agree with you that there is a need to distinguish between the treatment for false positives for transfer and renewal as opposed to the false positives for initial registration.

We don't want a big company who's been registering for the last 10 years and who happens to have a change in the IT staff who use their personal email as the registration point to lose their -- everything. That's, obviously, a nonsense.

What we're trying to catch from a law enforcement perspective is those people that either have set up a domain specifically to commit a criminal act, you know, British Airways -- or I should say actually Singapore Airlines ticketing.com has been registered for the express purpose of either phishing or for fraud. Those are the people that we're trying to catch from a law enforcement perspective as they register them. And we need to do that as quickly and as timely as possible.

The other people that we're actually looking at from a law enforcement perspective is those people that have registered and had long-term registration and, almost independent of that registration of their

domain, something else happens. And then that provides an avenue of inquiry for law enforcement in relation to a separate crime.

Those details are generally going to be fairly accurate.

And I think somebody made the point this morning at the other meeting that all those ones -- they're all very accurate. That's true. What we want is timely access to them. But they're generally going to be pretty accurate anyway, because they didn't set them up in the first place to try and avoid law enforcement.

So we just want a basic level of scrutiny there. But what we want is the higher level of scrutiny in relation to those people that register a domain with a specific intent of committing a crime using that domain.

I think that answers one of the questions there why should we review. I think that's it.

We didn't necessarily in the original WHOIS review look at what were we trying to achieve with this? It was very much an idea that we need to be able to find people on the Internet. Well, we do. But we also need to think of why do we need to find them? What is the purpose?

And you said the contact details, James. I think that's actually a really good point.

In law enforcement we call that attribution. So you attribute a criminal act back to a criminal. And that process starts very, very early in a law enforcement investigation.

You start looking at who the people might be. In the real world you talk to witnesses. You look at CCTV. On the Internet one of those sources is

the WHOIS data. It's not necessarily a definitive source. But it's one of those little snippets that we can use to catch the people who are out there doing badness.

And we've got to have some way of being able to track that data back to an individual. Otherwise, you're going to have lawlessness on the Internet. And that will actually impact on the registrars. Because you're having domains registered using false credit card details. So, essentially, somebody registers a domain. It gets turned over a few times. It's used for a spear phishing campaign. It's reversed. You pay the reversal fee on the credit card, and you end up losing money.

If we work together on this, actually, I don't see this as an us versus them. This is working together for a win-win. So we actually have a better Internet for everybody.

MARGIE MILAM: Chris.

CHRIS DISSPAIN: Thanks. I have a question for James.

James, you said you have got data on false positives, right? People whose -- okay. Do you have anything to show that what -- what Brad was just talking about about new registrations. Do you have any data that would show the percentage of domain names that, when you do a check, disappear, don't respond, as new registrations? Because that would give us some indication of how big -- instead of how big the problem is of false positives, how big the problem is of actual problem

in the sense of the names that are being registered. Because one imagines that, if we're talking about the sort of thing that you're talking about, if you do a check the way that you do, these people are not going to be able to respond or not going to respond.

So it would be very interesting to know the number of new registrations you had that have not responded and, therefore, have been taken off automatically by not responding.

JAMES BLADEL: So Chris, I think yes, we could easily get that information. But I want to challenge one assumption, which is that, if someone doesn't respond to a new registration, that they are then -- therefore, they could have been a defensive registration. They had no desire to ever get it resolved so suspension is not a real --

CHRIS DISSPAIN: I accept that. But I'm trying to narrow down the plate, if you like, or make it a smaller plate so we can look at what is actually happening. I accept, of course, that you can't necessarily say that everything that fits on that plate is exactly what I just said. But at least it will give us an idea of size as to what it is we're talking about.

And I think that might be useful in the same way that I also think the false positive are useful.

MARGIE MILAM: Avri, and then we'll open to questions from the floor.

AVRI DORIA: Thank you. Brief comments. One of the things that often concerns me when I'm listening to these discussions is that we get one bit of anecdotal very scary story evidence within a 90%+ things are going well statistical environment. So that begins.

The other thing I get concerned of -- and this is with all due respect to the law enforcement panelist -- is that, when we have just a law enforcement panelist and not a data protection panelist, we only have one side of the law-concerned coin. And one of the bits of lawlessness that I have myself -- that I find myself very nervous, very concerned about is the misuse of personal data, of people's data.

And that's a part of the lawlessness of the Internet that makes it dangerous to people, not the anecdotal cases of one bad actor here or one bad actor there but of the multitude of people whose data rights, whose privacy rights are indeed infringed when we publish all this data on them.

So I think that we have to take both sides of the "what is the law" into account.

BRAD MARDEN: I'd like to respond to that. Actually, I totally agree with you. The last thing that we want in law enforcement is more crime being generated by the publication of large amounts of personal data.

Personally, I'm still not sure why a lot of that information needs to be published. I know in the original discussions there was talk about

having two levels of data -- the basic contact details for members of the public to be able to contact the web or the domain owner and then another deeper layer. So I'm not entirely sure how that happened.

MARGIE MILAM: I'm sorry. We have to open the floor on the next topic because we've run out of time. Is that all right, Chris?

CHRIS DISSPAIN: I have a question. But, I happily defer to the floor, yes.

DAVID CAKE: David Cake, Electronic Frontiers, Australia.

The -- My question is, Brad, you mentioned -- It may have been you were sort of speaking off the cuff and you didn't mean it but you talked about basically wanting to track -- deal with criminal use of the Internet when they register. And I've just got to say, you can't. That's impossible. When they've registered, we don't even know what they're going to use the domain name for. I mean, ideally, yes, could you catch actual criminal acts committed in the process of registration, but that pretty much comes down to fraudulent credit card data and no one -- I'm sure all the registrars would say they'd love to crack down on fraudulent registration.

So it seems to be that -- I mean, there is an issue here where you're trying to -- the only possible way is to raise the bar on, you know, everyone on the Internet in order to, then, if they do prove out to be criminal, to have more information.

It seems that we do have a -- you know, this lacks proportionality at a sort of first guess, in order to respond to the small number of people who may be potentially committing a crime. We have no way of knowing yet. We need to put processes in for the entire registrant -- for all registrants.

BRAD MARDEN: I think I know what you're talking about.

No, what I'm talking about there is, essentially, you need that first step verification of someone registering. So if you register, as I said, SingaporeAirlinesTicketing.com, there's got to be some way of checking that there's, prima facie, some accuracy to that registration, that there's an email, there's a phone number. That's what we're talking about in the thing. That you can actually go back. It's not just whimsical. I'm not talking about getting their full data out and doing identity checks, anything like that. I'm saying really contact details are valid.

DAVID CAKE: Reachability, is what you're talking about.

BRAD MARDEN: Yes.

DAVID CAKE: Reachability is a very different standard.

BRAD MARDEN: That's what I'm talking about. Sorry.

DAVID CAKE: That's understood

PAM LITTLE: Hi. Pam Little, for the record.

I have seen some data points on the impact of 2013 RAA versus 2009 RAA, but I have not seen any data on the impact of the verification requirements.

I think that is the question or the data that we need to see, because whether a WHOIS complaint relating to a -- is sponsored by 2013 RAA registrar or 2009 RAA registrar to me is not relevant. It's the registration, whether that registration is subject to the verification requirement.

So my question is does ICANN or the accuracy pilot study or ICANN compliance have any data to show the impact of the verification requirement?

Thank you.

MARGIE MILAM: So I think we've got Kiran and then Volker. We have to close the queue and move on to the next topic. Sorry. And Rob. Where's Rob?

UNKNOWN SPEAKER: Impact on accuracy was what she said.

UNKNOWN SPEAKER: (Off mic.)

UNKNOWN SPEAKER: Sure, and the point of the accuracy reporting system is to try to report at different levels. We're going to have different kinds of reports that try to drill down in that. So that's what we're trying to build out.

KIRAN MALANCHARUVIL: Hi, Kiran Malancharuvil from MarkMonitor.

I have a couple of points. I'll keep them brief.

With all due respect to James, he made a comment that was sort of definitive, and I'd like to kind of take issue with it. He said from a registrar perspective, this is very disruptive and it's been problematic.

I don't actually think that's an accurate statement across the board with registrars. MarkMonitor does have a unique business model insofar as we are a corporate registrar and brand protection registrar. I'm the policy counselor at MarkMonitor, and I primarily represent the rights of IP interests, but Matt Serlin spoke about this earlier in the closed session.

We have not considered these requirements unduly burdensome, and we haven't seen any compelling evidence that it would be even in a broader context. And I think there are a number of commercial registrars that we have spoken to publicly and privately that this also don't feel that these are unduly burdensome requirements.

So I think before the registrar community is lumped kind of together on this, we need to have, perhaps, a discussion and maybe a survey even to go beyond just the registrars that are represented here at ICANN to actually see what the impact is across the Board from registrars before we make definitive statements like this.

I think my second point is about, you know, why do we do these -- these things? Is it to prevent criminal activity? I've said this before and I will say it again, it is very, very difficult if not impossible to see and to prove that an action has prevented a crime or an action has prevented any sort of activity that we're trying to prohibit here. However, we have seen that these kinds of exercises, so to speak, have gone towards fostering contactability and to creating a transparent environment in domain names. And we've spoken about this at length in the privacy proxy services accreditation issue working group, about that there is, in a number of countries, in a number of jurisdictions, laws that require contactability and require transparency when, for example, you're doing business online, when you're engaging in commercial activity with your domain name.

And I think that that's what these requirements are aiming to create; a transparent and contactable environment in which we can foster dialogues with domain name registrants when we have issues from an IP perspective or otherwise.

And there are plenty of opportunities -- for example, the use of -- responsible and restricted use of privacy proxy services, in order to prevent the misuse of contact details.

So I think that -- Those are my points. I think that this is a very useful dialogue. I think it needs to be more widely disseminated in the community, and happy for these opportunities to discuss.

Thank you.

MARGIE MILAM: So Rob, Volker, and then we'll move on to the next topic.

JAMES BLADEL: Sorry, Margie. Can I respond real quickly? I just want to apologize to Kiran because I did say "registrars," and I probably should be more careful, indicating explicitly MarkMonitor is a unique animal and that doesn't always feel -- I would say, probably, an overwhelming majority of registrars feel this has been an undue burden on their customers. And any other registrars who also believe that this has not been an issue, I would gladly exclude them as well. I do remember there were two speakers from the registrars at the session that said this was not a problem. Both were from MarkMonitor.

Thank you.

ROB HALL: Rob Hall from Momentous. I want to comment on something the law enforcement gentleman said. So I think you've kind of started down the right path here, sir, and I want to commend you for it.

You said that the problem wasn't really with these ten-year renewals where a corporate I.T. guy leaves, and I think if we look at the volume of

what we're seeing, that's certainly mostly what we're dealing with, is an address goes wrong in a long-term registration. You then said something that scared the crap out of me, which was you said you really want us to verify new registrations where the intent of the person was to become a criminal. And we were talking about validating identity earlier, and now you somehow want us to validate the intent of the person.

We're down a path here where there's no possible way this is ever going to get done. And I think we've got to say wait a minute, we're in a review period now. Let's concentrate on what the review is about, which is can we segregate somehow, as you suggested, and I think it was a good one, new, perhaps, from old existing, and is there perhaps a standard of, other than cutting off all communication 15 days in, where that often is the domain we're trying to communicate with them at, can we have a tiered standard that maybe would affect less people in the sudden death way of, hey, your domain's gone.

So I commend you, sir, for saying at first, you know, perhaps we should review some of this. I think that's exactly what the review intent is, and I would encourage the community to partake in it.

BRAD MARDEN: I'd like to answer that. Yeah, I totally agree with you. It's not your job to prove intent. It's actually my job. That's what I do for a living.

What I require is accurate information to attribute that back to a person so that I can then prove that intent. I can't go down that path of proving the intent of the registration, what they were doing, without

that accurate information. I don't expect the registrars to prove intent. That's my job. But I want you guys to have accurate information through your processes so that I can then actually get ahold of the one person who did do it and talk to them in person and have that discussion about how it came about.

Obviously at the time they do it, they will have that intent, but we need to actually be able to find it later.

Sorry, that was....

VOLKER GREIMANN: Yes, Volker Greimann speaking, speaking for 99% of the registrars who are not also member of the BUC and APC.

One point that struck me is the comment that what are we trying to achieve. We're trying to achieve less crime on the Internet. That was the proposition we were going into in the RAA negotiations, which, by the way, originally called for the deletion of a domain name if the validation was unsuccessful. The registrars were successful in downgrading this to suspension or deletion, and most of the registrars only suspend and do not delete because that makes absolutely no sense.

Now, in the -- in the meeting that we had prior to this one with the LAAs, the LAAs were unable to give even one example of where the added requirements of the RAA have helped them in actual fact in any investigation. We've asked for this. We've asked the Board, we've asked staff, we've asked the LAAs, and they say we don't have any statistics on that. Now we're asking you not for statistics. We're asking

for examples, concrete examples. And if we find out that, in the end, as a community, that all this crap that we have to deal with, all this hassle that our customers have to deal with, losing domain names, having domain names deactivated, does not serve an actual purpose, an actual need, does not -- or is not fit for that need, then we must consider rolling those back.

And to the statement of countries having laws identifying the business, doing business on the Internet, there are laws out there that state you have to write on your Web site who you are and how you're reachable, and that makes sense because the Web site is where you're doing business. The domain name is just how to reach that Web site.

In Germany, you must publish who you are on your Web site when you put out a Web site, even if it's only a blog. You have to identify yourself. As a business, the requirements are even harder for that. And that's the case for most of the European Union. And that makes sense. That's the place where the identification has to happen. And if a customer from the European Union finds a Web site that does not put their information on the Web site, then they're right to be suspicious. But nobody looks at the WHOIS for that.

So what I'm asking the countries, the GAC members and law enforcement agencies, lobby to your countries, lobby to your governments to implement such laws that make sense, that you have to put your information on the Web site, and you will not have this problem and you will have a much better result.

MARGIE MILAM: Thank you. And thank you for an interesting discussion.

We're now going to move to the final topic for this panel. And Susan Kawaguchi will talk to you about the status of the Expert Working Group and the next generation, a system that's been proposed.

SUSAN KAWAGUCHI: This has been interesting today.

Do we have the clicker?

So, as you probably all know, November 2012, in a Board resolution concerning the WHOIS Review Team's recommendations, the Board initiated a PDP to look at -- take a hard look at the -- at what could be done with a new system to replace WHOIS. And so you can see there are the members -- well, actually. So the EWG was formed and we provided a report last -- at the London meeting and gave some time for the Board to think about it. And then at the L.A. meeting this fall, a Board-GNSO Councillor group was put together to really think -- look at the recommendations and also looked -- take a hard look to see how this could move forward to a PDP, if that's the decision, to move forward. So it was balanced between GNSO Councillors and board members.

And next slide.

We took a lot of time and a lot of discussion to really try to look at this. Currently, this is where we are in the PDP process. It's the very beginning. You know, the next step would be the publication of a preliminary issue report. And since the EWG report was never provided

to the community and allowing them to comment -- the report was provided to them but no comment period was established, the EWG report would be part of the preliminary issue report, and comment from the community would be allowed.

So we're just at the beginning of this stage. So let's go to the next step -- next slide. So right now in the blue section, that's where we are today. We've thought about the guidance for the PDP, and we are hoping we can find -- in the yellow dates, we're hoping we can follow this timeline to deliver this to the community and maybe get moving with the PDP.

Next slide.

So this is a difficult -- a very complex issue, obviously, you can -- from the discussion we've all had today. There's a lot of agreement; more disagreement, probably; a lot of issues to flesh out. And so we broke up the EWG's final report into sort of three areas, and we are recommending a three-phased approach, but it would be a single PDP. A little more complicated than most PDPs, but there would be phase one where the policy requirements' definitions were created and agreed upon, so that's sort of the why. Why are we doing this and all of the decisions that needs to be made in the first phase by the community would be, you know, discussed and decided upon.

The second would be the actual policy functional design, the what of the new process, the new registration system. And then phase three would be implementation.

And what we're recommending is that we follow this three phase -- phase one would definitely be -- we'd do phase one, talk about it, figure it all out, go back to the GNSO Council and say are we on the right track? Is the community where we should be? Have we made the right decisions? Do we want to move forward?

And then phase two and three really could be sort of -- you may be able to move a little bit into phase three while still working on phase two, and we'll get into a chart in a little bit that shows a little bit about that.

But there's some steps that need to be taken before all of that work begins. And that's one thing we spent a lot of time discussing. What do we need to know?

The WHOIS review team, which I always sat on, always struggled with what are the laws and how are they changing? So probably an initial legal analysis of sorts.

A risk and benefits analysis. Would a new system truly be better than the old system? What are the risks we're looking at?

Now, I'm sure you can all understand how, as we go down the road with a PDP, we may need to refresh some of that information. There will be new questions, new laws in different lands. The EU is developing all the time. There's a lot of different changes in the world. And so, you know, maybe we continually do additional legal analysis and the risk and benefit assessment at certain stages. That would be up to the GNSO, in my opinion.

And so -- and we're also -- there's some work in the community right now that's -- most of it is about ready to be finished. But, for example,

the PPSI working group proxy and privacy. So what is that report going to say? And how can that inform this PDP?

So there's some work that needs to be done prior. But we do think there's a way for this to move forward and to work well within the community.

So, if you go to the next slide.

So this chart is a little bit complicated.

And it took a lot of work on our part and mostly staff to really put this together in a very cohesive manner.

And so you'll see on the first -- the preliminary steps, the issue report and input development: These are the categories we -- the EWG sort of worked on things. And, you know, are there -- what are the uses and purposes? Who are the users and why do they need the information? And so all of those different categories. And then we added the benefit analysis and the risk assessment, too. Because those are key areas. We all need to look at this.

And so phase 1 would -- we would develop those policy requirements in phase 1.

And until phase 1 was completed and then some sort of double-check with the GNSO -- and do we know what that looks like? No. This hasn't been done before. This is the first board-initiated PDP. We don't have a lot of guidance from the history of the community to work on this.

So we're -- so we all need to work together to figure that out.

But what we are recommending is that the policy requirements be developed. And then we go back to the GNSO. Whether that's a comment period or how that -- the mechanism is to review that, I can't give you that.

But it would be a check at that point.

And then, assuming that we would then decide as a community to move forward into the phase 2 and 3 then we work on those. And what are the purposes? And just go through all the different categories.

So this might be -- you know, we might be able to jump ahead on some of these things. After we finished one, go to the next one into phase 3. But we would work on that probably in subteams. We sort of imagined that we could break this -- this is a large PDP, but we could break it up into subteams and then have maybe some sort of a collaboration team that's an oversight to make sure that we found all the purposes and it works well with the privacy design, for example.

So let's go to the next slide.

So that's, basically, what I've talked about on this slide. There is some parallel progress that could be made. And there's been some thought about having some periodic face-to-face meetings and maybe add those on to an ICANN meeting. And -- which we all need longer meetings, but --

So, you know, in a time when we have a lot of work to do with IANA transition, this would be asking a lot of the community. But I think you can see from the discussion today it's important.

So next slide.

So we do welcome all of the input. The preliminary issue report should be out soon. Sometime in March.

And then you'll have the opportunity to comment at that time.

That's it.

MARGIE MILAM: So now we'll take some comments from the panel and then from the floor. Avri?

AVRI DORIA: Thank you. Yeah. I just wanted to comment on a few things before we got to the comments. One is that it's important to realize that we're taking this body of work, the EWG, and, basically, treating it as one among many input materials to this process.

Part of what we're trying to do with this process -- and we've done it with this process working group -- is open that work up to transparency. A lot of that work was done without the benefit of transparency. So, going forward, both in this process group and such, we wanted to work it out. Now, there's a real awareness of the complexity of this and the project management that we'll take and how to get all these things related.

And some comments that have already come up with people sort of relate is how do you deal with the parallel nature of some of these threads? And how do you make, you know, certain things get done

before others? So there's going to be much more complexity. And that interdependence is something that I'm hoping comes out not only in the comment period. But, when the GNSO, basically, has to stop and look at how to actually -- the charter will be presented in draft. But the GNSO then at some point is going to have to actually decide how do we take a charter and actually make this thing work? Because the complexity is beyond any I think we've tackled as a working group to date. So we're going to have to learn a lot.

But the most important thing I want to get back to is that this is going to take all of that discussion, use it as input material, but deal with it in a transparent manner which we didn't have with the EWG as it was going on. It wasn't in the nature of, perhaps, a special expert panel to have it. But since then ATRT has, basically, said we don't do anything nontransparently. Transparency is our default way of practice. So that is an intent here. Thanks.

MARGIE MILAM: Anyone else on the panel want to comment? James?

JAMES BLADEL: Yeah. Just to -- and thanks for the overview, Susan. Just to reiterate one of the comments I made over the weekend sessions.

This is a huge piece of work, undertaking that we're looking at with this. It could realistically last -- I mean, this is ICANN. It could go on for four or five years. It could -- and then we could be looking at perhaps a decade of this system operating in parallel, you know, with the legacy system.

So I have a question. And I don't know the answer. I'm just saying there's a question of what -- what is -- I'm concerned. Because at ICANN sometimes we get into this mentality of sunk costs, which is we have to proceed with this because the EWG did so much work. And the EWG had to proceed because the WHOIS review team did so much work. And phase 2 has to proceed because phase 1 was so much work.

At some point I want to be sure that we go into this eyes wide open of what it's going to take, what it's going to cost, both the development, the testing, the pilot programs, and the ongoing maintenance and then what the benefits on the other side are going to be. And I think we have to do a very good job at the outset of measuring that in advance to the best of our ability. Thanks.

MARGIE MILAM: Chris, you want to respond?

CHRIS DISSPAIN: James -- thank you, Margie. James, I think that's an extremely good point. I think I can say that the board has no appetite to do stuff for the sake of it just because we've spent some money on it. And, certainly, there is no intention to, you know, just -- that just wouldn't make any sense to us.

We recognize -- the board understands how big this is. It shouldn't necessarily surprise folks that we take on a task that might take five years.

I'm reminded of the ccTLDs have been working on their framework of interpretation stuff in respect to RFC1591 for about six years now. That in itself is not a problem. It's just a fact of life.

But, certainly, any thoughts that we would look at it and go, well, having spent much money, we'll do this, just doesn't happen and doesn't make sense. But thanks for raising it . It's a very valid point.

JAMES BLADEL: Just to be clear, I don't want to sound like I'm not saying we shouldn't do it because it's scary. We need to go into this eyes wide open and understand that at the outset. Thanks.

MARGIE MILAM: We just have two minutes left, so we'll open it up to the floor. Looks like Steve Metalitz and Volker have their hands up.

STEVE METALITZ: Thank you. Steve Metalitz from the intellectual property constituency. We've talked about a great many projects here. And I haven't heard anything about the identifier registration data access update system.

This is in the draft operating plan for the next five years. This system is going to be developed, approved, prototyped, revised, beta tested, and put into production over the next five years.

How does that relate to all of the WHOIS work that we've just been talking about?

MARGIE MILAM: I believe that's an IANA project. Steve, we can investigate that and send a response. But my understanding that it's related to IANA WHOIS issues. Okay.

Thank you, Steve.

VOLKER GREIMANN: Volker Greimann speaking, registrar constituency.

Just one question. In the first phase there was the question of why. That was missing something, in my view. We shouldn't just ask ourselves when we go through phase 1 why we should do this but also consider why we may not want to do this.

For example, James stole some of my thunder there, the cost implications of this. Will this be financeable? Who will pay for this? Who can pay for this? Will this be a trademark clearinghouse thing where the requesters pay? Or will every registrar had have to chip in a dollar or something?

The second question, when Susan said this can be done in parallel, by whom? The GNSO has its limit already. Certain constituencies do not have more people to dedicate to more working groups. When you say in parallel, then there must be people to do that equitably from all the constituency and stakeholder groups. When there's no one to do the job, nothing can be done in parallel. So we must consider our capacity as well.

And that's about what I wanted to raise here.

MARGIE MILAM: Does anyone want to respond on the panel?

SUSAN KAWAGUCHI: I think that the risk and benefits assessments would, you know, ask the question is this worth moving forward with? Also, you know, when the board decides to deliver this to the GNSO, I think that's another opportunity to say is this something as a community we're going to move forward with?

I don't think right now that's -- you know, the obvious -- I would hope that we would move forward. I also do not -- you know, but that's not -- I don't think that's agreed upon at all. I think that's something the community has to decide.

I also think, if this is truly not delivered to the GNSO until next fall, some of that -- the resources may be freed up if IANA is sort of settled somewhat.

We always have a lot of work. But it's important work we have to do forward.

So good questions.

MARGIE MILAM: I'd like to thank all the panelists for an interesting discussion. Thank you very much for attending this session.

[Applause]

[END OF TRANSCRIPTION]