SINGAPORE – 2013 RAA FAQs
Wednesday, March 26th 2014 – 13:30 to 15:00
ICANN – Singapore, Singapore

UNIDENTIFIED MALE: Wednesday, March 25, 2014. The session is the 2013 RAA FAQ session located in the Canning ballroom. The local time is 1:30 PM.

MIKE ZUPKE: Good afternoon. We're just going to confirm with our techs that we're ready to go, and then we're going to get started. Okay, we're getting the "Yes, we're ready." Are we recording? Excellent. Thank you.

So, good afternoon, again. I'm Mike Zupke of ICANN staff. I'm the director of registrar programs, and I have with me here, sitting next to me is Caitlin Tubergen, also on the registrar liaison team, and sitting next to her, Owen Smigelski of the Contractual Compliance team at ICANN. We're here today to present to you registrar accreditation agreement frequently asked questions, in particular related to the 2013 RAA.

The purpose of this session is really to try to help registrars to understand the obligations that are in the RAA because we know that this is still new to many and there is still a lot of learning that both registrars and ICANN are doing as this contract is rolled out. I just wanted to give a real quick background on some of how we got here and then what we're planning to do today.

The 2013 RAA was approved by the ICANN board in June 2013, and then we've had registrars coming on board ever since then. I think we're somewhere in the neighborhood of around 33% of registrars are currently on this new form of RAA. That represents something like 83% of the generic domain name space. There's been pretty good up-take in terms of adoption of the new accreditation agreement.

As part of our rolling out the new RAA, both registrars and members of the community said to ICANN, "We think there needs to be a really strong, proactive outreach initiative so that those who are under these new obligations will actually understand them.

So last year, ICANN staff and a handful of registrar volunteers, we created a bit of a roadshow. We started in Los Angeles, and we did a two-day session that was webcast for registrars on all of what we that were the most complicated aspects of the new agreement. We did this again in Jiangmen, China, and then again in Berlin. And then, finally, we did one in Buenos Aires.

[audio break]

Queue called RAA questions at ICANN.org, which is really intended for registrars to be able to ask questions about the new agreement. So what happens, generally, is the registrar questions that come to that address are primarily fielded by Caitlin and Owen. When there are questions where we don't know the answer, we'll occasionally bring in the legal team to give us some guidance. We do our best to try to be responsive to these questions from registrars. We're aware that there's occasionally areas where it's not perfectly clear.

Today, we've taken some of the most frequently asked questions through that ticketing queue and through some of the webinars that we've done, and we'll try and present those to you. We'll give a brief presentation on that, and then we'll open up the floor to questions and answers.

With just one further little bit of housekeeping, we've got remote participation, so people who are not in the room but have questions, feel free to ask them online. I think the schedule reflects that this is a 90-minute session, but we've actually planned for a 60-minute session, so just please be aware that we'll end not at the top of the hour, but half past the hour. So without further ado, I would like to hand it over to my colleague, Caitlin.

CAITLIN TUBERGEN: Thank you, Mike, and good afternoon, everyone, good morning and good evening to our remote participants. My name is Caitlin Tubergen, and I am the Registrar Relations and Contracts Manager here at ICANN.

I wanted to begin with an agenda of some of the topics we'll be covering in today's session. We'll start with a couple of 2013 RAA statistics, followed by how to request the 2013 RAA and the process time associated with that. Next, we'll talk about some of the new website hosting requirements, followed by the Whois Accuracy Program Specification and then the Registrar Data Directory Services Specification, also known as the Whois Specification.

We'll then talk a little bit about dealings with resellers under the 2013 RAA, and then also the expedited transfer of accreditation mechanism

to wholly-owned subsidiaries. And then lastly, I will be handing it over to Owen Smigelski from our compliance department, and he will talk about some of the common compliance issues associated with the 2013 RAA.

The following slide has some of graphics on it that represent the amount of registrars that have adopted the 2013 RAA. As you can see on your left, approximately 33% of registrars have adopted the 2013 RAA and also, as of last week, there are no longer any registrars under the 2001 RAA. These statistics are as of last Friday, by the way. As you can see on the right, approximately 83% of domain names under management are now under the 2013 RAA. That's a good statistic.

One of the most frequently asked questions we get is how to adopt the 2013 RAA early. If you visit our website where the 2013 agreement is, there is a form, an early adoption form, which you can complete and submit to ICANN pursuant to the instructions on the form. When ICANN receives the form, we'll acknowledge receipt and proceed to run a preliminary compliance check on the registrar. The registrar should allow for between 7 and 14 days for that compliance check.

Assuming everything checks out, ICANN will send the Registrar Information Specification to the registrar, which is a document in the agreement that essentially has some questions that the registrar needs to fill out and provide to ICANN. Many of the data elements are similar to what the registrar would provide when it initially applied for accreditation.

Then ICANN will send the 2013 agreement to the registrar via DocuSign, which is an online signing tool. If the registrar instead would prefer a hard copy of the agreement, there are instructions on how to request that when you receive the agreement.

Now, I'll talk a little bit about requirements for registrars websites. Section 3.7.10 of the RAA requires that registrars provide a link to the Benefits and Responsibilities Specification. A link has been provided on this slide. Also, section 3.16 of the 2013 RAA requires registrars to provide a link to registrant educational information and, similarly, a link has been provided on this slide.

Just a couple of notes about those links: the links should be either on the registrar's homepage or one or two clicks away from the registrar's homepage. This shouldn't be something that someone trying to find this information has to click 14 links to receive.

This slide represents some of the elements of the Registrar Information Specification that need to be posted to registrar's websites. When you look at the Registrar Information Specification, there are a couple of elements that are marked with an asterisk. Those need to be published on the registrar's homepage. I've included those up on the slide.

I just wanted to make a note about item 17, which is the full name, contact information, and position of all officers of the registrar. What needs to be posted on the website is the full name and position of the officers. The contact information does not need to be on the registrar's homepage.

Lastly, section 3.18 of the agreement talks about abuse contact postings. Section 3.18.1 provides that registrars need to publish an e-mail address to receive abuse reports. I wanted to make note about that: that does need to be an actual e-mail address. A Contact Us form is not compliant with the agreement.

Section 3.18.3 provides that registrars need to provide a description of the registrar's procedures for the handling, tracking, and receipt of abuse reports.

Next, we'll just talk a little bit about Whois Accuracy and the Registrar Data Directory Services Specification. The Whois Accuracy Specification is required for all gTLDs, as of the first of January of this year. I wanted to emphasis that is for all gTLDs. I've gotten a couple of questions about some registrars thinking that it's different between legacy gTLDs and new gTLDs, but it is required as of the first of January for all gTLDs.

The Whois Accuracy Specification requires the validation and verification of registrant and account holder data, in certain circumstances. In the following slides, I'll describe a little bit about the differences between verification and validation.

Also, the deletion or suspension of domain name registrations is now explicitly required in certain cases that are mentioned in the agreement. So section 3.7.7.2 requires deletion or suspension of domain name registrations for the willful provision of inaccurate or unreliable data.

Section 3.7.7.2 also provides for the deletion or suspension of domain name registrations for the willful failure to update data promptly, and the agreement defines promptly as seven days.

The Whois Accuracy Spec requires the deletion or suspension of names if the registered name holder doesn't respond to a Whois Accuracy request.

So Whois validation: the Whois validation is required for registrant and account holder data within 15 days of the registration, transfer in, or the registrant or account holder data change.

For Whois validation, the registrar is just checking that all the required fields are filled and they're filled according to certain standards. Those standards are specified on the slide. I won't bore you and read through all of them.

I did want to make a note that the cross-field validation requirement in the Whois Accuracy Specification is not required yet, and that's something mentioned in the Transition Addendum. That won't be required until the working group and ICANN reach mutual agreement on a technically feasible way to perform cross-field validation.

Whois verification is required, similarly, within 15 days of the registration, transfer in, or registered account holder data change. The registrar needs to verify that the e-mail address or telephone number is accurate, and that's found in section 1F of the Whois accuracy specification.

And the Whois verification, as opposed to Whois validation, requires an affirmative response from the registered name holder. So the registered name holder does have to verify that “yes, this is my phone number” or “yes, this is my e-mail address.”

Exceptions to the Whois Accuracy Specification: the verification and validation are not required if the registrar has already previously performed the verification and validation on identical data and the registrar has no reason to believe the data has become inaccurate or invalid.

An example of a reason to believe that the information has become inaccurate or invalid would be an e-mail bounce back would suggest that the e-mail is no longer valid.

Now, I'm just going to go through a couple of Whois Accuracy examples, and I know that Owen will be going through a couple more later in the presentation.

If a registered name holder updates its postal address, the registrar must validate that the postal address is in the proper format, and the proper format is defined in section 1(d) of the Whois Accuracy Specification. However, the registrar would not be required to re-verify the e-mail address or the telephone number of the registered name holder.

If the registered name holder updates its e-mail address, the registrar has to validate that the e-mail address is in the proper format, and the proper format can be found in 1(d) of the Whois Accuracy Specification.

The registrar would also have to verify that e-mail address if the registrar had chosen to verify the e-mail address further, to section 1(f)(i) of the agreement. If, instead, the registrar chose to verify the telephone number, the registrar would not have to verify the e-mail

address, unless it has a reason to believe that that data is no longer accurate.

If the registered name holder updates its telephone number, the registrar must validate that the telephone number is in the proper format. That can be found in section 1(c) of the Whois Accuracy program specification. The registrar would also have to verify the telephone number if the registrar had verified the telephone number further to section 1(f)(ii). If the registrar had instead chose to verify the e-mail address, the registrar would not have to verify the telephone number.

Now, we'll go through some of the new requirements of the Registrar Data Directory Services Specification. All of the requirements for Whois can be found in the Registrar Data Directory Services Specification, also known as the Whois Specification. There are additional fields required now in the registrar's Whois output. There's a uniform Whois query and output format, and the Whois output format should be in the exact order that is specified in the RDDS Specification.

EPP status values are exclusively required now for domain name statuses. There's now a SLA for Whois service, and that can be found in section 2.2 of the specification. IPv6 accessibility is now required. And Port 43 access is only required now for thin registries; however, web-based Whois access is required for all registries.

This slide shows all of the new Whois fields that are required as of January 1. Again, I won't go through and read them all, but on the next

slide I'll make a couple of points about some of the fields that registrars have asked questions about.

For the registry domain ID, this is a field that doesn't change for the length of the entire domain name registration. For the field for the registrar abuse contact e-mail and phone, those fields do have to have an actual e-mail address and an actual phone number, but it's up to the registrar's discretion who they would like to use for that.

Domain name statuses are exclusively EPP status codes. And the registry registrant ID, the registry admin ID, and the registry tech ID may be left blank if they're unavailable from the registry. And lastly, I did get a lot of questions about the DNSSEC field, and there are two options for the output on that field and I've displayed those below, signedDelegation and unsigned.

Section 3.12 of the 2013 RAA has certain requirements that the registrars must ensure that their resellers are doing, for example, displaying certain links on their website. A common question is, "How can we ensure that our resellers are doing something?"

Up on the slide is a non-exhaustive list of how registrars can ensure that their resellers are, indeed, doing something. For example, when it comes to website links, the registrar can implement some kind of monitoring process whereby the registrar periodically looks at the resellers websites to ensure that those links are there. Also, the registrar can include in their reseller agreement consequences for contract non-compliance when the reseller is, indeed, not doing something and is causing the registrar to be in breach of the agreement.

The Compliance Certificate is a requirement in section 3.15 of the RAA, and for registrars that had signed on to the RAA in 2013, all of you should have received a Compliance Certificate via the DocuSign to sign. For registrars that signed the agreement this year, in 2014, the Compliance Certificate will be issued early in 2015 to sign.

Another commonly asked question is regarding section 7.3.1 of the RAA, and that is the transfer of accreditation to the registrar's wholly-owned subsidiary.

Up on the slide, I've included the required documentation if the registrar would, indeed, like to transfer their accreditation to a wholly-owned subsidiary. In the event that the registrar would like to do that, it needs to provide documentation proving that the transferee entity, or the wholly-owned subsidiary, is in fact a wholly owned subsidiary of the registrar. And that can perhaps be a stock certificate or articles of incorporation or some sort of legal document evidencing that fact.

Also, the ICANN-accredited registrar would need to provide a letter on its company letterhead acknowledging it would like to transfer its accreditation to its wholly-owned subsidiary, and the wholly-owned subsidiary would need to provide a letter on its company letterhead acknowledging that it assumes and will be responsible for the existing registrar's obligations and liabilities. And also, the registrar can submit a primary contact update, if it's applicable.

Now, I will be handing the presentation over to Owen, and he's going to talk about some common compliance issues that the Compliance department has seen.

OWEN SMIGELSKI: Thank you, Caitlin. Next slide, please.

What I'm going to over here is what Compliance has seen since the 2013 RAA has gone into force, and most of the concerns we have seen have been regarding those things that went into effect on January 1, 2014. because the transition addendum no longer applies to those, these are things that are effective when the registrar executes the agreement.

The first area we've seen some issues with have been Whois inaccuracy complaints with regards to verification and validation. As Caitlin mentioned, registrars do need to verify or re-verify e-mail addresses of registered name holders, and that's even if the Whois inaccuracy complaint is even about, say, the postal address.

Another issue that we've been seeing with the registrars is that the registrars are required to suspend a domain name after 15 calendar days if there is no verification, or there needs to be some sort of manual verification by the registrar. Compliance will start inquiring about that after the second notice.

There are also two concurrent, parallel tracks that we're looking for for Whois inaccuracy complaints. (That was okay.) The first one is based upon section 3.7.8 of the RAA as well as section five of the Whois Accuracy Specification. In this instance, the registrar has to take reasonable steps to investigate and reasonable steps to correct the inaccuracy. This is where the 15-day time line is started, when the registrar sends an inquiry to the registered name holder.

Compliance is going to be looking for three different results. The first one is that the Whois was updated and that the registrar provides validation and, if needed, verified the updates to that. The other option we're looking for is if the domain was suspended. The third is that the registrar verified that the Whois is correct and that there was documentation of verification for that. Next slide.

The other track that we're looking for is pursuant to specification 4, and this one is a little bit different. The 15-day calendar timeline is started when the registrar receives a notice, so Compliance will be counting that starting with the day after Compliance sends that notice. This is where the registrar must verify or re-verify the registered name holder's e-mail and, if it's different, the account holder.

One difference we've seen is, in the past, what had been done is the registrar, if they were testing an e-mail address, would send an e-mail and state that there were no bounce-backs, and that would show that it was a valid e-mail address. That is no longer the case under the 2013 RAA.

There must be an affirmative response from the registrant demonstrating receipt of the e-mail. That can be accomplished from the registrant clicking a link in the e-mail, providing a validation code, calling the registrar, but there must be some action on behalf of the registrant for that.

The registrar can do manual verification, but we would need to see some documentation, specifically the date, the time, the method that that verification occurred. Next slide, please.

This is a representation of those two parallel tracks, and Compliance is going to maintain the 15 business day notice period for the Whois inaccuracy complaints just so we can be sure that if there's delays with sending the notices or the registrar processing it and sending it to the registered name holder, that would allow either of those 15-day periods to expire before the time for ICANN to follow up and do a second notice.

Here you see a Whois inaccuracy complaint. It goes to the registrar, who then must verify the e-mail and investigate the complaint. If the complaint is about the e-mail address, then only one of the tracks applies. But if it is the address, that would have to go through a separate process on the right, where on the left, also, has verification of the e-mail that has to occur. Next slide, please.

The 2013 RAA has abuse report requirements. Caitlin went over some of them earlier. What we're seeing is that law enforcement complaints aren't just ones from a local jurisdiction. They can be from any applicable jurisdiction, and those reports have to be responded to within 24 hours. You don't necessarily have to answer the phone, but they do need to be addressed and responded to appropriately within that timeframe.

As for abuse reports from the general public, registrars must take reasonable and prompt steps to investigate and respond appropriately. And what we're looking for in Compliance is: did the registrar receive it? What did they do with it? What steps did they take to address that complaint? That can certainly vary based upon the type of complaint and the severity of what the allegation is.

We will check to see that if somebody submits a complaint that a registrar did not respond, we're going to confirm whether the reporter actually did file the complaint with the registrar and if they provided sufficient information to the registrar. It's not just they can't say DomainXYZ.com is bad. There needs to be some supporting documentation to assist the registrar in investigating that and taking appropriate action.

Another thing we've seen from registrars is stating that they're not taking any action because it would require a court order. If a registrar takes that position, they do need to provide ICANN with a specific local law or regulation that states they need to have a court order in order to investigate an abuse report. Next slide, please.

CAITLIN TURBERGEN: Now we'd like to open it up for Q&A. If anyone has any questions, please approach the mic. Also, we'll take questions from remote participants now, if there are any.

WERNER STAUB: Werner Staub from CORE. Just about the e-mail address verification: we get the questions from people who have long-established contacts, e-mail addresses have been used for many years. When a new domain is added to a portfolio, for instance, our members will just kind of actually really bothersome for the customer to suddenly be told to have to re-verify an e-mail.

Is there anything like a statute, a long-established use? An e-mail address in correspondence could actually just be verified by the fact that it's been used in correspondence before?

OWEN SMIGELSKI: That was a question that came up during the registrar stakeholder group, similar. There is no requirement that for a domain that was registered – before the Whois Accuracy program spec came into play January 1 – there is no requirement to go back and do that unless the registrar does receive information suggesting that information is incorrect.

Compliance doesn't forward every complaint to the registrar automatically. We review it to see if there is sufficient information to support the allegation of the inaccuracy. It won't be just a blind report or just something for harassing.

Even if it is something that's there, that is what's in the contract. All we're doing is ensuring compliance with that, so that would be something we would need to see demonstrated. If it's not the case that there is inaccuracy, you have information that that is good, that's where you mail the invoices to, then that would qualify as manual verification.

WERNER STAUB: Even if there is no inaccuracy complaint, a new domain is being registered, would you then have to say, "Okay, now the new domain is being registered, added to an existing portfolio, everything is as it has

been for many years," would then an e-mail address verification be necessary?

OWEN SMIGELSKI: That is the requirement of the RAA.

MIKE ZUPKE: Owen, could you clarify for us thought that, once an e-mail address has been verified, whether the registrar would need to do that again?

OWEN SMIGELSKI: The question is that, if it's a new registration that's being done, would the e-mail address need to be verified at the time of registration?

MIKE ZUPKE: Right. So the question is: if a registrant registers a domain name and uses identical contact data for another registration the second time, would they need to re-verify all of that data, not just e-mail address?

OWEN SMIGELSKI: The data needs to be validated, not necessarily verified, at the time of registration. The affirmative response is only for the e-mail address at the time of registration.

MIKE ZUPKE: I'm sorry. I didn't mean this to be a trick question. I think Caitlin had a slide that maybe addressed this. If you want to flip back to that. I think what I'm trying to get at is we understand that there's going to be a learning curve for customers who have been interacting with registrars in a particular way for a very long period of time. Some of these new requests or new requirements will be placed on them.

But, I think, in terms of the overall burden on them, it's not. My understanding of the contract that is once the data has been validated or verified, it doesn't need to be validated or verified again, unless there is information suggesting that it has become inaccurate. Is that correct?

OWEN SMIGELSKI: Yes, I overlooked spec 3.

MIKE ZUPKE: Thank you.

WERNER STAUB: Okay, that's what I want to know.

CAITLIN TUBERGEN: Would anyone else like to ask a question? Remote participants?

MIKE ZUPKE: And just to be clear, it doesn't necessarily have to be a question about something that you heard in the presentation. Anything related to the new Registrar Accreditation Agreement is fair game.

KATHY KLEIMAN: Terrific. I'm glad you said that. This is Kathy Kleiman, NonCommercial Users Constituency. For those of us who haven't been part of the debate, we've been in other sessions, could you reflect the discussion going on on data retention right now, and the status with the registrars exception requests, and from our perspective, the noncommercial users, the protections that were given under national laws that allow our data to be deleted when it's no longer being used? Thank you. I'll stay up here to listen.

MIKE ZUPKE: This is Mike Zupke again. I volunteered to answer the question, and suddenly I'm full of regret. It's a complicated issue, and so I wasn't planning on answering questions today, but I'm going to try this.

The question is referring to data retention specification that, in addition to all of the data points that registrars are previously required to retain, there are now some additional data points. In addition, some of the old data points, the retention period was actually shortened.

So where in the past, for example, Whois data had to be retained for the term of the registration plus three years, it's now the term of the registration plus two years. Those are, I think, the two fundamental changes that are made in this new specification.

The question is about what happens in the case where a registrar has a conflict between their applicable law in their jurisdiction and what the RAA is basically telling them to do. There was recognition throughout the negotiation of the agreement that this was a possibility. So the specification itself includes a provision by which a registrar can come to ICANN and say, “I have this conflict. I wish for ICANN to waive certain of the requirements that conflict with my local law.”

That process is in place. It's in the agreement. That's always been something that we've contemplated. A total of, I think, 15 registrars have now invoked that process with ICANN, representing, I think, eight or nine different national jurisdictions. Of those, one has been through the entire process.

The process, I should say, that's specified in the agreement is that after the request is received, the registrar should also include some statement from either their data privacy authority or some reputable law firm in their jurisdiction.

They provide this and, typically, what happens in practice is that ICANN reviews this and determines that there is probably more information that's needed. That's been kind of the case for all of these that were received. By that, I mean registrars have submitted to us statements either from their local authority or law firm or from the Article 29 working party that says these requirements are, in essence, they're problematic. There's a conflict.

The part that we don't typically receive on the first go-round is the part to says, “Here's what we can do.” That's really what I think you're

hearing from people in the community is that's a really hard discussion to have because it's not entirely clear, based on most jurisdictions' laws that we've looked at.

So the process is sort of, it's been described by some as negotiation, but I think it's really more of a clarification of what the state of the law is between ICANN and the registrar. We've been engaged in that process with all of the registrars who have submitted these requests for waiver.

As I said, one of these waiver requests went through the entire process and then, as required by the specification, it was posted for 30 days to ICANN.org. We opened up a comment period for people to submit comments on that.

And, generally, while anybody is free to comment, the comments that have an effect on this are ones that might say something like, “You misinterpreted the law” or “There's some issue here that we think that you weren't aware of.” It could be that they think the registrar misinterpreted the law, however it isn't. Those are the sorts of comments that we're expecting might have an impact on the preliminary waiver that's granted.

After that 30 days passes, I'm sorry this is such a long answer, I said it was complicated, didn't I? After the 30 days passes, it generally will then become final. If we've received comments that indicate we need to change something, that's our opportunity to do that.

A French registrar went through the process and was granted their waiver. A Belgian registrar went through the process and is currently in that posting period. Assuming that there's no comments that come in

that suggest that we've made a mistake, then that one would also be granted and we continue.

There are a few other registrars who are, I think, kind of getting close to that process. I think it's been kind of a slow-going thing. I know that it's been challenging, I think, from the registrar perspective and, frankly, it's challenging from the ICANN perspective, too. It's just really difficult stuff. We're trying to talk to people in those countries to get insight into whether what the registrar is providing to us is accurate or, if they haven't provided us enough, if they can help sort of augment what we've got in front of us.

So, a very long answer. I hope I answered the question. Okay, good. Thank you.

AMADEAU ABRIL: Good morning, I'm Amadeau Abril from COREHub**.** I had one question, but now I have two. Going back to the answer to Werner's question before, sorry, but that got lost because it got two answers. One answer, I don't know who it was, but from compliance - perhaps Owen, I don't know the name – was something like each registration must be verified, validated. The other answer is, well, no, if it's originally been validated, that's concrete data set. The concrete e-mail in that case, that's it.

So, just for a stupid person like me, if we have a customer registering 1,000 domain names, we need to validate and then, when it comes to Whois Accuracy, to verify those e-mails one-by-one, even if it's exactly the same data? Or just once? And then we have all the subsequent

registrations we have from that customer, that's okay. Sorry, but that got lost.

OWEN SMIGELSKI: If I could answer that, I misspoke. And, specification I think it was paragraph three states that, unless you have additional, you don't have to do the validation or verification if it's identical information and the registrar has no information to suggest that it's inaccurate.

AMADEU ABRIL: So it's enough having verified?

OWEN SMIGELSKI: Yes.

AMADEU ABRIL: Now, back to everybody's favorite topic, the data retention specification. Now, here I have a different topic. We have requested the waiver, we are following all the procedures that have been described. I don't know who was talking. I think it was Mike. Sorry, I cannot see faces from the distance. Just one sign that we would prefer dealing with ICANN than dealing with outside lawyers, but you know life is as it is.

We have one problem, though, is that ICANN is only willing to discuss one aspect of the data retention article, which is 4.3, and it is how long. Now, they are accepting to discuss the purpose of the dataset.

But for us, there's a much important point, which 3.4.3, which is to whom we may disclose, we are forced or allowed to disclose the data. If we only keep the data for the sake of keeping the data, it doesn't make any sense.

For the customer itself, it may help, but the real interest in article 3.4 is where in 3.4.3 it says that we must give the data to ICANN upon reasonable notice without specifying the reasons that ICANN may have. It may probably be perfectly legitimate. And then, at the end of that part it says that ICANN may or shall not disclose, unless ICANN wants to disclose to a third party. That's the summary of that part.

And then, in the middle, there is something saying in case that you think that the request from ICANN to send the data to ICANN it's not according to international law, you will engage in good faith negotiations to discuss the limitations, the guarantees, the protections for that disclosure.

Okay. Let me tell you that what's absolutely clear in most European legislation is that we cannot give any post-constructal data to ICANN. The first question is why this cannot be addressed in the waiver? And the second one, if not addressed, what's the point of the waiver? If we again need to discuss each time whether we should send the data or not, the answer is very clear. No.

And the third question is the more important for this session here: what's this good-faith procedure? Should we discuss it with Compliance, with Legal, with Jones Day?

How we will discuss each and every time for this useless waiver we cannot include this disclosure, whether this is within the legislation or not, legislation that probably people at the table and most people in ICANN staff will not know because you don't have that many lawyers trained in your law, for instance, or Spanish law or Swiss law or Argentinian law, etc.

How will this work? It won't, but how do you think it would work?

MIKE ZUPKE: By my count, that's like five questions, so I'll do my best to answer all of them, but by all means, if I miss something, I'm operating on about one hour of sleep. Feel free to keep me honest here.

One of the things that you mentioned is that, as part of this process, we've asked our outside counsel to talk to registrars' counsel about these waiver requests. The way that this originally sort of was envisioned was that it wouldn't be quite as complicated as it is. We would do our bit of research on the matter, and we would have our registrar relations staff would go back to the registrar and say, "Okay, here's your waiver."

What we learned through this is that, first of all, it's extremely complicated and, second of all, I think there's perhaps a perception among some registrars that we don't understand the complexity of it. We absolutely do understand the complexity of it and, in fact, it seems to have made the process more efficient by having outside counsel do this.

Just so it's clear, although I think it's known our outside counsel is Jones Day for most of these, we've got, actually, European counsel who are quite well versed in these topics who are the ones engaging with the registrars' attorney. And so, from my perspective, it seems really helpful to have people who are talking the same language talking to each other. They're talking the privacy laws, and these things are quite complicated.

That was sort of the thinking. It's not an intent to try to chill the dialogue. In fact, it seems to be helping to make the dialogue smoother. But by all means, we're always happy to take feedback on those sorts of things.

There was another issue that you mentioned about the purpose for retaining data and the purpose for, potentially, ICANN disclosing data. So I'm not an expert on the paragraph 3.4.3 that you were referring to, but in the 2009 RAA, it was a considerably shorter provision. It basically said that registrars would make data available to ICANN upon request for inspection and copying, and that was in the previous agreement, too.

The newer version makes clear that this idea of making data available for inspection by ICANN might be impractical. You know, a registrar might say, "That's fine. Come to my office. It's on Antarctica," or someplace that's really impractical for us to reach.

What the agreement now says is that if the Compliance team makes a reasonable request, the registrar will provide the data. Then there's this carve out that says, "However, if you have reason to believe there's

some legal thing that prevents you from doing this, we're going to engage in that good faith discussion over it."

I think that the purpose of ICANN having access to data has never been to disclose it to third parties. It's always been about compliance, enforcement, and monitoring. I think there might be ways for us to address this just through either clarification or an affirmative statement by ICANN at the time of the request saying, "This is our intended purpose of it." So that might be something we can solve without having to go through an entirely new data waiver request process. That's that.

But about the purpose of the data that's being collected and retained by registrars, one thing I just thought I would point out is that, last week, ICANN posted a document for public comment that is intended to try to help clarify what we mean when we say the purpose of this data.

In fact, if you look at the correspondence from the Article 29 working party, they say it doesn't state in the contract why this data is being collected. We understand that. That's really what we're trying to address, not just for the working party but for the world, is we believe there are valid reasons for collecting this data, but it's not necessarily that ICANN staff should be the sole dictionary of purpose or sole definer of that purpose, or clarifier.

What we wanted to do was put that out for public comments that others who might have ideas of things that we didn't consider could also have input into that process. Hopefully, that's helpful, and it's not at all intended to make the process harder. It's intended to make it so that data privacy authorities as well as the attorneys who are considering

these difficult issues have that data point that maybe that didn't have or that they felt they couldn't rely on because it wasn't stated someplace in writing.

Finally, and I think maybe this is sort of no longer really relevant, but I think that in the event that you have a request from ICANN for data, it would be to that person who has made the request if you have an issue about that request or you believe it conflicts with your legal ability to comply. It would be to that person that you would want to raise that issue. There's not a new waiver process that you would need to follow for that.

Please, tell me if I've answered all of your questions.

AMADEAU ABRIL: Yes, thanks. I'll give you an example. We have no issues with Jones Day in general or with the specific lawyer we had. Quite the contrary. Our lawyer, the one we had and we are still having, is a very reasonable person.

For instance, she completely agrees with us that we cannot disclose the data to ICANN in any way, with any protection. We cannot allow ICANN to see the data in our offices because this is expressly forbidden by our legislation. Only law enforcement agencies. If ICANN gets a law enforcement badge or TLD or something, then we could discuss.

Now, when we address this issue with her and she says, “Well, I will ask ICANN.” And she comes back and saying, “ICANN doesn't allow me talk about that with you. This cannot be part of the discussion.” This is why I

am saying that it's not very helpful sometimes to have these intermediaries because you want to discuss with a real party whether we can discuss. If she has orders not to discuss a point, that's the end of the discussion.

And the reverse, well, I just want to tell ICANN Compliance, they can take a note that COREHub will never provide post-constructal data to ICANN. So if you want to start Compliance now, you may do it, but there is no way we can do it. And, if the [inaudible] doesn't work, we will send you the DPA the Digital Protection Agency to tell you why. Okay?

MIKE ZUPKE: Thanks, Amadeau, I think that's actually very helpful feedback. We'll take that back.

STEPHANIE PERRIN: Hi, I'm Stephanie Perrin, and I'm with the NCUC. My question is about how you manage the individual's personal data access rights under this particular regime.

If I'm understanding this correctly, and my apologies, I'm not an expert on how you do compliance whatsoever, my expertise is in data protection law. So you, ICANN, and your Compliance department have to comply with my access request as an individual to information about how you decided to let law enforcement have access to my data. And so does the registrar, right?

Is there a common procedure for this? And who bears the costs of these subject data access rights?

MIKE ZUPKE: I think that's a very valid question, but it's not one, I don't think any of us are prepared to give you an answer. I'm afraid it's a little bit beyond the scope of just the RAA, but we'd be happy to try and get an answer to you back on that.

STEPHANIE PERRIN: But you do that right now in the Compliance department, right? So it's not as if this is new.

MIKE ZUPKE: What I think is new is, at least to me, is this notion of an individual coming to ICANN and asking for information about their information. It's not that it's new, but that I have no knowledge of it. I think it's just kind of beyond the scope of what we here in the front can speak to, today.

OWEN SMIGELSKI: This is Owen. For the stuff that Compliance has, that is kept confidential. Nobody gets access to that information. That's not anything to be requested or anything like that. That is all internal to ICANN.

STEPHANIE PERRIN: Okay, so that's okay as far as that goes, but it doesn't cover your data subject access rights. Anyway, I'll pursue this offline. Thanks.

CAITLIN TUBERGEN: We have two questions from remote participant Marcus Schäfer from Hostserver. The first one is: is there a timeframe for re-validation of e-mail addresses, such as after one or two or more years?

OWEN SMIGELSKI: This is Owen, for the record. That would have to be there would be no timeframe in there in that contract, unless the registrar has information to suggest that it is inaccurate.

CAITLIN TUBERGEN: And Marcus' second question is: as a registrar under the 2013 RAA, am I allowed to do the e-mail verification before updating the Whois data to prevent the domain names from being suspended if e-mail verification failed or do no Whois update if the verification fails?

OWEN SMIGELSKI: Again, this is Owen. For that, we see those types things going on concurrently, not doing one and then waiting for that response, coming back and then doing the next. That's something where you would send the e-mail and then do any other validation or Whois updating and then doing the verification and the validation required for that.

CAITLIN TUBERGEN: We now have another remote participation question from Gavin. Can ICANN expand on the accepted methods for data validation? Is it clear that physical address format is outlined, which is fine. However, does ICANN require or expect validation of address accuracy with third-party data validation provider?

OWEN SMIGELSKI: This is Owen. The Whois accuracy program specification lays out the requirements for that, whether that's the telephone number has to conform to ITU-T standards. I don't recall exactly what all of them are, but they're listed there in that. I believe Caitlin put that slide up.

That's what it needs to go through. There's many different ways that registrars can ultimately achieve that type of validation, whether it's something they do manually, credit card validation. Software can do that. There's lot of solutions for doing that. And that's until there's the cross-field validation, which would further enhance that.

KATHY KLEIMAN: First, thank you. Thank you for the detailed answer. Thank you for your time. This is difficult material and new ground for us, for all of us, for the community and for you, Which is why I want to ask the question.

There’s a lot of time and effort going in, of yours, of the registrars, the registrants. Are there metrics being kept? And, if so, when might we see them? Are there metrics being kept about whether all this time and effort is achieving the purpose for which these rules were adopted?

OWEN SMIGELSKI: From a Compliance perspective, we are keeping a number of metrics on all of those things that are coming in, the new 2013 RAA complaints. We have different resolve codes for why we would close a complaint, and we are keeping track of that.

For some of the more, say, high-profile complaints, heightened interest in the community such as abuse or privacy proxy, we have additional resolve codes that we might do as opposed to, say, some complaint types might have a less number so we could gather that data.

I do know there is a Whois Accuracy study that's going on, which will look for a scope of not just sampling some domains. It's going to be specifically targeted to do geographical differences; registrar differences; big, small; 2013 RAA versus 2009 RAA.

That's not anything that Compliance is tracking, and it would be difficult for us to do just as a global basis, but that is something that's anticipated in that study and they should be able to draw some conclusions about whether Whois data is more accurate under the 2009 RAA versus the 2013 RAA.

KATHY KLEIMAN: But if I might follow up, verification and validation that the accuracy is for a purpose, not in and of itself, but for a purpose involving law enforcement and others? Are those kind of metrics being kept that with that this new accuracy is serving, again, the underlying purposes for which these rules were adopted?

OWEN SMIGELSKI: That's outside of the Compliance scope. We process complaints. That's a policy thing that would have to be handled outside of at least Compliance. I don't know if that's something that…

MIKE ZUPKE: This is Mike Zupke again. I was just going to point out that this question was also asked by registrars when they met with the Board on Tuesday. And at risk of misstating what the answer was to them, they raised this question directly with Fadi, and he did mention that work is underway with the law enforcement community, in particular, to try to do some tracking and reporting of that sort of thing.

I don't know that we have more specific information than that, but I think that it's clearly a matter that's been raised by others, and it's something that's important. So it is something that we, ICANN, and the big ICANN, everybody in this community, is probably going to be looking toward.

KATHY KLEIMAN: I wasn't in that meeting, so thank you.

CAITLIN TUBERGEN: We have an additional question on the chat from Marcus Schäfer. Is ICANN in compliance with the Safe Harbor program for data transferred to ICANN?

MIKE ZUPKE: The Safe Harbor provision, as I understand it, is a set of requirements that have been put in place between governments so that if you're a U.S. organization, by complying with these requirements, European organizations, in particular, are able to transfer data to you.

I think there are fairly specific requirements, so I don't know that that's something that we've actually gone into detail to address, but I think that's why that provision in the RAA allows the registrar to raise that question of compliance with their applicable law for data exchange.

STEPHANIE PERRIN: Graham's letting me come to the mic before him. The Safe Harbor agreement doesn't apply to non-profits, so ICANN can't use it.

MIKE ZUPKE: So, then that would be a no. Thank you.

GRAEME BUNTON: Graeme Bunton from Tucows. We were talking about this in the registrar session the other day, but I'm hoping Compliance can give us a bit more context into how they're interpreting some of the specifications within the RAA around if we get a Whois compliant that that has to kick-off an e-mail verification process. Especially considering, A, our investigation may reveal there are no inaccuracies or, B, that the Whois complaint is originally about postal code. Why would that kick off the verification process?

OWEN SMIGELSKI: Let me just bring this up here. I'm just looking up, bringing up the RA here so I can quote it. I'm not speaking out of kind here. Whois Accuracy program specification 4 reads, "If a registrar has any information suggesting that the contact information specified in section 1(a) through 1(f) is incorrect" – and that is all of the contact information that appears in the Whois output – "then the registrar must verify or re-verify the e-mail address."

It's not limiting to, I know during the discussion with the registrars, they said the intent was it would only apply to the e-mail address, but that's not how I read the contract, and I don't see where it just limits it to the e-mail address. It does specify all of the contact information in the Whois.

I do know that there is some other discussion on this and ICANN is taking this back to consider this further, but Compliance stays out of policy. We just look at what the contract is. It's not that exciting. We don't get engaged in those kinds of discussions. We just go by what is written in the contract and not what parties thought was or was not going to be included in there.

And that's a pretty clear read of that. If there's that unintended result, then we certainly will take it under advisement. I've checked with Legal, and there will be some things that we'll take back and consider after this meeting.

GRAEME BUNTON: Great. I look forward to the output of those conversations. Thanks.

STEPHANIE PERRIN: Again, I apologize. This is a naïve question, but even after a year of working on the Expert Working Group on the Whois new model, I can't get my head around how this process goes through – this process being the negotiation of the RAA agreement – without consulting end users, registrants, the grand public, as they say, in a more full-some manner.

Can you explain to me how, when the agreement was finally agreed, you consulted with the end users? Because basically what you're doing is signing away their third-party rights, through a contract with the registrar and ICANN. And if the registrar chooses to invoke the data protection agreement, and that will vary depending on how they do it, there could be plenty of instances where the registrars are, in fact, violating the data protection law, just nobody's noticed and they haven't applied for the exemption.

So I'm really confused and, after years in government, I know that government would at least have to do a regulatory impact assessment and consult on this to see what the impact on the stakeholders, the end users, is. I don't mean this as criticism. I'm just really mystified.

MIKE ZUPKE: This is Mike, again. I would be happy to sort of talk a little bit to the process by which we arrived at this agreement. I think that might help to answer some of the question.

When I started ICANN back in 2005, we had the 2001 RAA. That was in place until 2009, so that one survived a very long time. But I think that, all throughout, there was recognition among people in the community and on staff that there were changes that were needed, largely for the protections of registrants.

There were a number of issues, such as this concept of there being back-door accreditations where a registrar who couldn't get accredited by ICANN could go and buy another registrar and suddenly was accredited.

There were a number of issues that were raised in that round where we got to the 2009 RAA that were viewed as basically wins for consumers, and these were all improvements for registrar protections.

As part of that process, the GNSO provided a good amount of input, and a lot of their suggestions didn't make it into a negotiated agreement. So we kicked off, after that round closed, another process by which the GNSO was able to come up with recommendations for the next iteration of the agreement. So a number of those recommendations made it into the 2013 RAA.

But also, very frankly, a good number of the recommendations came from a statement by the law enforcement community saying we have these 12 recommendations that we think should be included in the agreement. Their statement was very widely received within the ICANN world. So the end-user community, I can understand what you're saying, is not necessarily quite as plugged in, despite the fact that there are different avenues within ICANN that do represent end users.

In any event, much of this was community generated whether it was through law enforcement paper or whether it was through discussions with the GAC or whether it was through this GNSO process. That's where the bases for these amendments came from. And then, throughout the negotiation, there were various points at which the negotiated provisions were put up for public comment. So there were public comment opportunities throughout.

I think the bigger concern that you're raising is that it's a very complicated thing, and the average end user is probably completely unaware of it. I'm not quite sure how that gets solved.

STEPHANIE PERRIN: Before I give this over to Elliott, I just want to say that I think that the risk here is extremely high. I could probably in 24 hours get a massive Twitter campaign to complain, and you'd be dying in privacy complaints, and so would all the registrars.

And that's something they really don't want to have to deal with, I think. Because, as someone who has been at the pointy end of that, when you start getting thousands and thousands of privacy complaints, you don't get to just toss them and ignore it as SPAM.

ELLIOT NOSS: Stephanie, I think that might be, actually, a great thing to do. I'd love to have that inundation and flow it down to these guys because, Mike, that was...

STEPHANIE PERRIN: Elliott, I'm trying to get along, here.

ELLIOT NOSS: No, well, I've got to say that was historical revisionism of the worst kind. To describe either 2009 or 2013 RAA revisions as anything but driven by IP and law enforcement, but instead to try and characterize them as registrant and consumer protection is a crock, from my perspective.

I think that, having been through both of those negotiations, both of those comment periods, in very painful detail, there was no question who was driving the other side of this agenda.

I think that the proper characterization can only be – and I'm happy to do this on a point-by-point basis, both looking at clause changes and outcomes and behaviors in what was being enforced and what wasn't – that in fact, it was the registrars who were on almost every provision lined up with civil society, lined up with privacy experts like Stephanie in favor of registrants' rights.

And you had IP and law enforcement in favor of more restrictive controlling provisions, almost without exceptions. I think that was just a PR gross mischaracterization, frankly, surprising from you.

MIKE ZUPKE: And on that, Elliot, you get the last word because we are about out of time, but thank you for that. And thank you all for attending. I just want

to mention that the registrars have that resource for asking questions about interpreting the RAA: raaquestions@icann.org.

So with that, I say thank you, and enjoy the rest of the meeting.

[END OF TRANSCRIPTION]