
ICANN81 | AGM – Joint Session GNSO Registrars & ICANN: Perspectives on Registration Data Accuracy
Monday, November 11, 2024 – 16:30 to 17:30 TRT

TERRI AGNEW: Hello and welcome to the Joint Session Registrars and ICANN: Perspectives on Registration Data Accuracy. This conference is being recorded and please note that the session is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. If you'd like to speak during the session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom, on-site participants will use a physical microphone to speak. Helpful hint, if you're in the room, turn off your speakers now, please. Please state your name for the record and speak at a reasonable pace. And with that, I'll hand it back over to Ashley Heineman, our RrSG Chair.

ASHLEY HEINEMAN: Thank you so much and welcome to all of you. As folks continue to come through the door, that is good. So, I'll talk slowly to ensure we get as much participation as possible. So yeah, we are here today to talk about perspectives as they pertain to the accuracy of registration data. And as you may have experienced in Kigali, we're trying to do things that are a little bit more interesting, a little more creative. I will request if we do this again, that we do it earlier in the day because my creative juices aren't necessarily flowing as well at this stage of the day.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

But I just wanted to first thank you for being here and also to say the intention of this session is to discuss, to engage, and to understand the different perspectives. This is not a platform for putting forward positions, and we have no deliverables or output. We're just going to chat and hopefully that'll be a good thing. So, with that, I also want to let you all know that we were originally going to have ICANN talk to us about what we're currently required to do in terms of data accuracy and our obligations. But for the sake of time and the desire to have as much discussion as possible, we are not going to have that session. Sorry, ICANN. But we will provide those slides to those who are interested so you can see what that is. So, with that, I am now going to turn it to our remote participant, Sarah Wyld, who is going to talk about what we're going to do. So please go ahead, Sarah.

SARAH WYLD:

Am I here? Yes, I am. Hello, everyone. I'll put my video on. You get early morning, Sarah. Okay. All right. So, hi. In just a moment, we are going to split out into breakout groups using the flip charts that you see around the room, and I will remain here in Zoom for our online participants. Let's put up the next slide, and I will talk about the process.

So, each breakout group will be assigned a specific internet user's perspective. There are a few different options, and we ask you to put yourself into those shoes, the metaphorical shoes of your assigned perspective. Be in the mindset of that person and work through the questions that we have laid out for discussion, which will be up on

screen. The goal is to consider perspectives other than our own and try to understand why they are what they are.

We are not here to win arguments, as Ashley said, not here to create policy, but rather to come out of this conversation with a better understanding of the issue from the many different viewpoints, a better understanding than we had at the start of the session. We trust everyone here to remain constructive, polite, and open-minded. We requested input ahead of time from these various user perspectives on the meaning and importance of registration data accuracy, and we got inputs from representatives from most of those perspectives.

So once your group has done some brainstorming, the group leader will share that perspective's input, and you can see how what your group came up with matches or differs from it. There are also additional questions to prompt further thought. We definitely do not expect you to answer them all. Pick the ones that seem the most relevant or useful or interesting for the conversation within your group. Most of the breakout time will be spent discussing those questions and considering the input. Your leader will document the group's thoughts on the flip charts, and then when we have five minutes left, we'll ask the groups to review their discussion and choose high-level points to share with the room.

As you look around and think about what group you're going to join, we encourage, because we cannot require, we encourage everyone to join a group that is not your usual. Pick a group that you maybe have the

least in common with, if possible. We hope that this approach will help to expand our understanding of each other's views. Thank you.

ASHLEY HEINEMAN:

Thank you, Sarah. And just to note, the breakout rooms that we have are law enforcement, security, business, ISPs, end user, and registrant in the virtual room. I'm sorry? I said law enforcement first. And just to reiterate what Sarah said, do not go to the constituency that you're a part of. It's not fun if you do that. So, take a moment, get up, figure out what group you want to be in. I know, this is weird, huh? Come on, you can do it. You can do it.

ZOE BONYTHON:

And just to mention, we're obviously going to be trying to form equally sized groups. So, yeah, just try to spread out, and hopefully, and I understand that some community members belong to multiple groups, but yeah, try to pick one that you're not really participating in, typically.

TERRI AGNEW:

And, Zoe, can we pause the recording?

ZOE BONYTHON:

And Zoe, we can pause the recording. Yes, thank you. Can I get Ashley? Ashley? Not listening. Ashley? Everyone can stop. Okay. All right. So, we're going to move on now to the feedback, where group leads are going to be feeding back to the main group what came up with. I think, Ashley, it might be easier for me to pass the mic around for this, if you

like. Yeah. So, let me just get the slides back on screen. Okay. I need to stop sharing what's on screen currently. And let me choose. There we go. All right. So, we are going to start with ISP. So, I'm going to hand over to Eric.

ERIC ROKOBAUER:

Thank you, Zoe. All right. So, our group, we had Internet Service Providers. What was fun, I'll say in a nutshell, they were a little more technical than we were, but not much, though. We actually were aligned a lot in what they had provided. Those keywords, reliable, up to date, those are the items that we identified. We also said they would look for two-step verification, always want the context updated. We believe that ISPs want to see the reminders to keep data updated, and we also felt that they would want to send educational campaigns, maybe teach registrants about phishing campaigns, things like that.

And so, then what we differed, I'm just going to pull my notes real fast. My group is watching me do that. Okay, differences. So, they provided a lot more specifics about the RAA provisions. We didn't go into that much of a detail. It's excellent to see that they're calling that out. It's helpful that they recognize that. So, that was great. We just didn't get that far. One item that they went into was promoting KYC. We were a little more lenient when we were discussing. But what we liked is how they call out the promoting, so interested to have that discussion, see what options are there.

And then, finally, when we talked about how they internally want to make sure they had the data, we didn't go into what they identified in

the second question when they may get requested by law enforcement agencies for the data. We didn't get to that point. So, that was one area we differed. But otherwise, we had a great group. We were kind of spot on. So, well done, team.

ZOE BONYTHON: Great. Now, we are moving on to business. To, Ashley.

ASHLEY HEINEMAN: Thank you. So, yes, our group was putting ourselves in the shoes of businesses. And I think one of the first things off the bat is that it was identified that it really depends on the business and that a lot of businesses probably don't really care or have an interest. For example, banks would, for sure. And we pretty much aligned quite a bit with what the business perspective was that was submitted in advance and that having accurate information is helpful if you need that data. So, an accurate email address, there was a desire to have a physical, accurate mailing address, a mobile number, full name. And I think it's also interesting to note that if your interest is in trademark, that the interest is to defend that trademark and should contact their LEA or civil courts.

When considering what should be done to ensure accuracy, we had a whole bunch of different ideas. One was cross-check business databases. But when we further kind of explored that, we kind of realized, well, that's not always going to be reliable or authoritative, not necessarily trustworthy. Lots of different ideas on know your customer, including in-person registrations, relying on government databases,

facial recognition, and to achieve this, creating a global service, that their job would be to do this.

There was also the idea of having all governments work with ICANN, and it would be ICANN's job to facilitate ID verification. So, ICANN would have the responsibility to work with governments around the world and be able to tap into their ID verification databases or whatever other things are available. The idea to focus exclusively on digital IDs, again, and have the governments be responsible for verifying using their databases. Sorry, I'm too far away. Let's see.

There was recognition that KYC is definitely much more expensive. There was recognition that this would be difficult to do at a global scale, but there is, I think, obvious note that this is doable in certain countries, and I think that is it. So, thank you to my group.

ZOE BONYTHON:

Okay, moving on to security now. Thank you, Prudence.

PRUDENCE MALINKI:

Thanks, Zoe. Okay. Not that it's a competition, but I had the best team, just saying. Okay. So, we had the task of having the security perspective. And when it came to looking at what it is or what is it to have accurate data, we looked at things such as is the information, the data current or up to date, is it complete. And then we looked at broader, more philosophical things such as does it respect privacy laws relating to individuals. And then we looked at things such as the practicality of the data. Is the data able to be used for a purpose? Are

we able to contact someone? Can we use post or email? Sorry. And also, is it verifiable rather than fictitious and not fictitious and not fraudulent? So, those are the accuracy questions.

When looking at the effects of inaccurate data, we looked at things such as identity theft, we looked at things such as not being able to contact the actual person or the registrant, and then things such as fraud and the loss of domains. However, the team were really, really creative with regards to looking at the processes that we need to create in order to address the issue of inaccurate data and if they pose risks. Our responses were pretty much very close to the security perspective in that we looked at things such as verification processes, so the verification of email and phone, we threw up, as well as syntax checks, format of email, zip code, we came up with stuff like gibberish, but also we looked at the risks.

With the verification process, we discussed the risk of identity theft, but then we looked at broader issues. So, we kind of saw things such as human rights issues, issues to do with threats to life or political affiliation through verification of individual registrant data, and then we saw things such as, we went as far as to look at things such as loss of freedoms, religious implications, and a real threat of personal safety with regards to the verification of personal data, so we looked at that as well.

And then, with regards to syntax checks, one of the risks that we identified was the lack of globalization. So, for example, if we're doing syntax checks, they're very Western-centric, so we'd need to look at

things such as geographical regions like countries in Africa, which have completely different formatting, and also verification checks of this nature are not foolproof. So, we kind of looked at that as well as a team, and yeah, we kind of were pretty much in line, but the security perspective differed from ours. We actually placed more emphasis on the importance, whilst the feedback from the security sector actually was leading on the less need to have registration data accuracy, so we found that very surprising.

ZOE BONYTHON:

Okay. So, Ashley, if you wouldn't mind changing the slide while we go to the next perspective, which is going to be law enforcement.

JOTHAN FRAKES:

And Zoe, I'll save you some trouble running the mic over here. I'll stand here at the table. Yeah, so for law enforcement, we had a really good group because it was a mix of different people. It wasn't just law enforcement. We did have one person who was helping with that perspective, and we also had the benefit, I think, of getting some good feedback from some people in law enforcement going into this, so we had some fuel.

So, some of the things that you'll see up on the slide talking about that the true details are reflected. You want to basically see who the beneficial owner, for lack of a better term, or beneficial user of the domain name is. And then it became about, I've got my conscience here next to me, who's helping me with this, but essentially contactability

was the core thing, making sure that you could contact the person, and that sometimes would give way to, there might be a need to make physical contact to the registrar.

An example might be, for example, like a bomb threat or an exigent matter that you need to maybe go address, assuming that the person who's making a bomb threat might give the actual address in their WHOIS. Maybe they could be contactable. Somebody could knock on a door was the example. But making sure that the other entities involved was important, according to the early feedback. When we met as a group, we really did kind of aim towards where sometimes physical contact was needed.

On the next part on validation, being able to make sure that you can contact the registrant, that's true not only for law enforcement, but also something for registrars. Like we need to make sure that we can contact them so that they will renew the domain name so that domain services are not lost. Like, for example, if the domain name expires, gets re-registered by another party, and then a new person is now the registrant, making sure that that's all accurate as well.

And then digital certificates and things, like, for example, recovering from 2FA, two-factor authentication, were things that could affect a registrant, and that might mean where somebody might leverage a process like that to socially engineer taking over a domain name or an account.

Finally, for question three, KYC was a big one, and talking about that, I mean, that's where you actually physically sit with an ID and you go

through a lot of additional validations. And there was a belief that using KYC would reduce high-risk registrations. That there's a higher level of accountability associated with taking an ID, having maybe live photographs and ID taken as part of that verification process.

You could also clearly distinguish the roles and entities in the registration data, and then have periodic reviews to refresh. And some of those already exist in our material. We have people annually go and update and confirm their contact information, but it's still not, like, that verified. So, we had a great group, really good exercise. Really, ultimately the risks were making sure that accessibility of domains-- I can't read your notes.

FARZANEH BADI:

Okay. So, KYC, basically, we don't have a global identification mechanism, so providing the providing identification documents and requiring identification documents might hamper accessible access to domain names and registration of domain names.

JOTHAN FRAKES:

Thank you. Yeah, so we're not bouncers. We don't have a booklet of IDs. So, thank you all very much, and on to the next person.

OWEN SMIGELSKI:

So, this is the end-user group, and I will try and speed this up because we're pressed for time here. We had a little bit harder of a challenge because, first of all, we didn't have feedback on the end-user

perspective, so we had to start with that ourselves first. And then also there's the issue that an end-user is not a registrant, but registrants are indeed end-users. So, some of the things applied to that, those differently.

So, some of the information we found what does it mean to be accurate? Obviously, name, contact info, need to be able to contact them. Some of the concerns, the effects that could have of inaccurate data was inability to reach a point of contact or be able to try and buy a domain name or not receive renewal notices, that one was a registrant, and inability to identify a scam or fraudulent activity. How could that stuff be done? ID verification and reporting inaccuracy.

Some of the concerns that we thought, and we kind of didn't do it for each of those three areas, we just kind of did them globally. We had some concerns with cost. Is there a necessity of this rights of the data subject by doing that? The vulnerabilities with data leakage. We had some discussion about how some places could do identity verification, such as the ccTLD level, but not at a gTLD level outside of that country. So, we had some good discussions here. And then also thought about possibly using third-party verification services, but obviously there's some concerns and stuff like that. So, I'll wrap this up so we can move on on time. Thanks.

ASHLEY HEINEMAN:

Okay. Sarah is the last group. So, Sarah, would you like to go ahead?

SARAH WYLD:

I'd be delighted. Thank you. Hi, this is Sarah. Oh, I've closed the camera. I'm sorry. Okay. Hi. So, my group was the registrant perspective. And so, we started thinking about the main questions for what accuracy means. We want to be properly listed as the domain owner to make sure that we are reachable and we can get renewal reminders or notifications in case of compromise. The effect of inaccuracy that we considered was that I, the registrant, might not actually own or control my own domain name. And that can be very difficult for my business or personal use of that domain.

Then we thought about risks posed from accuracy processes, like the risk of my identity documentation being compromised, or risk of social engineering or getting spam email if the accurate registration data is public. But sometimes I do want to share my data. So, then we thought about what we can learn from services where validation of identification is required. So, for example, sometimes I want, well, definitely, I want my bank to know who I am, so that they can give me my money.

For a domain name, similarly, we want to be properly listed as a domain owner. And the overlap that we see is that in both cases, we want our data to be handled appropriately. So, the main takeaway from our group is that there's a difference between data being accurate and data being publicly available. Anything that's shared is at risk, whether that's the registration data itself or the identification to go with it. So, it's about proportionality of risks and making sure that it's balanced properly and handled securely. Thank you.

ASHLEY HEINEMAN: All right. That was it, guys. Again, the intent being just kind of thinking about a different perspective, thinking a little bit deeper on things and what it actually means in terms of what's being proposed and what's being asked for. And I hope this was useful. We're trying new things. Does anybody have any questions as a result of this or any comments that they would like to make before we wrap up? Go ahead, please.

UNKNOWN SPEAKER: Can we get a copy of these slides of the perspectives? They will be online?

ASHLEY HEINEMAN: Absolutely. And we're also going to provide the ICANN prepared slide deck that we didn't have time to go over. So, we'll provide that as well. Yeah, probably on the schedule, like when it shows like the Zoom recordings and everything, we can post the documentation there.

Any other comments, thoughts, parting ideas? Again, this was just to think things through a little bit and get to know each other as well. All right. That's it. That's it. Thank you, everybody. I appreciate your time. I appreciate those who provide input. Have a good day. We can end the recording, please.

[END OF TRANSCRIPTION]