ICANN83 | PF – GNSO: NCSG Discussion with SSAC Leaders
Wednesday, June 11, 2025 – 10:45 to 12:15 CEST

ANDREA GLANDON: Hello and welcome to the NCSG discussion with SSAC leadership. My name is Andrea and I am a participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. If you would like to speak during this 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. Please state your name for the record and speak at a reasonable pace. And I will now hand the floor over to Rafik. You may begin.

RAFIK DAMAK: Thanks, Andrea. This is Rafik Demak. Thanks, everyone, for joining us today for this joint meeting with the SSAC. I believe this is maybe our first time to meet with the SSAC, and we were looking forward to this for quite some time and happy we could make it for the Prague meeting.

As you can see in the agenda, we have several topics. There are some proposed or suggested by the SSAC. They want to share from their side to let us know what they are working on or they want to give us some highlights. And from our side, we want to share some

topics to give maybe more from our perspective if it can be an input or to help the SSAC on their work.

Again, I would like to welcome you for joining us and we are looking forward to have this conversation and dialogue and to keep it as much as possible because we understand about the technical part. We have technical people in our group that they care about human rights and so on. And we want to create more synergy and to find where we are in alignment and we can share our input, but also to hear from our side if what you are working on is something you are looking for, our perspective and so on. So, Ram.

RAM MOHAN

Rafik, thank you so much and thanks for inviting the SSAC to this session. We also have been eagerly looking forward to interactions with you, and if this session goes well, you will hopefully be motivated to call us again and engage with you. So, I am Ram. I am the chair of the SSAC and my apologies for coming late and beginning this session late. I will try to make up on the time with what we are looking to present.

I wanted to just go through for those who are not familiar with the SSAC just very briefly who we are and why we do what we do and then speak a little bit about the things that are on our mind, particularly some of the things that we think may be of interest and relevance and things that perhaps we can collaborate with you on.

So first, just a quick overview of the SSAC itself. We are founded as an advisory committee inside of ICANN and really our job is to provide advice on matters relating to security and the integrity of the Internet's naming and address allocation systems. We have a bunch of responsibilities. We perform those responsibilities. On the next slide, we perform them by mostly collaborative methods internally and then providing public reports that are available to the Board and to the community. In the last couple of years, we have shifted our way we work at the ICANN meetings. We have now shifted to having by default all our meetings being open. So, we invite anybody from the community to come and visit and watch and engage with us as we do our work.

Really, if you look at our focus, we focus on key SSRs, security, stability, and resilience issues. And on those issues, we really have published 127 reports over the last many, many years. Now, in that, we have, in the last year and a half, we have identified five keystone topics. It's an effort to enhance our role on critical security, stability, and resiliency items. And the five keystone topics are listed on the screen here in front of you. And really, our focus is on two pieces here. One is to make our existing advice more accessible and digestible. We have 127 reports. Roughly speaking, each report is probably 35-40 pages long and a lot of technical pieces in it. So, we are trying to get them down to a 500-word summary that can be easily accessed and digested.

And the other thing that we're also working on is how do we make sure that the recommendations we're making can actually have an

impact and can improve the ecosystem that we are a part of. So, that's the core part of how the SSAC engages and works. We are about a little over 40 people from around the world, mostly engineers, but a lot of technical expertise inside the group so that we can focus on these areas and any others that come in front of us.

I wanted to share with you some work that we have begun with the At-Large Advisory Committee. This is a campaign that we started a year ago called Safer Cyber. And I wanted to share that with you because there might be some interest and some relevance to what NCSG is doing. So, if you look at what the SSAC really does, we write reports, we provide advice, and the end goal is to enhance security and stability of the DNS ecosystem.

And we wanted to work with the At-Large to empower end-users in that area. And one of the things that we identified was end-users have a bunch of vulnerabilities, primarily from cyber threats. So, we worked with the ALAC. We provided the ALAC technical expertise as well as our analysis on threats to DNS security and stability. And then what the ALAC did was it took that work and was able to convert that into a curriculum, into a training program that is now being put out to all of not only the ALAC, but the ALSs and that entire model that they have, the various chapters and things like that. So, that's been put out.

So, if you look at the campaign, the first campaign has been on phishing and credential management. It's to teach people, end-

users, what is phishing? How are you going to be phished? You know, it's not a, are you going to be phished? It's a, how are you going to be phished? Because it's going to happen to you. Then what can you do when you get phished? How do you protect yourself? But also, how do you recover after you get phished? So, practical things like that. And that is now done. We have now initiated some work with the ALAC on the next set of topics that might be interesting and useful for end-users. You know, we've been, so, and that process has begun.

But we think that the important thing is when recommendations come through or when advice is given to the right people or to people who don't know what to do, when they have trouble, you need to have a plan. If you don't have a plan before you get into trouble, then it becomes a panic situation. We want to try and find ways to educate and provide materials that can allow the stakeholder groups and the advisory committees to be able to get to its members and say here are specific things that you can do. So, that's safer cyber.

The other thing that I wanted to brief the NCSG on is the work we have done in the recent times on name collisions and the new gTLD program. For those who don't know what this is, the idea is somebody comes in and somebody applies for a TLD string. And for whatever reason, that string is already getting traffic on the internet.

And therefore, you could have a confusing situation. In 2011, when the last round of TLDs came through, the SSAC came in with advice on name collisions. And the most prominent examples of those were .home, .corp, and .mail. And people who applied for those strings didn't realize when they applied that those strings were actually already very prevalent and there was lots of traffic for it on the internet. And it would cause problems.

So, we have created a framework to assess name collisions. And we provided that as a report to the community and to the Board. And the Board has accepted those recommendations. And the recommendations are, for the most part, have been implemented as an operational piece of this next round of TLDs. There is one part that we've started up a new work party called the Responsible Integration into the DNS Ecosystem, RIDE. We're a technical group. We have to have acronyms. So, we have the RIDE work party.

And the biggest thing that we're looking at is there are identifiers in the blockchain space. And those identifiers in the blockchain space are trying to interact and engage and integrate with the DNS names and the DNS system. At the same time, you find overlapping words. In the blockchain space, you will hear people calling them blockchain domain names. You will hear people calling things that happen in the blockchain space as resolvers.

So, there are words and meanings that come from the DNS space that are also being overlapping and are being used in the blockchain space. But much more important than that is that there

are behaviors in the DNS space that we know. We know that if you get a domain name, certain behaviors can be attributed to it. You can attach DNS records to it. You know that it'll resolve in a certain way. You know that the name has a registration term. There is an owner or registrant for the name. There's a registrar associated with the registry.

There's a bunch of parameters associated with it. If the name is abusive, there is an abuse protocol that you can engage. If the name is squatting on a trademark, there is a well-known mechanism to go and resolve those kinds of things. Those are some attributes and characteristics of domain names or identifiers in the domain name system.

Now, when there are identifiers in the blockchain system that are linked to these identifiers in the domain name system, then you have claims that get made that say there is equivalence or there is some a loose or tight coupled linkage from one to the other. That makes us worry about security and stability, especially stability issues that come with it, because you have trust in the DNS system. And there is an implication of trust when there is a linkage from the blockchain system into the DNS system.

So, the first thing that the right work party is doing is to look at the blockchain identifiers, especially as it relates to the next round of TLDs. We expect to put a public comment into the applicant guidebook that warns of collisions and warns of stability issues that are linked from names in the blockchain identifier space and

names in the DNS space. The work party at this meeting is meeting in public. So, if you look at the ICANN schedule, you will see the right work party. So, if you'd like to listen to the SSAC members deliberate on this and see where it's going, you're welcome to come and do that.

The SSAC also, by the way, has an open mic at every meeting. And we welcome anybody to come. And it's our version of ask us anything. We promise to hear everything. We don't promise to provide answers to everything because we may not know the answers. But again, it's a part of fostering and opening up the SSAC to input from the community. So, that is really the quick overview of not only the SSAC, but of where our time has been spent and where our priorities are.

RAFIK DAMAK Thanks, Ram, for this quick overview. I mean, you covered several points. So, I will start myself with some question or comment, and then we can see if anyone wants to comment. So, just about, since you talked about the safer cyber and your collaboration with ALAC, I assume we are interested in next efforts or initiative to see if we can help and join, bringing that perspective from registrant, but also like the human rights and so on, just to help in that regard. So, we are looking forward to such collaboration, if possible.

And regarding all your advice and report, more here process or procedural matter, do you expect just you want to have engagement with the community, like come to us and try to

present your work or you are looking maybe some formal input if we can review and share with you some comment is something you can envision is you are looking for such way of engagement or just you want to present more education and building awareness or is it possible that I'm not saying a public comment per se, but if we in our side, we feel in some advice or report, we think that maybe we see some point that can be elaborated or clarified and we send to you it's to create a dialogue or engagement.

The last maybe question, I understand like about the role of the SSAC. I mean, I'm not asking about the membership and so on, but I believe it's just clarifying, since I said we have also members in our side, but we can also try to bring from outside that can bring not necessarily that geographical and so on diversity, but also different perspective from technical side, those who are not sure that some work maybe in corporate world, they have different perspective, other work maybe for non-profit or organization or in different venues, so if we can encourage them to join.

And so just if you can help to explain maybe about process, how it happens, but also what skill set or profile you are looking for. Because even in term of technical things are changing, it's many for people when you say technical we think all we are the same, but for like we are engineers and we are working on different aspect and we are maybe more expert on one area than another. So this is just three question or comment.

RAM MOHAN

Thank you, so in no particular order, I think on the collaboration and providing input into the work that we're doing, we welcome that, particularly at these meetings where we have our work party meetings that are held in the open, there are opportunities to engage and comment. The rest of the work happens intra-sessionally and those things we just run on our schedule, those are not public meetings. But at the ICANN meetings, we are very welcome to engage not only disseminate, but also engage. That's one part of it, Rafik.

The other part of it is that we are quite eager in addition to getting your members input and suggestions, we are also eager to find a way to understand what are the unmet needs of your constituents, what are the things where they have questions or where they could benefit from some of the work that we've already done. And if you could help us identify what that is, we will provide the summaries, the reports, things like that in a way that is accessible for your constituents to be able to spread that. I mean we have a body of work, and we're quite interested in making sure that it's put to use. So both aspects are important.

As to membership, we have a defined process. If you go to the SSAC website, which is on part of ICANN, you will see what that process is, anybody can apply to be a member. There is a membership committee that is constituted by SSAC members who review all applications. Typically, the initial stage is a set of questions that are asked, it's written questions. They come into the membership committee, the membership committee reviews both the

responses to the questions as well as the credentials and the resume, if you will, of the person applying, and once they make a determination, then they typically will invite the candidate for an interview.

And one of the big expectations in that interview is that the candidate actually look at one or more of our reports that we've published and develops and can develop and can articulate their view on it, their own independent point of view on that topic. Because what we're looking for is the additive value, an assessment of what the candidate can contribute to the SSAC in its own deliberations. And it's also a sense of their intellectual ability to engage in complex topics and be able to contribute.

So, those are at a high level, the way it works, and Tara Whalen, who is not here, but she's the vice chair of the SSAC, and she heads up our membership committee inside of the SSAC. I'm wondering, Georgia, if you want to take a moment, you're somebody who has joined the SSAC not so long ago, perhaps share your experience in how was it to think of becoming an SSAC member, and then the process of becoming an SSAC member, and also how has it been once you've been in the SSAC?

GEORGIA OSBORN Hi, thanks, Ram. Georgia Osborne. I know you, Fazi, and nice to meet you, Rafik. So, I joined the SSAC, I want to say, for the last SSAC meeting, so, to the last, sorry, for the last ICANN meeting in Seattle. So, that was my first one as an SSAC member. The process

to join was there's a long sort of process to get to the interview stage. I think you had quite a few candidates that time. So, it took a little while, but then once I was in, it was very welcoming. I feel very welcomed, and it's very friendly, and the discussions are really interesting. So, it's been a great experience, but if you have any specific areas or specific questions, I'd be glad to take them. So, yeah, thank you.

RAFIK DAMAK Okay, thanks, Georgia, and thanks, Ram. So, maybe just a quick follow-up, and then go to Farzana. So, yeah, about the engagement, we can understand that we can join, but we're thinking maybe if we, like, that collaboration you have with, like, if something we can try to do. I mean, we see in which area. And the other point is that you say they are eager to get input and suggestions. So, do you mean, is it possible for us as NCSG to suggest to the SSAC to work on a specific topic to see if there is an area of interest or something to elaborate? So, it's not just for you to determine what are maybe the area, but getting input from us, we tell you.

RAM MOHAN Absolutely.

RAFIK DAMAK Okay, we will take that offer. Yeah, Farzana.

FARZANEH BADIEI

Thank you. Hi, everybody. I'm Farzaneh Badiei. I'm a member of NCSG, and I'm a member of the GNSO Council. So, my question is that, so basically, that Safer Cyber project is very interesting. Some of our members work with human rights advocates and activists, especially in diaspora, and sometimes there are phishing campaigns against them to access their sensitive data, and this can be very useful if we can also, like, get involved with other than providing comments, which is a great opportunity. Maybe we can provide our perspective and be integrated, or maybe we can have our own mini project.

So, that was one thing that I wanted to mention. The other things that, in SSAC reports, and also, Ram, you mentioned that you want your advice to be impactful. So other than technical impact, I believe that you also consider societal and human rights impact, and also you have privacy experts as a part of SSAC. Do you consider other, do you actually put that on your recommendations, like the societal and the human rights impact that your recommendations might have?

RAM MOHAN

Thank you for both of those questions, and certainly happy to not simply adopt the Safer Cyber that we're doing with the At-Large, but to do something that is individualized for the needs of your constituents, so happy to do that. Our reports tend to be quite focused on the technical pieces. So we don't specifically point out

the societal and human rights impact of what we're doing. And part of it is informed by the fact that we like to speak on things that we have expertise in.

I can say for myself that I would feel uncomfortable putting an SSAC report out on, say, responsible integration of blockchain names into the system, and be able to speak authoritatively about the societal and human rights impact. We can speak quite authoritatively about the security impact or the impact on the ecosystems that we're in, but we're willing to learn about it, but we don't have that, in general, that expertise in-house to be able to opine about it and to write that into our reports.

STEVE CROCKER Thank you. I've had to learn to shuffle here because a lot of feedback. A couple of points that resonate very strongly with me, so just a little extra introduction. I'm heavily involved with SSAC, but I've been spending my main focus worrying about the general WHOIS problem, and in that regard, not only have I been participating inside of ICANN via SSAC, I also joined the business constituency, which is not, I understand, part of NCSG. It's part of those other guys, but particularly, I joined it to get an understanding of where they were coming from with respect to those issues.

Where all this leads is that, from my perspective, the right answer for WHOIS should, for what the successor for RDRS and future systems, is it should include a framework that specifically allows

for focused attention to things like human rights and so forth, as policy issues to be provided, policy determination to be provided by the appropriate parties, with a framework that is not only neutral, but is provide specific hooks that allows those determinations to be made as opposed to ignoring them. We're not having any way of dealing with it.

So Farzanah, that's why you and I find ourselves in certain kinds of meetings together. And the one kind of meeting that you're in that I have, do not go to is the council, the council and in the back of my mind. I keep wondering exactly where are the key decisions being made sometimes implicitly, sometimes dare I say, cluelessly. and when I go through that line of thought, GNSO council comes up prominently in my list of candidates of where some of that action is or should be. So I just wanted to mention that for everybody. I'm deliberately using multiple avenues here to attack the same problem.

FARZANEH BADIEI

Thank you very much Ram, and Steve. So yes, GNSO Council very complex , but we do provide some kind of like briefings from time to time. And we can chat a little bit about it more to see which sessions and working groups you can you can monitor.

One of the things, we have a small team on accuracy and now I'm talking exclusively in my personal capacity. This is not the council or anything like that, but in the topic of accuracy we suggested that we should do educational programs for the registrants to

understand why accurate data is important and why it is important for them to keep their data accurate, their WHOIS data accurate in the system. So maybe in the future, that could be something that you know, we can work on together to do some kind of like educational thing. So that was very inspiring. Thank you.

And another thing. So Ram, I understand that you are you you're technical and you want to keep that technical remit. but what we can do, we can bring that human rights impact assessment to your advice and we can like look at it, use a framework that as digital rights advocates use usually for HRIA to look at your advice and to provide you with some recommendations. On how to consider human rights.

RAM MOHAN That would be really welcome. Again, because we don't have the background in that, if you know, for those given you have the background that would be both informative and I think we'll learn something from it. So I, I look forward to that.

RAFIK DAMAK I will take this as an action item for us kind of to follow up later. Okay. Let's see if there is anyone else in the queue I mean, here or on Zoom. Okay. If you want to discuss more about the topics from your side, or you want us to move to the NCAG. Okay.

So the NCAG, we have several topics. I think the top three, that's really what we are working on. And I believe maybe Farzana will try

to explain for each. And at the end, I think it's more because the DNA is blocking. We know there is the report. Maybe some could have some like skimming it quickly. So maybe we can ask you for a few questions, but I believe also maybe Farzana will share from her side because we don't necessarily have a position on that. Just we find out. I think for many of us are interested because some of us, they know what's DNS blocking in terms of sensor heap and so on. Okay. Let's start with-- still we are not in any other business. Still we are in the same business. Go ahead.

FARZANEH BADIEI

Thank you. I'm sorry, I was preparing some slides, but then I didn't finish them. So you just have to listen to me. So for the topic of accuracy, this is the accuracy of domain name registrant data in RDAP. And so there are conversations going around in the community about how do you verify accurate data. And there are certain suggestions that also some want to use NIS2 for verifying the accuracy of data.

And one thing that is concerning to us is that in these conversations some groups believe that accuracy is, can be done through verifying the identity of the domain name registrant. And that's, for us, is a very, very concerning suggestion because we believe that domain name registrant anonymity is very important. Even a human rights advocate wants to have a website or a campaign and wants to remain anonymous.

And another problem that we see with that is a matter of access. So how are you going to verify the identity of people globally? Some people don't have identification. And another is a grave concern of ours, which is privacy like, and data protection. So when you ask them like how, what sort of mechanisms can we come up with for the registrar to keep that data protected?

So this is why we believe that accurate data actually means data that enables the domain name registrant to be contacted in terms of like to ensure security and stability. And we also believe that there should be accurate data because the domain name registrant will lose their domain name and which we really care about.

So we think that they should keep their data accurate in order to keep their domain name. But at the same time we believe that accuracy means being able to contact the domain name registrant. I just stopped there. I want to know, because I think I read some, I'm not dreaming that you, you have some opinion about the topic of accuracy. I think in 2023, I saw an SSAC. So, yeah.

RAM MOHAN Steve, do you want to take this?

STEVE CROCKER I'm in a strong agreement with you, Farzana. But in addition, another aspect of what I consider to be part of accuracy is an even more fundamental question. The registrant is where the main focus is, but when you look at the other roles, admin contact, tech

contact, and so forth, then a question comes up as to, so what do those mean? What are the roles actually entail? And to be more precise about it, I would say that every single role that is defined, however many there are, you should be able to answer two questions. What is the obligation of that, of the person in that role? And what are the capabilities? What, what authority do they have?

For the registrant, it's pretty well defined, but for the other contacts, there's remarkably almost nothing written about what those actually mean. And if you dig back into the history, they have been carried over, over many, many, many years, and evolved. But then if you try to break it down to the basics, you get nowhere. We should have an extended conversation. I share what I'm saying primarily for the benefit of everybody here, just to be alerted to the idea there.

But when I brought that up in the accuracy discussions, the answer is, oh, that's out of scope. I say, well, wait a minute here. You're trying to nail down the precise accuracy of that data, but it doesn't mean anything. What are you trying to accomplish here? So things get interesting after that.

RAM MOHAN

Yes. SSAC has written about this topic, I think most specifically in our input to the EPDP. And look there are some in the ecosystem who believe that accuracy, security, and privacy are all opposed to each other and that they are mutually exclusive and at least our opinion is that they each have a purpose and you have to make sure

that that purpose is achieved. And having access to the information is an important part for certain organizations or certain parts of the ecosystem. If you're in law enforcement you want to find out who is the owner of a domain name that's an important thing.

And there are two parts to it. One is how do you get, how do you find the information? The other is, do you even have access to it? You know, you find some systems today that rate limit, a law enforcement agency's queries after a very short amount of time. And that is not doing necessarily any good to anybody in the ecosystem.

As far as accuracy is concerned, we think that what we have said is, is that the evolution as technology has gone and as practices have moved forward, the data that is publicly available, you know, through the registration data systems, the relative accuracy or accessibility of that data has reduced, right? There's been a lot of accuracy in the registration data. That's one part. And then the other part is that there is really nobody validating whether the registrant of a name that is public is actually the registrant of a name, right?

FARZANEH BADIEI The registrar is not validating?

RAM MOHAN

Well, I don't know that the registrar, that all registrars validate that the registrant of a name is actually the registrant of a name, because if they did, you wouldn't have names in the WHOIS record that say Mickey Mouse. You wouldn't have names that are quite clearly not valid names. They presumably know who the registrant is, but it's not public. It's not available in any public way. They know who they build to get the money to buy the domain name from them, right? So they have that data.

And law enforcement has a way to get to that data through proper means and methods. But I'm distinguishing that information from the information that is publicly accessible, you know, and available through registration data access methods. And there's kind of quite a gulf between them. The advent of GDPR has also resulted in the kind of unintended consequences, but a lot of data is now just redacted.

FARZANEH BADIEI

Private personal data.

RAM MOHAN

Right. It's private personal data. And so what we're finding is that when law enforcement says, I want to have access, there are two parts to it. One is, do they have access just because they ask. And the other part is, should they be given access when it is legitimate. And we're much more clear that when there is a legitimate need for access to who owns a domain name, and there are specific

mechanisms for it, that those there should be a way to do that, number one.

And number two, even being able to access WHOIS systems and not have arbitrary rate limits put for legitimate requests for requests that come from law enforcement, for example, that's something that we've had discussion in. We have not published an opinion on that to the community, but it's an area of concern. Because we talk to our friends and colleagues in law enforcement who say when they begin an investigation to even gather the basic information may require tens, if not scores of queries into the system. And if you're limited at 10 for a day, now you've inadvertently slowed down or stopped an investigation.

FARZANEH BADIEI

So I have a few points. So actually, so when we talk about actual domain name register, we don't have to identify them and see who they are. We should, in order to keep preserve their privacy, we believe that when they actually-- so the registrars are contractually obligated to verify that the information that the domain name registrant provides is accurate. And the registrant has, I think, two weeks to verify their email address and phone number in some cases.

So we think that for the investigation and matters like that, if they are outside of ICANN mission, I don't think that we should solve the problem through ICANN and by requiring registrars to identify the domain name registrant. So I actually think having Mickey Mouse

is okay as a domain name registrant name, as long as they are contactable and when there is a security problem, you can contact them.

But these are the actual conversations that we always like get into. We just want to make sure that the community understands where we are coming from, that this surge to identifying the actual domain name registrant. Well, Steve is here. I don't know if I can say this, but I never thought WHOIS was actually about identifying who is the owner. It was about contacting the domain name registrant. But we might disagree on that. Just to point that out.

RAM MOHAN

That's really good perspective. Inside the SAC, we've not had a detailed discussion on that kind of differentiation between the need to have the ability to contact versus the need to be, to guarantee that everything that is presented is verified. I'm very sympathetic to what you're saying. The foundational piece there is that when there is a problem from a security and stability point of view, you ought to be able to find a way to take some action on it without it being onerous.

LYMAN CHAPIN

I don't have a nice little card, so Lyman Chapin, I'm a SSAC member. One of the things that we've been trying to do, again, within SSAC is focus on not on absolutes as if accuracy were a platonic ideal and everything had to be accurate simply in order to be accurate. We've

tried to take the approach of saying, what are the purposes of accuracy? What are the purposes of access? So, instead of thinking about them as, well, of course, everything should be accurate. That's on its face. That's obvious.

But in context, what matters is why are certain things important? Why should certain kinds of information be accurate? Why should certain kinds of access be allowed or not allowed? So that you can apply a much more specific set of criteria to the way in which you create systems that either allow or disallow or create criteria for access to information.

There's a tendency, I think, to very quickly allow the apparent conflict between the rights of people who want their actual identity to be concealed when they register a domain name in one way or another and the obligations of a variety of authorities to be able to pursue information when they have investigations. And we can dance around that and pretend that that's not a source of tension. It is, and it's going to be.

We can't solve all of the social and governmental and other kinds of problems entirely within the DNS. These are things that exist in a social framework that is much larger than what we're dealing with, which is why we're trying to be very careful not to think in absolutes, but to think in a much more careful and nuanced way about the purposes of pursuing a stance that goes this way or that way on some of these spectrums.

RAFIK DAMAK Okay, Georgia.

GEORGIA OSBORN Hi, I have a curiosity just about your kind of approach to it in terms of, I did some checking on the NIS Corporation group who have taken a risk-based approach. So I guess I'm just curious, just in my own personal capacity, whether you've looked at that risk-based approach. I know it doesn't define the risk, which is obviously complicated, but I'd be curious to know what you think about it and if you had any takes on that approach. Thank you.

FARZANEH BADIEI So are you talking about the NIS2?

GEORGIA OSBORN Yes, yes.

FARZANEH BADIEI So we have looked at it. And yes, that is an interesting approach. It's just that like there are different interpretations and this is a directive. So some countries will go, I mean, so these are guidelines. But some countries will take a very, I would say, extradical approach to it. And some countries take, and it's like NIS2, frankly, it provides countries with different approaches that they can take to the verifiability.

But unfortunately, when we want to apply that framework globally, it becomes very, very difficult. But that is a very good point. We can look into it and we can actually, as NCSU, we can do some sort of analysis. But what we want to do is to be a little bit more jurisdiction agnostic and look at this from the global point, but definitely it's very relevant and we will look into it.

And thank you so much for your comments. So this one is the favorite of Steve. It's disclosure of private data to third parties. So I thought that we should discuss this because, for the NCSG, we believe that the disclosure of private data of domain name registrant, when the request is submitted, we believe that there should be another layer that when the registrar gets the request, they should do a fundamental rights balancing or a human rights impact and see if there is an impact on the registrant if they disclose the data.

And so one thing that we are concerned about is if we go down the route of, and I'm not claiming that we are, but if we go down the route of automating these requests to, like the response to be automated, then that part of the fundamental rights balancing might not be done by the registrars. And while some of them are obligated by the law to do that, but we want to see that globally, that all the registrars do at least a minimum of, okay, so if I disclose, what would happen? And we are generally, we are very concerned about law enforcement agencies because law enforcement agencies, not all law enforcement agencies are human rights

respecting. And sometimes they want to have access for nefarious purpose.

So that is what worries us. And so we wanted to discuss if you have any position on that or if you're discussing it at SSAC, because I think that cybersecurity researchers also want to have access to, want to use RDRS or whatever ICANN comes up with. So we wanted to know what your opinion is on this additional layer that registrars have to do before they submit the domain name registrant data to the requester.

RAM MOHAN

It's a good question. We haven't discussed this specifically inside the SSAC. So I'll open it up here for SSAC members to provide their point of view in their own capacities. I will say this from my point of view, with my experience with the contracted parties and what they have to do, my worry is that unless this balancing of fundamental rights is well-defined and has some minimal but global scope, my fear is that either registrars are going to interpret it in the way that is most beneficial for them or the least work for them. That's one thing.

And the other is that you're going to end up having a very uneven treatment of requests for information that come through. And I worry about that because I think you want to have the appropriate safeguard and some level of friction to make sure that these concerns are managed. But how do you do it at a global level with a registrar who is, say, in Russia, another registrar who is in another

jurisdiction in the United States, for example? That's where my concern is. And I worry that two things. One, it'll get bound up in an endless policy debate here inside of ICANN. And we'll be talking about this topic in another 20 years. But the other part is that when it comes to implementation, it will be very uneven and will lead to a poor user experience.

STEVE CROCKER

Thanks. I think this is the beginning of a extended discussion which we should schedule. But just to give sort of a preview or a teaser of things, I think your instinct that there needs to be another layer there is perfectly understandable. The challenge is, okay, then what happens in that layer? So let me cast it in slightly different terms. That decision that you're suggesting gets made by the registrar will fall into three buckets, in my view, in general. Either yes, easy to understand that that's okay, good, do it. No, absolutely not going to do that. Or, oh, that's complicated. We'll have to think about it.

And if that's where the discussion stops and we just say they're putting another layer, then we just have an unholy mess on our hands. There is no uniform solution, not going to be able to make a policy that is applicable worldwide in all cases. But you can make piecemeal policies. You can pick out pieces of that and implement those in ways that are more efficient for all parties and clear and give you comfort ahead of time as to what's going to happen. It's not really very helpful to have a system that says, well, you can

make a request, but we have to do this complicated test. And we have no idea how it's going to come out, so we can't tell you in advance whether or not this is going to succeed or not. That's just a not very helpful marketplace.

So that's kind of the elements from where I'm coming from of how to begin that discussion. And teasing apart what the elements of that decision are and where you can carve out pieces that you can answer firmly one way or the other will be helpful in a couple of different dimensions in terms of clarity, in terms of efficiency, and guiding people toward clarity in their thinking about things.

So let me just sort of fill in one blank. With respect to the human rights issue, and now I'm in your territory and not mine, but I'll venture there anyway. There are human rights conventions in various jurisdictions, and it makes a big difference, I believe, if you know that the other party is part of that convention and that may lead you to a positive decision more quickly. And if they're not, it may lead you to a negative decision more quickly. And having a system that allows that level of information to be known will be helpful, I suspect.

FARZANEH BADIEI Yeah, that is actually very helpful, Steve. I think that we should continue these conversations. And so at NCSG, we actually have these different projects for providing registries and registrars with certain human rights impact assessment tools, because we also want this to be standardized. And because we don't know how

they do their fundamental rights assessments. And we have a session on Thursday, if you're around at 3.30

STEVE CROCKER I'll be on an airplane.

FARZANEH BADIEI Yes, everybody, unfortunately. Yeah, you see, it's either overlapping.

STEVE CROCKER This is not a topic to be disposed of in a particular session or at a particular time. So we'll find a way to schedule some quality time.

FARZANEH BADIEI Absolutely. Thanks. Thank you.

RAM MOHAN Yeah, just for the record, I think this is, I agree, this is the opening of a dialogue and look forward to more discussions on this. And Rafik and Farzana, I think that is actually a, perhaps something where either you invite us into one of your intersessional meetings, or we invite you into one of our intersessional meetings. You know, we hold monthly meetings and we might be able to invite you to have a bit of a discussion with not just the few of us who are here, but other members who are there as well.

RAFIK DAMAK: You can take that also as an action item to follow up. Okay, good.

RAM MOHAN: Yeah, my goal is to leave all the action items with you.

RAFIK DAMAK: Don't worry. I will send it to follow up. Okay, so any more on this topic or we can go to DNS abuse. Trying to see if there is anyone in the queue. So should we go DNS abuse? I think it's a good time.

FARZANEH BADIEI: Okay, so DNS abuse. I'm going to be short about this because all of these topics are kind of like related to DNS abuse mitigation. But we wanted to tell you our approach to DNS abuse mitigation. We believe that like the sense of urgency that some stakeholder groups feel, we haven't come to an agreement in our group that there is a sense of urgency, but we think that the DNS abuse should be mitigated.

We have been providing, we have been having these sessions on DNS abuse mitigation and human rights. Because we believe that when mitigating DNS abuse, it is sometimes there are some risks to human rights that should be considered. Because of course, at the DNS, I mean, I'm in the crowd of the techies, so I have to be a little bit careful about what wording I choose. But so it can be very disproportionate when they take down a domain name that is not

that like falsely or it's a false positive. So and that person's access to the domain name can be blocked. And sometimes there are compromised or hijacked domains that the domain name registrant is not the perpetrator.

So we do the human rights impact assessment sessions we have in collaboration with the registries and registrars. And we did two sessions and we discussed different scenarios on what would happen, what the registrar can do to kind of analyze the assets, the human rights impact, and then mitigate that impact. So if they have to take down what sort of other remedies can they provide for the domain name registrant, if that is false positive.

So these are the conversations that we are having and it would be great to-- We also invite law enforcement agencies and others and it would be great to have a SSAC involved with those conversations as well so that we can come up with a framework or some kind of guidelines about how to mitigate DNS abuse while reducing the risk to human rights and access to domain names in general.

RAM MOHAN Yeah, we welcome that interaction with you. So far the dominant emotion in me after these conversations is there's much to learn about especially the human rights part of it and its interaction. You know, I've come at it often with either a technical mindset or with how does it impact the security piece of it. So I welcome the

dialogue and the collaborative learning that can come from it. So count us in with that.

FARZANEH BADIEI: And also you might have some technical solutions that can make the remedy a little bit like more proportional and you can bring that perspective because we are looking for solutions. We are not blocking the policies.

RAM MOHAN: Sorry to interrupt, but that, Farzana, might be actually the headline, if you come to one of our monthly meetings and we have an interaction, that might be the headline that will help bring engagement from our members to work on this topic because it's DNS abuse, but it's an aspect that hasn't had too much discussion inside the SSAC. So I would suggest that that might perhaps be the first topic that you come in to discuss with us.

RAFIK DAMAK: Yeah, first let's see if there is any comment or anyone in the queue. Yes, so just to be mindful on time, we have, I think, how much, 20 minutes left. So we can go to the next topic and after maybe any other business to wrap up.

So the next topic about DNS blocking, because as shared at the beginning, it's about the report. Not sure everyone on our side could read it, but even if you can give a quick overview, and then

maybe I think it's more like not an NCSG position. It's really, I think we'll ask our member further thought. I think Farzan and maybe Pedro, it's more maybe question or comment, but if it's possible, just really quick overview or highlights, because for me, one question, why talk about DNS blocking right now? Because it's something that happened for so many years. So just to understand the background and what may be the main outcome from this report.

RAM MOHAN

Sure, thank you. The SSAC has written about DNS blocking years ago, and we recognize that it's a well-known topic. So it's a good question. Why now? Why do you have a new report out? Part of it is, really, there are two parts of it. One is that technology has changed quite a bit from when we wrote our report then to where things are now. That's one part. The second is that the state of play is quite different. There are some jurisdictions that have rules now about the use of VPNs. There are certain jurisdictions that have specific requirements that are now laws that are based on national security and providing rights for governments or other people in authority to take actions. That's one part of it.

On the technology side, there has been quite a bit of evolution. If you look at, for example, the resolvers, there are now public resolvers. You look at Google's public DNS, 8.8.8.8, or you look at CloudFlare's public resolver at 1.1.1.1 or Quad9, the 9.9.9.9 resolvers. Those now are a firm part of the global internet

resolution ecosystem. Even in places where blocking exists, if you configure your systems to go use those public resolvers, then you have ways to circumvent. You look in the EU, there's a government-sponsored resolver. DNS for EU is, again, something new that has come through.

Our question was, when you look at DNS blocking now, we wanted to clearly point out the collateral damage that comes through with overblocking. In our report, we have some examples. Italy has a piracy shield. That piracy shield requires internet providers to automatically block domains that are designated by their telecom regulator as piracy sites. That's a requirement. They do that. It's a law, so they do that. In 2024, October, when they did that, they blocked a Google domain name when they did it. And for several hours in all of Italy, users in Italy were unable to download files from Google Drive and couldn't access YouTube. That was collateral damage that was overblocking, that happened there.

The second thing is that it's actually often, it just doesn't work. It's often ineffective. It's a matter of degree, because you have alternate resolvers, there are VPNs, there are other technologies that have come through, and that's a second thing. The third, which we think is quite concerning, is that it actually may weaken security. Let me give you an example. You're at someplace, and you try to access the internet, and you get a pop-up. And the pop-up says, you're trying to access a site, the certificate for the site does not match the site that you're actually going to. Are you sure you want to go through? And then there's a little button that you

can click that says Advanced, and then you click on that button that says, yes, go to this insecure site.

What you're doing now is you're training users to ignore a legitimate security concern, a legitimate security problem. Just so that you can access the site that you want to go to. And that pop-up came about most likely because there is DNS blocking of some sort going on. So that's why what we recommended in this report is if you're an entity that is implementing DNS blocking, understand what the implications are.

Because you have unintended side effects, there are unintended consequences. Or if you're an agency or an authority that is going to mandate blocking at the DNS level. recognize that sometimes you can say, it's not even at the DNS level, we're going to block it at a domain name level. But imagine if you blocked something, a domain name that has underneath it a whole bunch of subdomains that depend upon it. So there's a great deal of education that has to self-education that has to be done. So that's an important thing.

The second thing that we're saying is that we have come up for the first time, we've come up with a set of four guidelines for any entity or organization that intends to block. That's a change, Rafik and Farzana, from what we did last time. Last time we said, this is dumb, just don't do it. Now we're saying, okay, world's moved on, people are doing it. So if you're going to do it, here are things that will at least avoid some you shooting yourself in the foot. So that's the second part of what we've said.

And the last part is there's actually some work that has been done that allows at the protocol level in the DNS, today if a site is blocked, you'll often get one of three responses. One is you just automatically redirected somewhere else. Or a second is you get a response that says, you are blocked. Or a third is it says, it's just, you don't have access, your request was just dropped on the floor.

So there's a DNS extended error code that has been created that allows for a response to come back that says, access not allowed because it's censored or something like that. So we're saying, hey, recursive server operators ought to consider implementing the extended error code so that they can accurately state why they're not providing a response for a legitimate query.

So it's a practical approach to reality in the world today. We're not endorsing DNS blocking in any way. So when we're putting out guidelines, we're not saying, oh, here is what, here is how you should implement DNS blocking. We're actually saying, in general, it's actually a pretty ineffective mechanism and it's often an overreach. But if you feel compelled to do it, at least do it in a way that is going to cause the least harm.

RAFIK DAMAK Thanks, Ram, for this overview. I asked about the timing and thanks for clarification, but also, I don't know, it's just maybe the coincidence because I saw also the report from the Internet Infrastructure Coalition. They had something about what they call, I think, DNS at-risk or DNS fragmentation. So I think maybe it's just

interest for everyone. Just that's why I was wondering what's going on, why we have two report, maybe on the same topic, but yeah, still relevant.

RAM MOHAN Genuine coincidence, we didn't coordinate with them.

RAFIK DAMAK There are three reports, sorry. Go ahead.

FARZANEH BADIEI Excited to tell you about my report on that. So yeah, I know DNS resolvers are becoming very critical because of all this search. So I did a research which was funded by the Digital Infrastructure Fund. And so I looked at, if centralization of DNS resolvers was happening and if it's happening, why it's happening. So, and in the midst of the research that I was doing, one of the reason that people don't provide public DNS resolvers, and we have just like a few that are trusted. One reason is that there are just too many regulatory frameworks to comply with because the nation states have, like there is this surge in nation states to block at the DNS level.

And I also looked at the internet freedom and how public DNS resolvers were used or if they were used during like political uprising or during elections. And so that's another thing that I looked at and it was interesting. I call it Jeff data, what is the

APNIC's DNS resolver and it has like a really great data that you can see the usage of the DNS resolvers by the ISPs and others.

One thing that I was involved with at RIPE NCC, there's the RIPE task force on best practices on DNS resolvers. And we finished that work and we actually worked with Martin, I think Martin. So, that group also came up with a few recommendations on better transparency and some technical recommendations. And also if you have block lists, how do you keep that block list updated so that there are not like many false positives. And I also looked at quad9 and others. The data analysis part of this was done by .ie so we worked with them to that.

DNS resolver and the infrastructure level blocking and censoring is becoming very prominent in conversations. And I really, really appreciate that you paid attention to it, and this report is great. We need to do some kind of collective action to also inform the lawmakers because sometimes they just don't know what sort of facts. They're like, yeah, I know.

RAM MOHAN

Yeah, I agree with you. In fact, yesterday we had a conversation with ICANN's government engagement folks. And we were saying, hey, we have a report, and we think it's on DNS blocking, and its prime audience is actually policymakers, but we have no access to them or we don't know how to get in front of policymakers so help

us do that. And so they've said they will consider our request to help get in front of them.

Because the consequences, I mean, in the US several years ago, there were other misguided attempts to do blocking and things like that. We were able to help push back on that. But it's now become standard operating procedure across the world. Some kind of blocking is assumed everywhere. And the other part of it is that users have started to become used to, oh, their access to the internet is likely to be not just monitored but regulated, blocked. So we're moving to that era, and that's something to really be noted.

RAFIK DAMAK Yeah, unfortunately, bad ideas die hard. So I think we have Pedro, Bruno and then Manju.

PEDRO LANA Pedro Lana for the record. Just a quick one because when I already answered the first question, I was going to ask if you had any info about how governmental agencies are reacting to reports considering that we have a rising of those blockings on many regions, including Latin America. So there is a normalization of how this is happening and what they were asking is exactly this approach that we had. Oh, so if you were saying that we can't do that but we need to do that. So how to do that in a minimizing way of how the effects are going to last.

And the second part is that if you have any study or recommendation about some of these policies, they just say about requisites to block but they don't say nothing about the permanency of those blockages. So what you can see is a lot of internet resources that are blocked by those agencies. They kind of stay permanently blocked until they arbitrarily think this needs to be changed and there is no recommendation at least that I have seen anywhere about having a temporary order regarding blockings.

RAM MOHAN

You're right. Sometimes there's a lot of attention and zeal in the original blocking orders, but then once that whatever situation resulted in that goes away, there is no cleanup of that that happens. And over time, you end up having systems that just have more and more sets of pieces of the DNS that are just inaccessible in some cases for poor reasons.

And the consequence, the side effect of that is that users are going to want to get to those sites, are going to go deploy VPN, they're going to go deploy these other technologies that are available. And it kind of makes it somewhat futile at the end. I mean, I know in some jurisdictions, they have now said either VPNs are banned or only known VPNs are allowed. And which is to some extent an oxymoron. But even in those jurisdictions, you find that users end up circumventing those kinds of rules.

MANJU CHEN

I want to say I really appreciate this report because in Taiwan, the TWNIC, they're doing the same thing. They have this thing called DNS RPC, which is basically DNS blocking, and it's purely a response to government trying to take down websites. And the same thing actually happened in Taiwan where there was a morning, all the Instagram, YouTube, whatsoever are down because they took down blocking the wrong DNS, whatsoever domains.

And we have discussed this on one of the committees of TWNIC too. I will definitely share this report with them and advise them to follow your recommendations. But yes, I agree with the previous discussion where we really have to educate the government more about this because most of the time, they're just asking to take down things. They don't care what you do. As long as they see it's down, they feel very good. But yeah, and I wonder if you have been having these discussions with the CCs because a lot of them kind of just do things in response to the local authorities. Maybe this is something they should take into considerations when they're responding. Thank you.

RAM MOHAN

Thank you, that's good advice. And we do intend to engage with the CCs. We have spoken with the GAC about this and our intent is

to engage with each of the communities on this topic. It's an important topic for our times.

RAFIK DAMAK

Okay, I think we did well in term of time and then we can end up the session for today. So thanks again for joining. It was good opportunity for us to discuss on several topic. For me, what I can take from this, I understand that we can follow up and tell maybe intersessional. We don't need to wait till Oman meeting. So we can maybe the sum of topic we discussed that we can organize and schedule, use your monthly calls for that purpose. So we'll handle that.

And also I am looking forward if we can have now this regular meeting. We will see if we can have it every ICANN meeting, but also we need to work what kind of topics or what type of engagement or dialogue you want to have. And looking forward, we can have this continuity because at the end, it's not just about to discuss for the sake of discussing, but we can share some input and hear from you from what you are work on and to try to find some synergy and try to build on top of that. So thanks again. And I don't want to keep you all from your lunch.

RAM MOHAN

Thank you so much, president. Thank you so much. I agree. This is about impact. This is not just about conversations, but impact

	begins with conversations. I'm glad we've started it. Look forward to more.
RAFIK DAMAK	Thanks everyone. See you later. We can close the meeting for today.

[END OF TRANSCRIPTION]