ICANN86 Seville | PF – GNSO: NCSG Policy Committee Work Session (1 of 2)
Monday, June 08, 2026 – 10:00 to 11:15 CEST

ANDREA GLANDON

Hello and welcome to the NCSG Policy Committee Work Session 1 of 2. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct Concerning Statements of Interest.

Please observe the following guidelines to participate in this session. I will also post them in the chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during this session as time permits and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. And I will now hand the floor over to Farzaneh. You may begin.

FARZANEH BADIEI

Thank you, Andrea. Hello, everybody, and welcome. So, we are the Non-Commercial Stakeholder Group. We care about human rights, access to domain names and a host of human values. And at ICANN, we try to infuse those values. We care about registrants and users in general and access to open internet as well. But most people here know us. That's great. And I am the policy committee

chair of NCSG as well as representing NCSG on the council, the GNSO council.

Today, we wanted to cover two topics. One on remedy mechanisms for domain name registrants when things go wrong. And another is the topic of authentication of law enforcement, which is happening at ICANN at the moment. And there are many discussions and these are the issues that we deeply care about because we care about human rights. And I just remembered I forgot Benjamin's books.

Okay, so now for the remedy mechanism, why do we have this agenda item? As you know, we are talking about DNS abuse mitigation and we have a policy development process that is working on associated domain checks. Associated domain check is about, so they want to obligate the registrar to look at the, like if there is a DNS abuse, if there is a domain name that has been involved with, that has been registered maliciously and been involved with DNS abuse, they want to obligate the registrar to check if that domain name and the registrant is involved with other abusive domains. And so that has a host of issues. We were not happy that they wanted to work on it in this way. We think that it creates a cultural surveillance and also it's bad for privacy. It is also bad for access if something goes wrong.

In that group, we are discussing the safeguards that we can have so that ADC can be carried out with minimum impact on the domain name registrant and access to domains. We are not really winning

the fight for safeguards at the moment, but we should not back off, obviously, we should not back off and talk about safeguards and having safeguards in place. But there is another important thing that we deeply care about is if things go wrong, we need to have remedy for the domain name registrant who has been implicated in some kind of DNS abuse mitigation as a result of the associated domain check.

So we have been discussing what sort of remedy mechanisms we can have for the domain name registrant if things go wrong. And the different parts of the community says that no, we don't want to have remedy as a part of the ADC and we want to talk about remedy for domain name registrant in general.

And I personally don't agree with that. I have been involved with policymaking in different areas of digital governance for a long time, and it is a standard to when you do policy, you do detection, mitigation, enforcement, and remedy for every policy that we come up with. But since we are not winning that fight either, we are going to see if we can push for a PDP on remedy, but still talk about the remedy in associated domain check.

In order to set the scene to come up with that PDP, we need to know what sort of remedy mechanisms are already in place and what the registrants usually struggle with. And this is why I have invited ICANN compliance, Leticia, to tell us what are the different means of providing remedy for the registrants. And without further ado, go ahead, Leticia.

LETICIA CASTILLO

Thanks, Farzaneh. Hi, everyone. My name is Leticia Castillo. I am a senior director with ICANN contractor compliance and here today with my colleague, Amanda Rose, who is the senior registrar compliance lead.

We prepared a very brief presentation based on the feedback that Farzaneh sent us about what type of information we would like us to present today, specifically to put the topic of what remedies currently exist in the agreements for registrants into the context of what ICANN compliance does. So we expect this to be interactive. So a question at any point, like I said, we want to be brief and try to cover what Farzaneh shared that would like us to share. So I'm going to hand it over to Amanda.

AMANDA ROSE

Thank you, Leticia. We can go ahead and jump in and just go to the first slide. Here we have a breakdown of the registrant rights and responsibilities specification that's found in the RAA. So this provides information that registrants are entitled to, that they have a right to, and lays out specifically what registrars must provide. So primarily they first have to enter into a registration agreement for all domain name registrations. Registrants are entitled to always have access to those terms and they must be able to download it and view it at any time.

Secondly, registrars have to have available information that is accurate, which allows registrants to have set their expectations and to make informed choices regarding their domain name registrations. I'm getting a lot of feedback. Okay, keep going. Okay, that's a little bit better, I think.

So namely, they have to know who is their registrar and any privacy or proxy service that is provided through the registrar as well. They again have to have the terms of the registration, including pricing information regarding the registration. All registrars must make available how they can resolve disputes, how they can raise concerns with their domain name registrations, both for the domain name itself and any privacy proxy services as well.

And lastly, under the spec, they have to be able to have information that explains their processes for being able to manage their domain name, transfer, renew, and restore domain name registrations. Sorry, that is lastly. The registrants have the right to not be subject to false advertising, deceptive practices such as deceptive notices, hidden fees, and illegal practices. We can go ahead and move to the next slide.

So under the RAA, this is not the specification, but under section 3.77, it lays out what must be included in the registration agreement. And there's several specific terms that are required to have in every registration agreement for every domain name registration. So I know that part of the ask was specific to data protection. So we pulled out some of the main provisions that

apply to the data protection requirements that have to be in that registration agreement. So they have to inform registrants about the purpose for the data collection, intended recipients, what's mandatory, what's voluntary, and how they can access or correct their data.

Next, they have to agree that it will, or the registrant has to agree that it will not, I'm sorry, the registrar will not process the personal data collected from the registrant in any way that is incompatible with the stated collection purposes. And the registrar must agree that it will take reasonable precautions to protect personal data from loss, misuse, unauthorized access, or disclosure alteration or destruction. And then on the flip side, the registrant must consent to the processing of their data and confirm that any third party whose personal data is supplied to the registrar by the registrant has received the required notice and provided consent.

And then I know another question that you had was specific to resellers. So there is provisions that pass through these requirements that if the registration agreement is entered into with the reseller, that still has to carry through to that registration agreement, whether or not it's directly with the registrar or with their reseller.

FARZANEH BADIEI Let me just like explain. Sorry, I thought that request for data protection was a little bit late and you may not presume, but thank you so much. The reason I also ask for data protection clauses that

they have is that in DNS abuse in the ADC, we are working also on what sort of impact ADC could have on registrant privacy, if it could have any kind of impact. And that's why I wanted us to look at what sort of data protection clauses we already have in the contracts that could reduce that impact, the potential impact on the registrant's privacy at the ADC. So that's why you kindly went over that. Thank you. Do you want to, are you done?

AMANDA ROSE

I'm done with the two slides I was presenting. So if there's any questions on what I've just presented, feel free. And then we also have two more slides to get into some specifics. Yeah.

LETICIA CASTILLO

We can go to the next slide. This is Latifa, I can see you again. I'm sorry for the record. So now we're going to put, we're going to give some more examples about what type of remedies can registrants seek through our complaint submission form based on actions or inactions by the registrar. As we all know, ICANN contractor compliance can only enforce what it is in the agreements. We cannot enforce laws, we cannot enforce regulations, we cannot enforce the terms of services of a specific registrar, just what is in our policies and agreements. So some of the examples are regarding the suspension of domain name registrations.

As Amanda mentioned before, there's the obligation for the registrar to provide those terms and conditions to the registrant so

they know what to expect and make informed choices. They also need to agree to that agreement. It has to be executed by agreements. So basically they need to know if you engage in this activity, the consequence could be the suspension of domain name and or determination of the agreement. And what we cannot do is we cannot evaluate the suspension itself or require the registrar to lift that suspension when it is completed after the investigation and in accordance to their own terms of service.

And to put this in a little bit of context, this is not a high volume complaint type for us. We do not get a lot of complaints where registrants say my domain name was suspended, I didn't agree with it, I don't understand why the registrar did this. And this was like this before the DNS amendments and has continued after. Some data points. So the year before the DNS amendments became effective, which was April 5th, 2024, we initiated about 34 investigations with the registrars regarding the specific requirements.

Again, we were not evaluating the suspension itself, but you know that the registration agreement existed, that the registrar was informed, that the consequences were consistent with what their agreement said it would happen. During the two years after the amendments, that number was 60. So it is very consistent. First year before, 34, two years after the amendments became effective, 60. So it's very consistent. It's not a high number. We're not saying this is not happening. We're just saying that this is what we're seeing in our complaints, the cases that come to us, we have this

visit, this is limited to the complaints that we receive in the enforcement actions that we take. So let's go to the next slide. Or do you want to, questions here?

FARZANEH BADIEI

So we can all ask questions. Don't let me go on and on. So, when you say that you cannot require the registrar to lift the suspension, even when the registrar has suspended the domain name wrongfully, like it's a false positive DNS abuse?

LETICIA CASTILLO

Thanks for the question. So what we're saying is that we are not party to the agreement between the registrar and the registrant. Therefore we cannot evaluate how those terms of service have enforced after the registrar completed a, they provided information like reasonable investigation and determined that their terms of service have been violated and they have enough information evident to take the action that the agreement warranted. We don't have contractual authority to evaluate that.

Now, for what we have seen in the cases, again, limited to the cases, the very few cases where there was determined a false positive, after receiving that information from the registrant, the registrar has lifted the suspension themselves. So again, we have not seen that in the cases, but we cannot evaluate how a registrar enforced their own agreement with their customers. So long as all the actions that we are seeing are compliant with all relevant

requirements and everything adds up, there's a reasonable explanation, there's evidence, yeah, we cannot.

MICHAELA SHAPIRO: Hi, Michaela Shapiro for the record. Thank you so much for this presentation. I had a question about how you evaluate whether a registrar has a process for how to raise disputes. Like are there specific criterion that you have in place? Like how do you go through that process of assessing? Thanks.

LETICIA CASTILLO: Thanks for the question. So there are two different avenues through which we will address and enforce that requirement. If in any complaint we have information suggesting that the registrant didn't have access to the information, we will ask the registrar, this is an obligation you have to provide your registrant with this information, where is it, what evidence of it is provided. We also have the audit where we do a different type of evaluation. We have our questions and requests for records that we request from the registrar. So that is also not triggered by someone or individual registrar, but more again as a whole check of compliance.

MICHAELA SHAPIRO: Michaela for the record, a quick follow-up. So would that look like, does it have to be in the terms of service? Is it just about availability and kind of somewhere easy to find on the website? Like I guess I'm thinking about that criterion a little bit more specifically.

LETICIA CASTILLO

This is Leticia for the record. Thanks for the questions. It's normally on the website, but there's no requirement that has to be on the website. So it has to be the requirement, it has to be accessible at any point, at any time, and it has to be up-to-date and accurate, but there's a requirement that has to be a specific place for the registrant to. That's why we were normally asked for it, because we perform that check, sorry jet lag, but sometimes we do need to ask them.

FARZANEH BADIEI

Thank you. So there is no requirement even after suspension, so the registrar tells the registrant that we suspended your domain, but here is where you can go and complain. Is there a requirement to do that?

LETICIA CASTILLO

This is Leticia for the record. They have to have information on how to raise disputes and complaints related to customer service and other to the registrant available in general, and that's how that normally happens. There's no requirement for a registrar to say we have suspended a domain name and this is the reason why, specifically said every time, and this is what you need to do with this process to provide us with information to remove that.

However, again, what we have seen is that registrar do normally do it, like they say if you provide us with this information, we're going

to review the case again. Normally, doesn't happen with malicious domain name, clearly registered for the purpose of conducting DNS abuse, but we have seen in the cases that registrant do that.

FARZANEH BADIEI Thank you. So are there any other questions? Leticia, so you don't have, you don't receive many disputes and many complaints. Could be that because registrars are mitigating and responding, but could it also be because the registrant might not know they have that avenue of, like, how is like the registrant awareness in this?

LETICIA CASTILLO Thanks for the question. This is Leticia for the record. We cannot speculate. We really don't know. Like, abuse, DNS abuse is a number one in volume. We get a lot of abuse in DNS complaints and it's over, I would say, around, like, legally, like, almost 2,000 new ones a month, whereas this type of complaint where the registrar may come to us and say the admin domain name has been suspended and I don't know why or I don't agree with this, which can be DNS abuse, can be other violation of the terms of service, doesn't have to be specific for DNS abuse. It certainly has been very low and continuously low, but we cannot really speculate on why.

FARZANEH BADIEI Yeah, thank you so much. So, if there are no other -- so, as I said, like, the reason that we are having this meeting is to think about

how we can work on a policy that is holistic and provides remedy mechanisms and builds upon the already existing remedy mechanism. And also the thing that we should also focus on is what sort of contractual, what sort of power the compliance has and what we want to see. Like, for example, I see, I think that in certain situation it might be good if ICANN compliance could require the registrar to lift the suspension. But that's something that we need to discuss among our group and then see what we can recommend. Yeah, go ahead, Benjamin.

BENJAMIN AKINMOYEJE Good morning, my name is Benjamin. I want to assume in this room there's no stupid question. Okay, so, does this have anything in shape or form or effect to do with URDP? Does it? Because we've looked at some URDP files where disputes, I mean, IP violations, and most of them were done in English.

So supposing you don't understand English and you don't even have enough time to challenge some of those disputes, conversations, how do you ensure that the people in violation know about these issues going on and have enough time to raise objection or to say, no, that's not actually what is happening, or give their reasons why they might have seemed to be in the wrong?

LETICIA CASTILLO Thanks for the question. This is Leticia Castillo. Again, this is, again, it's speculative. If I've understood your question wrong,

please let me know. We do not know it is because there is a duration that they don't know what the information is up there. We don't know if it's a language barrier.

There are certain requirements in the agreement that say, well, they need to provide notice, not a specific scenario, they need to provide notice to registrar that need to be at least in the language of the registration agreement they enter into. So we do not know if the language can be a barrier. It could be that's information that we don't have to give you an informed opinion in that regard.

FARZANEH BADIEI

But that's an excellent point. I think that we need to do a little bit of research and see how registrars that deal with Domain Name Register and that English is not their first language, how they deal with them, how they can complain and what, like, if they have access, and because I guess that the complaints have to be in English, right Leticia?

LETICIA CASTILLO

Thanks. they complaint to us? They don't have to be in English. We mainly receive complaints in English, and we address it. We sometimes receive complaints in other languages, and we have different people in the department that can address this as well. And we know we need to do a better job at this and continue working on it.

For example, last year we published a guide to submit valid, well, actionable DNS service complaint to ICANN. We wanted to do something that was, like, user-friendly, not a lot verbose, like, clear and specific about what we need, and we published that in English, in all UN languages, plus Portuguese. Our complaint form, the main form is in all UN languages. The individual complaint forms are not yet, but that's something that we continue to work on, because we really want to make sure that we make ourselves available for different languages as well.

FARZANEH BADIEI That's great. So we need to look at registrar's practices and see how they communicate with their registrants, because, like, you know, if you don't know English and you receive, like, an email that, yeah, you can complain through at ICANN about this decision, then that's kind of ineffective. So that's a really good point.

Oh, yeah, actually, I forgot. There is a question by Francis Ojeifo. ICANN compliance does not evaluate a registrar's independent decision to suspend the domain under its own terms of service, nor does it have the authority to order a registrar to lift such a suspension.

Okay, so I don't see the question there, but, okay, let's move on to the second comment. Francis, if you can raise your hand and explain as well, that would be great. So second comment is contractual validity. Registrars must legally bind registered name holders to their TOS during registration. Okay, so, yeah, these are

the things that we have discussed previously. Francis, I encourage you, like, if you have questions or comments about this, raise your hand.

Okay, so let's move to, how much time do we have? Do we have another 10 minutes, maybe, of your time? Okay, because I really want to move on to the data protection because that's really important for us, and also I want to know if, if we have, like, can the registrant come to you and say, I think that my privacy was like, there was not enough data protection, and my privacy was violated. Can they do that?

AMANDA ROSE

So we don't have specific requirements to address their individual issues directly with their registrar. So if they have those obligations that need to be in the registration agreement that I went over in the first or the second slide, we can ensure that those are actually in there, but can we enforce those with respect to that agreement between the registrant and the registrar? The answer would be no, because that is not within our contractual scope.

We do get complaints, very limited, that do sometimes have those such allegations, and we provide resources for how they should escalate that and where to, who to contact generally, because we don't know if it's a specific, everyone has different jurisdictions and different protection agencies that might apply to each individual

registrant in that case. So we would suggest that they escalate to the appropriate authority or their registrar itself.

FARZANEH BADIEI And what if they don't have a data protection authority or any kind of law that could protect them?

AMANDA ROSE Again, we're limited to what we have contractual authority to enforce, and that would be specific to each jurisdiction, like you said. If they have that available, obviously that would be the correct escalation path. If not, to pursue whatever legal remedies may be available. Unfortunately, there is none. That is not still something that we can step in and fill those shoes of.

FARZANEH BADIEI So I really wanted this point to be made because we are working at a global scale. We care about every registrant in the world, regardless of where they are. And as we know, privacy and data protection laws are different in different parts of the world and in different countries, and sometimes they don't even have that kind of protection. I still think that we need to provide them with a minimum privacy and data protection, regardless of where they are.

And I was thinking that maybe we can do a little bit of mapping and see how ICANN contractual obligations for data protection can help those registrants that are in jurisdiction with weak data protection

laws to protect themselves and also be able to seek some sort of remedy or recourse, even if they don't have a data protection authority in their country.

And let's not forget that the registrar usually is serving different countries, but it's usually based in countries that could have strong data protection laws, such as Europe and not the U.S., really. No, I'm kidding. We do have data protection in the U.S.

And so I just want us to think about what sort of minimum contractual obligation we want to have, what sort of standards we want to have in the obligations for the registrar, and what sort of enforcement power we want to have for ICANN to help meet the minimum of data protection for everyone in the world, in terms of being able to complain if their privacy was violated and stuff like that. All right. So are there any other questions?

ANDREW CAMPLING

Hi. Andrew Campling, 419 Consulting. Just a thought. Is that really a problem? If I'm in a country with weak or even no data protection, what's stopping me from contracting with a registrar in an alternate jurisdiction, say under GDPR, for the sake of argument? So would that be a lot less complex than trying to construct some sort of data protection contractual obligations? It might be much simpler for people to make sure there's information available so people could choose where to contract.

FARZANEH BADIEI

So actually, the registrants have been doing this all along. They try to choose a registrar based in jurisdiction that have data protection obligation as well. It's just that registrants, sometimes they cannot do that, or sometimes they deal with resellers and they don't directly deal with the registrar.

And if something happens, I don't think that they have the means to go to the data protection authority of the jurisdiction of the registrar to hold them accountable. So if my data has been leaked or it has been disclosed unfairly to a law enforcement agency and I am based in country A that doesn't have any data protection, but the registrar is based in country B, do you think that I can go and complain to that, the jurisdiction B? Go ahead.

ANDREW CAMPLING

So I am not a lawyer, but I'm pretty sure if I contract under a named jurisdiction, then the laws of that jurisdiction apply to both contracting parties. So I'm not sure what you said is correct, but there may well be lawyers here that are better qualified.

FARZANEH BADIEI

I am a lawyer, by the way, Andrew. And what I'm saying is correct, because what I'm not talking about is the matter of like, yes, of course, they can go, but no domain name registrant is going to just go all the way to another, unless the registrar actually provides them with some sort of avenue to make a complaint. That is online. Yeah, go ahead.

TAPANI TARVAINEN Yeah, well, I guess in practice, the issue is that when you are registering a domain, it may not occur to you at that time to look for a country or registrar that does it correctly. And when you are in trouble, it's too late. So that's why we should have it in for all registrars.

FARZANEH BADIEI We need to have the baseline. Okay. So I wanted to ask this specifically. So I understand that registrants can't come to you and complain about the privacy issue that they have. Compliance-wise, after GDPR and after the registration policy that went into effect, how do you actually enforce these privacy policies that we have at ICANN?

AMANDA ROSE And is your question specific to, I know you referenced in the email, section 5 of the registration data policy. Okay. So under section 5, it requires both contractors. Go ahead.

FARZANEH BADIEI So I'm interested in section 5 because it's about the resellers, right? No, it's about the agreement, the data protection agreement. Yes. Go ahead.

AMANDA ROSE

So yes, that is the section of the registration data policy that covers what agreements must be in place with respect to data protection. So essentially it says all parties, whether it's ICANN, registrars, registries, they must have data protection agreements in place if applicable law requires. So all of those are dependent on each individual assessment of whether that protection agreement is necessary. With respect to ICANN and contracted parties, we have a data protection specification available that they can request to enter into with us if they determine that it's needed for data processing.

So again, it's dependent on their individual jurisdiction. So with respect to the contracted parties agreements with each other, they also have to enter into agreements between the registrar and the registries that transfer data and process data if they determine that there is actual transfer of data that's going on. Under some more commonly, they're shifting away from sharing data and transferring personal data.

So a lot of registries have gone to like a thin type model where they only transfer the technical data in that case. DPAs are likely not going to be determined to be necessary under applicable law when they're not processing personal data for those registrants. When there is that transferring, that is dependent on the contracted parties establishing that they need a legal basis for transfer and then putting those data protection agreements in place.

Now, we don't get complaints about this. We thought about this during implementation. How would this be coming into us and how would we receive complaints? Probably not very likely for an individual to say, does my registrar and registry have these data protection agreements in place? So how we envision that would be through registrar audit or registry audit, asking specific questions. Did you make that determination that there is legal basis or that a data protection agreement is needed? Is there a transfer of data in the first place? Those types of questions would be fleshed out through the audit. I hope that helps.

FARZANEH BADIEI

Yeah, absolutely. It helps a lot. So, I have this dream that instead of looking at each jurisdiction and have a data protection agreement, if there is a need in the jurisdiction, in the specific jurisdiction, to have a data protection agreement in general based on standard privacy and data protection. A policy that we globally have, like OECD has one and there are other global privacy standards that we could use, but that is not like the compliance job.

But I just wanted to show you where the gap is and if we want to address that. And we've been talking about this for many years and we've done a really good job of providing minimum privacy for the registrants, even in jurisdictions that they have weak data protection.

But we can do more and this is something that we need to discuss. But also in light of the ADC, we need to see if we need more data

protection measures during the PDP and do a data protection impact assessment. And our job there is to go beyond jurisdiction by jurisdiction, whether they have GDPR or not. Our job is to see what sort of minimal privacy standard we can have so that the registrars can get audited on the standard rather than just what their jurisdiction requires them to do.

Yeah, you're all so excited about my idea. I mean, it's not just my idea. My civil society has been working on this for many years. But yeah, this is something we should keep in mind. Any questions from our guests? No? Okay. I have one last question.

Sorry, I'm an ICANN obsessed person, so I spend a lot of time. When we were in the transfer review policy, we were discussing the reseller and the registrar, kind of like what are the data protection obligations that the reseller should have. And we were told that there is enough measure for the reseller to be obligated to protect the data. And also like during the transfer as well, as well as in general. Do you ever receive, how do you audit that?

AMANDA ROSE

So I would presume the discussions were centered around the reseller obligations under the RAA. And then if you need it, the section 3.12 has all the pass-through obligations that would apply what needs to be in the reseller agreement between registrar and reseller, if they have them. And then also mainly the provision that the registrars have to ensure that if the resellers are providing

registrar services on their behalf, that whatever services they provide, they do so without making the registrar out of compliance.

So every obligation that the registrar has under the RAA or any ICANN consensus policy, the reseller must fulfill if they are stepping into the shoes of the registrar. Now, ultimately, compliance is on the registrar. So we have to go through registrars. We don't have contractual basis to enforce anything against resellers as they're not our contracted parties. But we do enforce those obligations through 3.12. Yes, audits as well. We check the reseller agreements, make sure all the provisions are in there, and then, yeah.

LETICIA CASTILLO

Can I add something really quick? This is Leticia for the record. Through audit but also through external complaints, like let's say for another contract obligation, we get a complaint about a registrant that is trying to renew the domain name and pay for the renewal, and it's about to lose the domain name because the reseller is not taking the steps to renew the domain and comply with the consensus policy.

So that would be also a scenario that is a common complaint that we get where we would enforce the obligation with the registrar even though the actions are being taken by the reseller because they need to comply. The registrar is responsible for the provision of register services in compliance with the agreement and the

policies regardless of whether the registrar is providing directly or through a reseller.

FARZANEH BADIEI

Thank you so much. So the reseller is very important for NCSG especially because we care about registrants everywhere, but the majority of people who are based in the global south, they use generally resellers to register domain names. And it's very important that we consider that in our advocacy, in our policymaking, to make sure that the reseller protects their privacy and also is in charge of taking measures when things go wrong.

Okay, well, I have asked all my questions. Thank you so much. Any other comments? Anybody? Nobody? All right. Great. Thank you so much. Right.

So the next one, we are going to talk about authentication of law enforcement. This is very important for us because of the human rights implications that it could have on the registrant. People get prosecuted, they get wrongly imprisoned because of their political opinion, and we need ICANN to really consider these issues when coming up with authentication of law enforcement or different systems.

I wanted to talk to you about, and I'm sorry I didn't prepare slides for this, because we had this major meeting yesterday about SSAD, and we talked about authentication of law enforcement, and I just wanted to do a briefing on what went on during that meeting and

where we are at. And you will tell me what we should be doing in that group.

So around eight years ago, when GDPR came into effect, the domain name registrant private sensitive data was fortunately redacted from most of the registrar WHOIS. Not all, because not every registrar is obligated to follow GDPR, so people use privacy proxy services. But it's helped quite a bit.

But as a result, they kept saying that WHOIS going dark, and you know, they need also disclosure of domain name registrant private sensitive information to the legitimate interest holders. So who are these legitimate interests? And this is a provision by GDPR. Legitimate interest is if you have an intellectual property dispute and you need access to the personal information of the domain name registrant, or if you are law enforcement doing some kind of like public safety work.

So eight years ago, we had to come up with this kind of like disclosure mechanism at ICANN. How does it look like? How is it going to happen? And for a while, the group came up with this mechanism called SSAD. And I don't know what the acronym for that is. Can somebody remember? Yeah. So this was a mechanism for having access, like requesting the registrant data and receiving it from the registrar. But when they were at the implementation phase, they saw that the system they had come up with was going to cost millions of dollars to build and sustain. So they decided to come up with a pilot that they call like RDRS. Yeah.

So SSAD is System for Standardized Access Disclosure. Yeah. So they came up with this triage system called RDRS, which is the Registration Data Request System. Wow, I got that acronym right. So the RDRS, the only thing that the RDRS does is that it triages the request to the registrar that has opted for this, for the system. Because it was a pilot, they didn't make it obligatory for all the registrars to opt for it. And they wanted to test it out. So it's been two years. And that system was, like the pilot project was also extended for another two years.

But as a result of what we learned when we had that system in place, we learned that we need authentication mechanism. We need to come up with some kind of accreditation or authentication mechanism that could help with the registrar understanding where this request is coming from, who is it from, who is behind the request.

Because at the moment, the system is just like you just go and you sign up, you give your email, and that's it. You're just subbing to request. So especially this authentication became very important because the Board, and I have told you this, we actually, like, we were not quite sure. We didn't want the urgent request to be approved and be included in the policy in the form that it is now. But that's not, like, we, again, lost that battle. So many lost battles. But we won a lot, too.

But so for the authentication is very important because now urgent request is in the policy. And anybody can go and ask for domain

name registrant data and say this is urgent, but it's based on three criteria. It's like the threat to life, critical infrastructure, and CSAM, I believe. It's not. Yes, I think it's CSAM. But then for urgent request, in order to kind of not have everybody and anybody just submit urgent request and give the registrar some information, we need to authenticate the law enforcement so that the registrar knows that this is a real law enforcement asking for this and evaluates the request.

And we are not coming up with new policy about this. The council decided that to do this supplemental review team that we are a part of as well and discuss these various things that the Board also wants. Also, like, we need to look at whether this system should be obligatory for the registrars because at the moment it's just voluntary.

Another thing is that we need to look at how to authenticate law enforcement. And the system, unlike the data protection for registrants that is based on jurisdiction, this system is global. So it serves, it could potentially serve every law enforcement in the world.

And one thing that is very important to understand is, so we are coming up with an authentication mechanism, which is great. We want authentication to happen. We want the law enforcement to be authenticated. But what we don't want to happen is to have, like, the system that just authenticates the law enforcement and

then registrar thinks, okay, well, this is a law enforcement request. I'm just going to disclose the data.

In yesterday's meeting, and there are our other council members are here as well, and they can add to what I'm saying and also, like, correct me if I'm wrong, but yesterday we were talking about authentication mechanism that ICANN wants to come up with, and ICANN Board insists on coming up with this authentication mechanism because there's a major pressure by GAC.

So one thing that it's important to note that authentication is different from authorization. And I wish I had the flow chart that they showed us yesterday, because I do sound like an alien. So basically, when the law enforcement wants to be authenticated, the group is discussing, so what does this authentication mean? And the group, the majority wants the authentication to just be that, okay, here is this law enforcement agency. Who is this person who is requesting the disclosure? So they just want to limit it to authenticating the agency and the organization.

And then later on, when you are authenticated, then you will submit a request for registrant data, private sensitive data. And in that request, you need to say, like, why you need this data and some sort of evidence that you are working on a case and a few other things. And then the registrar will look at it and they will decide, based on the legality of the issue, if they want to, or sometimes even if they are obliged to, disclose their data.

So we have been advocating for registrar doing a fundamental rights balancing as well, as well as doing legality. So each request, and according to GDPR, they have to do a fundamental rights balancing anyway, but we don't want that to be restricted to GDPR. We want this fundamental rights balancing to happen for every case that they get, especially when it comes to law enforcement.

And for the authentication, our approach was that, at least what we tried to do, our approach was that we want to know more than who this person is, or this law enforcement agency is, in order to be authenticated. We want to know whether they are authorized or they have a mandate in their jurisdiction to be able to have access to people's private sensitive data. We also want to know whether, you know, kind of like give more information so that we don't authenticate agencies that don't even have the mandate to have access to private sensitive information.

But it doesn't sound like we are going to win that. Everybody's like, no, we should just like see, we should just authenticate. Authentication just means who is behind this law enforcement agency. Any comments on that? Go ahead.

MICHAELA SHAPIRO Michaela, for the record. I was just curious, kind of what kind of pushback you've gotten on that? Is it just an efficiency, or like what's the justification?

FARZANEH BADIEI

So, one thing that they mentioned was we want to provide a global system for law enforcement agencies, for every law enforcement agency. And then we can't just like create barriers. But that was not an overwhelming, like dominant point of view. The thing is like, you know, efficiency. We want just like minimal things. But it was very interesting to see that Steve Crocker was on our side. Yeah. And he said that this authentication mechanism has to help with creating trust between the registrar and the requestor. And of course, they should do the fundamental rights balancing and everything else.

But that first step is very important because, you know, just not, because you can prove that you are like, you know, some consumer protection agency or some law enforcement agency in some country, you should not be authenticated. You should not just like join the authenticated group. But didn't manage, like at the moment we are still pushing for it, but it seems like we have to work on authorization more, which I'm going to explain.

And so, the other -- oh, really? We only have 12 minutes? Okay, good. Rest assured, I can talk for 12 minutes. But I really wanted to brief you on this because I have not been as active about this issue on the mailing list, and it's very important for us.

So, we are going to work on authorization. Authorization means that the registrar evaluates the request, and then as a result of that evaluation, it decides whether to disclose the data or not. So, it's possible that we could add human rights respecting mechanisms

in that stage to help registrar with its evaluation of the request, and to help them to do their fundamental rights balancing. But of course, we need to come up with the elements that we want for that forum to have. What sort of questions should be asked?

And also, I would love to see for the, for us to provide some kind of basic fundamental rights or human rights impact assessment method for the registrar in case of, like, receiving these requests, for example. And I don't know if we can do that in this group, if we can do it as, like, implementation guidelines. I would have loved to have a fundamental rights balancing in the contract so that they would be obligated to do fundamental rights balancing, but, you know, there's a lot of pushback. But, you know, Steve Crocker was talking about automating fundamental rights balancing yesterday, wasn't he? I mean, but that was great.

Like, we have come a long way. They, like, for the most part of ICANN, domain name registrants and their rights and the privacy rights were not really, like, the centerpiece that they would work on. I was pleased to see that we have come a long way, but it took us a long time and we have to keep repeating the negative impact that domain name, that this kind of, like, disclosure can have on domain name registrants and their rights. So, for the authorization, we have to consider what elements we want to add to the submission form.

And the other thing is that we need to come up with a fundamental rights balancing for the registrar to do it. And we have done

fundamental rights, most of us here are very familiar with human rights impact assessment. Some of us do it on our, during our day jobs, but also, so we can come up with some kind of, like, lightweight fundamental rights on human rights impact assessment that the registrar can consider when deciding whether to disclose or not.

Yesterday, we actually had a good conversation about how do you do fundamental rights balancing. It happened mostly in chat, but these are, like, the two issues that we need to think about. What do we need in the authorization form, in the request form in order to help the registrar with deciding and evaluating the request? And what do we need the registrar to consider when they receive a request for accessing the private sensitive data from a law enforcement agency? And how can they do fundamental rights balance?

So now I'm going to let you all tell me about your great ideas and how we are going to move forward.

ANDREA GLANDON You have two hands.

FARZANEH BADIEI Yeah, Bruna. Andrew.

ANDREW CAMPLING

Hi, Andrew Campling. Clarification question. When you talk about a rights assessment, you used impact assessment and balance, so interchangeably. I assume you would, you're advocating for doing a rights assessment of both the registrant and the, where it's appropriate, the alleged victim. So you're balancing the both sets of human rights, not just a one-sided rights assessment.

FARZANEH BADIEI

When we talk about human rights impact assessment, we are talking about looking at the risk to all parties. Now, if the risk is higher for the registrant, if their data is disclosed, than the potential harm, then the registrar should not disclose. And what we are talking about here is like circumstances when like, you know, there is an oppressive regime, there's protests happening in the streets. They want to have access to people's private information to prosecute them or quash the protest. So they submit a request for private sensitive data and it's going to happen. It's might not happen. It's just a risk assessment.

And in that situation, so the registrar has to be aware that, okay, if I'm receiving this request, I should not just respond and give the data because this law enforcement is authenticated or claims that this is urgent. What they should do is to do their due diligence. They should also look at, is there a protest happening in that country? Is this agency that is asking for that data, does it even have the mandate to ask for that data? And sometimes these countries, they go to a harmless law enforcement agency and they

ask them to do that request so that it doesn't look like they want to kill and prosecute people.

So these are like the things that we want the registrar to have an understanding of and they might happen rarely, but still, when we do impact assessment, of course there's balancing rights, it's in the policy as well.

BRUNA SANTOS

I just wanted to clarify a couple of the organizations or eligible entities that would have access to data, right? Because the SSAD discussions, they started from a lay-up perspective, so law enforcement agents, but at the same time, we also have like a list of other organizations that could fall within this category, right?

And although we're starting with that, I just wanted to highlight that within the SSAD recommendations, we had like civil and criminal law enforcement authorities, but we also had data protection regulatory agencies, we had judicial authorities, the obvious ones, but also one category that interests us that would be consumer rights organizations granted a public policy task by law or a government entity acting on the same interests and so on. So this is also another of the areas that we will pretend to contribute in, in qualifying the access and what for. So yeah.

FARZANEH BADIEI

That is a very important point, Bruna, because also like when they said, oh yeah, law enforcement agencies, they said, oh, we are not

going to define them. We are not going to say what type. So anybody that is kind of like government affiliated can be like some kind of law enforcement agency.

And this is why we thought that we should push for authentication, not to be this automatic that you just like say, oh yeah, I'm this agency and just, and they authenticate them. And it is not unknown that, when the, some of these registrars, they get an authenticated request, they say, okay, well, I'm going to disclose it without doing any kind of fundamental rights balancing. So, we thought that maybe we can solve this problem of like having all sorts of law enforcement agencies be able to authenticate to their specific mandate.

Doesn't ICANN want to rely on each separate jurisdiction for data protection? Like, well, how about we say that, okay, well, if this law enforcement agency has a, does this have a mandate to actually have access to private information? And we are not talking about only oppressive regimes here. ICE also is a law enforcement agency. Well, actually, I think most countries these days are oppressive regimes. So yeah, there's no hope for democracy, which is all gone.

I have two minutes. Okay. So any other ideas on a practical? Benjamin, go ahead, make that comment.

BENJAMIN AKINMOYEJE

So I was saying on a practical level, you know, and I agree with you that there are oppressive regimes and governments, but let's say a registrar is just buried in his work and is not politically aware of things happening. Are there places or platforms they can quickly check with like, hey, what is going on in this country or what is happening here? Should I be mindful of the level of disclosure I make and things like that?

That might also be a very helpful tool to people who push back on some of these requests or these approaches we are requesting for to say, see, in case you are helpless, there are places or reference points where you can find out before you disclose things to anyone who asks you.

FARZANEH BADIEI

Yeah, that's an excellent idea, Benjamin, because what we can do if they keep saying that, oh, it's expensive and stuff like that or not, we can make it cheaper for them by providing information. And I think civil society organizations actually are in a good place to do that. It's just that civil society organizations are under-sourced as well.

But that's an excellent idea. I think we should talk about this and we should see whether civil society can come up with or whether already there's a mechanism. For example, Freedom House comes up with ranking mechanism for countries like freedom. That's one

thing they can data points that they can consider. But that's a really good idea. We should raise that.

Okay, great. So thank you so much. We have another policy meeting today. At the end of the day, we will be talking about what we are going to do at the council. It's going to be thrilling. Please join us. Thank you.

[END OF TRANSCRIPTION]