ICANN85 Mumbai | CF – GNSO: NCSG Interim HRIA DNS Abuse PDP
Saturday, March 7, 2026 – 09:00 to 10:00 IST

ANDREA GLANDON

Hello and welcome to the NCSG Interim HRIA DNS Abuse PDP. 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 and I will post them in the chat for your reference. I will now hand the call over to Farzaneh Badiei, you may begin.

FARZANEH BADIEI

Hello, everybody. I am sorry that I could not be with you, but this is a very interesting session as NCSG put together because we are going to start our work on the policy development on DNS abuse, the first, which is like the PDP is about associated domain check. And we need to do a human rights check for this PDP.

So, NCSG decided to put this session together to walk you through and talk to you about how to think about human rights when we are doing our work during the PDP on ADC, Associated Domain Check. Next slide, Andrea. Thank you.

So, this is how we are going to go about it. We are going to tell you a little bit what a Human Rights Impact Assessment is and what

does the chart already require? But Michaela will go through this through the lens of the overall process that usually Human Rights Impact Assessment processes use.

Then we are going to talk a little bit about how the associated domain check works, but we are not going to go into details because the registrars have many sessions on that. But we need to talk about it a little bit to show how to think about the human rights implications. And then we are going to talk to you about looking at human rights through five lenses that you can use in your work and then five questions that you can ask when we are coming up with these recommendations.

But of course, this is not a set in stone process. It's just our recommendation and we are here to discuss it and later on if we agree, we can also go to the PDP itself and discuss it. But this is like one of the first sessions that we have on how to do it on discussing the Human Rights Impact Assessment on a PDP and we are going to have more sessions as the PDP progresses in its work. Now, without further ado, I pass it on to Michaela to go over, what is an HRIA?

MICHAELA SHAPIRO Perfect. Thank you so much, Farzaneh. Hello to everyone who traveled over to Mumbai. I hope everyone had a smooth journey and yeah, please bear with me. I'm calling in at a very weird hour from London, but very excited to talk to you about what a Human

Rights Impact Assessment is and why we should be discussing it within the context of this working group.

So, this should not be a new topic for those of you who have followed some of the Noncommercial Stakeholder Group sessions, but we wanted to give you just an introduction to what an HRIA is and how it's relevant. And the types of questions that you should be asking as we go through the process of assessing what to do about the topic of associated domain checks.

So the idea behind a Human Rights Impact Assessment is that it provides a framing. So essentially a set of questions that you can ask to try to assess what action to take and how to find that balance between the actions that are required to take, that you must use in a certain context versus what is necessary to address a particular issue.

So, the kind of three main questions that we have outlined here are, is it necessary, is it disproportionate, and is it legitimate? And to go into more detail about each, the necessity element is about, is this required to achieve the aim? So, you have to think about, is there a less intrusive alternative to address the issue at hand? And this is something that, of course, will vary depending on the particular issue.

Similarly, in terms of proportionality, one question to ask yourself is, is the extent of the limitation balanced and not excessive relative to that aim? So similar to the necessity question, but really focused on, you know, is there an ability to think about this slightly

differently? So, again, similarly, is there a more a less intrusive option that you can take that hasn't been considered yet and how do you find that balance?

And similarly, is it legitimate? And the question that we put here is specifically, does the policy pursue a recognized public interest aim such as security or protecting others' rights without using that aim to justify disproportionate restrictions on rights it should instead promote.

And within the ICANN context, the working group is expected to consider whether there is a likely human rights impact and then assess who are the groups expected to be impacted and the expected severity. And again, this will all vary depending on the particular topic at hand.

As I said, the idea behind an HRIA is that this can be applied to a number of different issues in different ways and how you answer these questions will vary. But the questions themselves serve as a reference point that should be guiding how you decide how to address these issues.

And something that the Noncommercial Stakeholder Group really wants to emphasize is that these questions are not only necessary to be asked at the beginning of a policy development process, but should be continuously serving as a reference point throughout the process.

So not only just in the beginning, but also as we develop the different policy recommendations that will be considered by the working group and also in the implementation phase. So, it's not just a one and done, but it's a process that's continuous. So, if we go to the next slide please, I'll then go through some of the specifics here. Thank you so much.

So here we've outlined really the main principles that we see of relevance to the particular issue at hand. So, there are five articles listed here. The first being Article 12, the right to privacy, and unsurprisingly this is very closely linked to Article 19, the freedom of expression and access to information.

Privacy here specifically as it relates to the topic of associated domain checks is focused on investigation access to registrant data, so payment information, behavioral patterns across accounts. And to what extent this may or may not be thought of or is legally considered to be personally identifying information. And of course, that's something we can delve into more specifically later in the presentation.

On the freedom of expression, specific, so the Article 19, we also think about a suspended domain as a method for silencing speech. This is one of the initial reasons why a lot of the Noncommercial Stakeholder Group members are particularly interested on this topic.

So, we see this as, we understand that registrants have a right to know why an action was taken and also to understand. And as part

of the process of doing Human Rights Impact Assessment, you have to consider is the content that has been removed, is that worth, does that counterbalance in terms of proportionality the kind of, quote unquote, malicious action at hand?

And on that note, when you think about Article 11, the presumption of innocence, a compromised domain's registrant is a victim, not necessarily a suspect. The policy must distinguish between this, a victim and a suspect, and the presumption of innocence must come first.

We'll then move into Article 20, freedom of association. So, domain serves as the organizational infrastructure of a civil society, activism, journalism. This is not going to be a new thing exactly for people who are really well versed on this topic, but just as a reminder, a domain suspension not only impacts the ability to access certain web pages, but it also means that the email services, for example, for a particular entity is no longer available.

So, if you think about in the context of, let's say, a news outlet. If you suspend the domain of the New York Times, that will block not only the content that you might find, let's say, problematic, questionable, et cetera, but it also means everything from election coverage, which is essential for democratic participation, to New York Times recipes, which are essential for my enjoyment of my food. That all of those will be rendered inaccessible beyond just because domain suspension is a blunt force tool.

So, I just wanted to reinforce that, particularly as we think about the implications of a domain suspension and what the different options are available to you.

And lastly, on Article 2, non-discrimination, we also want to emphasize that compliance requirements must not structurally disadvantage smaller or non-Western operators. And so, essentially, the point of this slide being is these are all different elements that must be considered throughout the process of the policy development process, which I'm very excited that Farzaneh will be presenting next, so I'll turn it to you.

FARZANEH BADIEI

Thank you, Michaela. That was an excellent high-level framework. So, there are these three actors that we see that are involved in this process of associated domain check. There is the registrant. It could be some registrant that has registered like a portfolio of tomato gardens of like 500 domains. And then you have the reseller. It could be a hosting company or others. And then there's the registrar.

As you know, registrars, like the data that they collect and keep is different from the reseller and different business models has different registrars. With different business models have different data that they can do the associated domain checks based on. So, what they do is that -- and please if like the registrars are in the

room, if you want to add anything at this stage, then please just raise your hand and turn the mic on and let us know.

So basically, when they want to do associated domain check, they go around, they search and they find the malicious domain and they want to see if this same registrant has registered others.

Like they look for like email or name or other fields, but what is very important here is that during the PDP, when we discuss this, the policy that we come up with, it should not kind of like maximize the data collection or have like data collection obligations, but I will cover that later on.

So, then we have the reseller and also like there's the issue of malicious domains that you do associated domain check or compromise domains. And this is what we are talking about here. What we want to actually discuss is that whether this is an actual issue, whether doing an associated domain check could just kind of unknowingly or unintentionally get a compromised domain and kind of like suspend all of the domain names of the compromised domain because there was like one or two compromised domain that it was associated with that registrant. So that's one of our questions from the registrars. I hope it was clear, but we can cover it later. So, the next slide, Andrea.

Registrars don't want to correct me here, right? Come on, guys, I'm not in the room. You can correct me. Okay, so let's think about what happens when the data needed for the check doesn't exist yet? Imagine if registrars are asked to investigate associated

domains, but if the relevant data is not there because there was no requirement to collect it, and then we say that no, we want to require data collection, like more data pieces.

One response is to require registrars or resellers to collect more data to enable the check, but this will have a direct impact on privacy. And we strongly believe that we should just rely on the current data registration policy to do the associated domain check.

And then we look at like does a recommendation that requires new data collection pass the necessity and proportionality test? So, if like down the road at some point there are like data collection requirements, it has to pass the necessity and proportionality test. So now let's go to the next slide.

So now let's have this scenario that a registrant uses some of their domains for malicious purposes, but they also have completely legitimate domains. Like they register their grandma's tomato garden, a hobby site, a personal blog, or like, you know, they have like journalist friends. And an associated domain check that is triggered by the malicious domains could potentially sweep up the entire portfolio, including those innocent ones.

And our question is, if that is the case, and if the registrars think that this is a plausible scenario and it could happen, so how can we come up with some mitigation mechanisms? And also, how can our recommendations address this issue?

So, every recommendation that we have, it should ask what happens to this person, to the tomato garden registrant? Or if there is a compromised domain -- I see a question from Michael Graham about what is a compromised domain, I leave that to the room. So, let's go to the next slide, Andrea. Thank you.

I think that you are supposed to cover this slide, Michaela. No? Oh, yes. It's all good. Don't worry about it. So now let's look at the five reasons for every recommendation.

When you have the HRA guidelines, which is like a template, and it's just a guideline for ICANN and the community when they are doing their human rights check. So, you look at these issue areas, diversity, participation, due process, accountability, transparency.

Then we say diversity, does this treat all registrants equally regardless of size, origin, or resources? Then it's a matter of participation. Does your recommendation protect the registrant's ability to register, use and speak through their domain? The due process when the check goes wrong, is there a meaningful and accessible remedy for them? And by accessible remedy, we mean that like, you know, you figure it out quickly and you handle the complaint.

Then there's the accountability. Can the policy be audited? Is there oversight of how these checks are conducted? Is there enough transparency in the processes that they do the investigation? And

then our favorite transparency, which is, does the registrar know what happened to them and why? And then the next slide.

Okay, so one thing that we think about a lot is a matter of like, what if a smaller registrar or a registrar that is in a lower income country that lacks the infrastructure for automated domain checks and stuff like that, or they lack the techniques or the access to tools?

If compliance requirements assume a sophisticated detection, they effectively kind of exclude them. Or they make them, kind of they incentivize them to use techniques that like without being careful could just suspend the domain. So, the questions that we think that the participants should ask, and you know, anybody who is doing the associated domain check in general, does our recommendation accommodate different registrar sizes and technical capacities? And do we understand the business model and the charter already asked to consider?

But then also like when you want to look at it, you should talk about like, is this recommendation necessary? Is it proportionate and is it legitimate? Oh, Michele's hand is up. Go ahead, Michele.

MICHELE NEYLON Good morning, everybody. It's Michele here. I think the other thing that should possibly be mentioned is cost. Doing this will increase the cost across the entire chain, and I don't see any benefit to this. Also, the assumption that our small registrars in a lower-income country, I mean, there's plenty of registrars in higher income

countries, whatever the hell they are, that also would be impacted negatively if they have to jump through hoops to implement something that may or may not really impact them at all. And it seems like it's creating extra work and burden for little to no advantage for anybody.

Personally, I'm opposed to this being a PDP anyway. I think it's ridiculous. This should be just an advisory. Thanks.

FARZANEH BADIEI

Yeah. So, Michele, I corrected myself. It's an unfortunate slide thing. We had like smaller registrars and registrars based in lower income countries and we messed up. I mean, I messed up the writing. Andrew?

ANDREW CAMPLING

Hi, good morning. I guess the other side of that is by not doing certain things, what is the human rights impact on end users, if you will? So, for example, by not knowing who the registrant is, if that then is a malicious registrant that's targeting vulnerable groups say, and impacting negatively on their human rights, be that privacy or perhaps more significant ones, then yeah, there's a downside by not doing it.

So, I think just by looking at the impact on the registrant, that's maybe missing a significant chunk of the human rights assessment requirements.

FARZANEH BADIEI

Yeah. So basically, we are looking at, not just the registrant, we are looking at the end user and this is a PDP that is trying to address those issues. And in the human rights impact, as I said, of course, you have negative and positive impact, but it's a matter of proportionality and also the necessity. But I'm going to go down and pass it on to Michaela to explain further.

MICHAELA SHAPIRO

Thanks, Farzaneh. No, I just wanted to give a quick response to Andrew because I really appreciate that question. And the way that we think about it is, as Farzaneh said, it's a balancing act. So, we're trying to think about the idea is to elucidate as many of the necessary perspectives here. And so, we're not thinking about this from one particular type of registrant.

The idea is to find that balance of, okay, well, if I do this and it negatively impacts that group, does that counterweigh the necessity to address the issue at hand? Does that actually -- sorry, I'm also not, I might be slightly incoherent given the time from London, but what I'm trying to say is you have to do a cost benefits analysis, really. But I'm sure Reg can probably give better detail and say so much more eloquently than I can right now. Go ahead, Reg.

REG LEVY

Thanks Reg Levy, Tucows. I don't know that I'm more articulate than you are, for sure, but I would submit that the human rights that are frustrated to a person who is a victim of a scam would be resolved by suspension of the domain, which has already occurred in the circumstances that we're discussing. And disclosure of personal data is not necessarily ever going to provide any recourse to the victim of a scam. So, I'm confused about what human rights you think might be implicated, and would love to hear more about that.

ANDREW CAMPLING

If it's okay for me to respond, yeah. So, for example, if you don't have knowledge of the registrant that's behind malicious domains. For some definition of malicious domains, it may be that they're doing something that has a significant impact on a vulnerable group. As I'm, amongst other things, a trustee of the Internet Watch Foundation obviously, we have a particular focus on CSAM. The impact of CSAM cuts across many human rights of children, be that privacy, right to life, a whole host of things in between.

So, I'd submit, in that case, if you know who's behind the malicious domains, that's important to know to actually resolve the underlying crime, for example.

REG LEVY

Right. So, when you said crime, it sounds more like you're thinking about the law enforcement aspect of it as opposed to the victims.

And CSAM, we're going to leave to the side because that's not DNS abuse. When a registrar suspends a domain, the human rights that we're looking at right now are the human rights of the registrant, because we need to make a determination about how to allow them to continue to use their domain in the event that it is a compromised domain, for example.

The human rights that are frustrated by the domain itself are a different conversation and were already dealt with before the domain was suspended. So, they are also being looked into, but that's a different conversation.

FARZANEH BADIEI

Okay. I see Anil's hand is up and we actually encourage that. So yeah, let's have a conversation. Anil, go ahead. Is Anil in the room?

ANIL KUMAR JAIN

Sorry, I think my mic was closed. Anil, for the record. This is regarding the discussion on small or big registrar, whether they will be able to collect the required data for the domain check, associate domain check or not. I think the fundamental question is that domain check is required for the entire internet ecosystem and they don't distinguish between a small or a bigger registrar. So, I agree that a small registrar, it may be difficult economically to check and do the required check, but definitely, we have to find a solution.

For example, one solution can be that ICANN can provide a technical help, provide the technical platform, which can be extended to the small registrar to do the important check. But I personally feel that we should not say that big registrar do the check and small registrar we may relax. Thank you.

FARZANEH BADIEI: So, we are not really suggesting that, but it's a reality that if we have like very prescriptive, which the PDP shouldn't, but if we have very prescriptive ways of saying that you should do associated domain check, but it's a complex thing from the start anyway. At least this is what I have heard from multiple people, that this is not something that you can easily do without support.

And what worries us is that we don't consider those registrars that don't have the know-how and then come up with something complex that only a few of the registrars do and impose it on the smaller ones. I think that in any conversation or recommendation, we need to consider that. Go ahead, Michele.

MICHELE NEYLON: Is that me, Farzi?

FARZANEH BADIEI: Yeah, Michele, your hand is up.

MICHELE NEYLON Oh, thanks, Farzi. Sorry, I was half asleep.

FARZANEH BADIEI No, not Michaela. No.

MICHELE NEYLON Now just in terms of this thing, this suggestion that ICANN could somehow magically help a registrar, considering that, that's just technically not possible. Because in order to do the associated domain checks, you need to have access to all the registration information.

And basically, the only information that ICANN as an external third party would have is that which is public, which would be the domain names associated with the registrar, and the name servers. And you could obviously extract from the name servers some DNS records.

The only way ICANN can help a smaller registrar is financially, not technically. That's, anybody who thinks that they can somehow assist us technically hasn't understood what we're being asked to do in this case. Or maybe I've missed something completely, but I don't think I have.

Also, I'd have to support Reg's commentary as well about every time we discuss abuse, people immediately go to CSAM, that is just, intellectually it's just ridiculous. The conversation we're having here today is around a specific PDP, which is to do with associated

domain checks. If you're not familiar with what the PDP is about, please go off and read the summary. Thanks.

FARZANEH BADIEI

Thank you. Let's go to the next slide. Okay, so participation, Article 19, freedom of expression, and Article 20, freedom of association. So the associated checks triggered by volume threshold could flag legitimate bulk registrants. It could be like political campaigns, could be non-for-profits, could be journalists. And it's not just about like commercial assets, it's about like channels for expression, information, association.

Okay, so if you have like associated domain check and then you automate the process and you say that, okay, so this is too much work, I want to automate this process, which happens in the industry or sometimes almost impossible not to use some kind of automated mechanism. But then there has to be some kind of human review.

We have to ask, is there a human review step before any domain is suspended, if there is any action is supposed to be taken, and who notifies the registrants? When do we notify the registrants?

So, the charter question asks a reasonable investigation and whether criteria are proportionate and necessary. The answer must account for the range of people who register large portfolio legitimately. And there could be like something that could happen that suddenly like their portfolio includes these malicious domains,

which like we also have to think about the probability of these scenarios happening.

And so, if you think that this would never happen or the probability is really low, then we can of course consider that when we are doing a Human Rights Impact Assessment, which is all the time during the coming up with the recommendations.

Okay, so are there any responses to this or any comments, any feelings about automation or using different -- Oh, Michele and then Sarah. Okay, go ahead. Michele, go ahead.

MICHELE NEYLON

Thanks. Michele, the one with the moustache, as opposed to Michaela, who doesn't have one. I suppose one of the things I would look to is fear. For smaller operators, the fear of ICANN compliance, the fear of potentially breaching a contract means that some people may opt for a high level of automation or as is the current fashion to throw AI at the problem. Because obviously the AI is infallible and will never ever, ever make a mistake. We all know that one, that's pretty obvious and that I think is something that cannot be underestimated.

From the larger registrars, for those that have been around for longer, sure, I think most of them would probably realize that throwing automation on absolutely everything without any human review is probably a bad idea. But we've already seen with some of the new registry operators from the 2012 round that when the anti-

abuse things were brought into place, that their immediate reaction was knee-jerk. So as soon as they received a single complaint in relation to a domain, they suspended it.

And the amount of time, energy and effort to get that domain unsuspended is disproportionately high. In many cases, it's hard from the registrar side to even find out who to contact to get the domain unsuspended and what they expect you to do to prove that the domain was not being used maliciously. Thanks.

FARZANEH BADIEI That's very interesting. Thank you, Michele. Sarah, go ahead.

SARAH WYLD Hi, this is Sarah from Tucows. Honestly, I could have lowered my hand as Michele was talking because those were the same points I wanted to make so I'm just going to stop there and say yes, I agree with those. Thank you, plus one.

FARZANEH BADIEI Thank you. [inaudible - 00:36:05]?

UNKNOWN SPEAKER Hello, everyone. My name is [inaudible - 00:36:28]. I am from National Internet Exchange. This my personal research and I wanted to bring about an issue related to mechanism, related to DNS abuse, which is DNS tunneling. So, what basically is DNS tunneling is, it is a covert communication technique that exploits

the domain name system to transmit an arbitrary data established persistent attacker control and bypass network security protocols.

So, I want to quickly complete this, that there are core five categories in DNS abuse related to ICANN. So, malware, botnets, phishing, pharming, and spam. These are five categories. So, I basically summed up some recent cyber-attack incidents.

First one was the Detour Dog Stellar attack that happened in August, December 2025 where tens of thousands of websites were compromised using TXT records. Second was BeyondTrust RCE Exploitation, initial exploit followed by Cloudflare and Vault Viper late in 2025. These were related to C2 botnet. What I observed in these attacks is the initial access phishing or exploit DNS tunneling as persistence and large maliciously registered portfolios for rotation and resilience, there was no web page hosting and these attacks were high skill evasions.

Now, I want to quickly bring about some report that was published by ICANN itself. Informal study and persistent usage of bot activities. So, this was proposed by Maciej Korczynski, KOR Labs, and it was also included in ICANN OCTO by Samaneh.

The key findings in that report, the informal report was botnet command control repeatedly identified as the core maliciously used case alongside with phishing. So that was repeating in that report. API access, there was a 401% increase in malicious --

FARZANEH BADIEI I'm so sorry, [inaudible - 00:39:19], for interrupting you. Is there like a human rights connection?

UNKNOWN SPEAKER Ma'am, can I sum up the whole thing?

FARZANEH BADIEI So just like yeah, if you can and also if you could relate it to human rights, that would be great.

UNKNOWN SPEAKER Ma'am, I wanted to say that DNS tunneling is currently not in the DNS abuse section. So, can a policy be made or some things can be done to at least look at that issue since it is a major issue? And the reports say that it is quite persistence, that's my question.

FARZANEH BADIEI Yeah, thank you, [inaudible - 00:40:05]. So, the thing is that at ICANN, the mandate for ICANN is limited and botnet ecosystem is a very complex ecosystem that ICANN doesn't like govern every aspect and every actor. And most of these examples that you made actually go, like are within that complex situation.

So, like we should have this conversation later on. I can see many hands up. I hope that they also like touch upon your question, but let me go to the people who are asking questions and then also I

see some questions in chat. So, we have three, four more slides, but we wanted this to be a conversation. So, Michele, go ahead

MARC TRACHTENBERG

Mark Trachtenberg for the record. Thank you, Michele. I think I'll address one comment Michele made first, which is that maybe at some point a few registrars were being overaggressive in addressing abuse complaints, but we are not seeing that in practice now. It is actually quite the opposite. So, no one is overreacting and taking down domains without any justification whatsoever, regardless, neither are.

But that aside, I would say that I don't think there is a human rights issue here because the associated domains check is not being done in a vacuum. Once the complaint is submitted, no registrar or registry will do that. Rather, the associated domain check, as I understand it to be contemplated, is only going to be conducted after there's been a determination that there is actually DNS abuse.

And so, if that is the case, or if it's not the case, and we can specify that, that really, I think, takes the human rights issue off the table. Because once it's been determined that someone is actually engaging in DNS abuse, the likelihood that the associated domain check is going to sweep up all these other domain names that are being used for political speech or other legitimate purposes is incredibly low or really non-existent.

And so, I think if we can either specify that or that's already assumed, this kind of takes that issue off the table. And then at some point later we can do a Human Rights Impact Assessment maybe a year in to see, has this actually been the case and has anything been swept up into this? But from a logical perspective, the likelihood seems quite low.

FARZANEH BADIEI

Marc, I totally disagree with you. So, basically, I think that we made examples of like how human rights can be implicated and it's not just about like, you know, if we go down the path of like more data collection, that privacy can be implicated. So, it's not only about like suspension. And even, if we have made examples in which there are some scenarios that could be a malicious domain, but the guy could have like 500 domain portfolio and others could be implicated. So we have to be careful about this. So it is not [CROSSTALK].

MARC TRACHTENBERG

With respect, Farzi, I mean, we can't let human rights stop every policy that exists in ICANN. To the extent that a person is determined to have engaged in DNS abuse, which is a very narrow definition and we're not discussing how narrow it is here, but it is narrow. And so, we know that it is quite malicious behavior, which is basically phishing or fraud or, you know, botnets or malware. And so, to the extent that --

FARZANEH BADIEI

No. it is not fraud, by the way. It is not fraud. Let's state that, but thank you, Marc. I think that, yes, we are quite familiar with the other positions that others have. With this regard, we are not saying that we should stop the recommendations. We are just saying that consider these things and if they can happen and see what the risk is. We are not even saying that stop the recommendation. We are just saying that be conscious about what you are suggesting. Reg's hand is up. Go ahead, Reg.

REG LEVY

Thank you. Reg Levy from Tucows. I wanted to address the DNS tunneling concern that was brought up earlier. And my understanding of DNS tunneling is that it actually is part of the DNS abuse definition and the amendments because it falls under malware and DGAs and command and control systems. So, yes, absolutely. That's something we're worried about. Thank you for bringing that up.

I also wanted to address Marc's insinuation that criminals are not due any human rights at all. It is entirely possible that there are some countries in which that is the case, but even criminals deserve due process and have other rights. So, I will also say that a lot of what we're talking about here goes toward compromised and not necessarily malicious domains. So, we're looking at the broader

scope of things, and we are concerned about making sure that the human rights of everybody involved are respected.

FARZANEH BADIEI Right.

MARC TRACHTENBERG I just want to point out I did not insinuate that criminals have no rights.

FARZANEH BADIEI Oh, yeah, so --

REG LEVY You literally said that people who have phishing domains don't deserve rights, so.

FARZANEH BADIEI Yeah, you said human rights topic is off the table when we find a malicious domain. Okay, Santanu, please.

SANTANU ACHARYA Thank you. Okay, my question is, how might aggressive DNS abuse mitigation strategies -- Good morning, everyone. My name is Santanu for the record. My question is how the aggressive DNS abuse policy could affect the human rights? Could you discuss it on a HRIF framework, please?

FARZANEH BADIEI

Sorry, you mean -- so I think that we are kind of discussing exactly your question if I got your question right. So, we are kind of coming up with different scenarios and thinking through how it can affect. But of course, if there is any need for further clarification, we are here and can explain or I will put my email in the chat. Michele, go ahead. And also, we have three, four more slides and yeah, short.

MICHELE NEYLON

Okay, just sorry. So just very briefly, Michele again. You've been talking about compromised domains. One I think which is very important, specifically in relation to Marc's comments is compromised accounts.

So, when an account at a registrar, which is compromised in one way or another, we've seen this happen multiple times over the last couple of years. So, the domain, the account with us is legitimate, it's a small business or an individual or whatever, and the account is compromised in some way. And then the scumbag is able to control that account and starts using either the existing domains in the account or registers other ones for malicious purposes.

So, if you apply the associated domain checks too broadly, you could end up sweeping up a load of innocent domains and websites and other services.

FARZANEH BADIEI

Yeah, that is true. Let me cover this next slide and then I come back to Sarah and Marc, if that's okay with you. We only have 12 minutes. Okay, let's go. So, let's go to the next slide, Andrea.

Okay, so actually, this is what I think Santanu was kind of saying, how is it like human rights related? So, we are talking about like the remedies and what does appeal look like for registrant whose domain were suspended because they share an email pattern with a bad actor. And what is the corresponding remedy?

Like the PDP doesn't have to talk about the remedy. They could say that, yeah, there is remedy there according to this contract. You can make a complaint or you can, I don't know, there are some other obligations, other mechanisms that you can use. And also like, is the remedy accessible? But this is such a -- Okay, so I think we are going to be in this room for the next 45 minutes. Go ahead, Sarah.

SARAH WYLD

Hi, this is Sarah Wyld from Tucows. I'm noticing some really interesting conversation in the Zoom chat about, at what stage in the process does this Human Rights Impact Assessment happen? And we should figure that out. Not we, the PDP working group should figure that out.

I did look at the checklist from the Latin Diacritics PDP and I was under the impression that that HRIA happened towards the end of their process, looking at the recommendations and what effects on

rights there might be, but maybe I'm wrong about that. Maybe it was earlier. Either way, I do think, and I think I agree with Michele, that it should be happening throughout the whole PDP process.

As recommendations are being considered, the working group should think about, not only how would this recommendation help to address DNS abuse, but also what would be the impact on the registrant's human rights. That human rights consideration should, in my opinion, be part of that conversation at every stage of the work, just like how data privacy impacts should also be considered throughout the work. Thank you.

FARZANEH BADIEI

Thank you, Sarah. Actually, you know, so when the transfer review policy came about, we did just like an ad hoc Human Rights Impact Assessment. And I had a conversation with Roger, who was the chair of that PDP. And he told me that I wish we had this conversation at the beginning of the PDP and not after the fact so that we could have these conversations and dialogues which we could like have a clearer understanding of what is like urgent.

You don't have to have the mechanisms in the PDP, like get the PDP to come up with remedy mechanism. You can say that, yes, remedies are really important. This is what we're doing about it in the future.

There are various ways to do this. This is not set in stone. We are not that powerful. Unfortunately, NCSG is not. So, don't worry

about being like we are not going to stop the group from making progress, but we just want the group to think about human rights in this framework. And I have like five questions that they can ask themselves as they are coming up with the recommendations. Marc, go ahead.

MARC TRACHTENBERG

Right. I mean, to clarify, again, I don't think anyone has no human rights, and I have no issue with human rights being part of this process, and they should be assessed in every process. But here, where a domain name has been determined to be used for DNS abuse and that triggers the obligation to check for associated domains, that human rights assessment can be part of that process.

And so, in fact, when the registrar looks at the portfolio and they see, okay, every other domain name is used for some legitimate purpose, but this one is being used for abuse, okay, that probably indicates that maybe this domain name is compromised so I'm not going to do anything.

And the associated domain name check, when you talk about sweeping everything up, it doesn't sweep anything up, right? All it is, is part of the investigation where people look at what else is in this account as part of my investigation, determine what is likely happening here.

So, if I'm a registrar and I look at an account and I see this one malicious domain name and 50 others or two others that are used for legitimate purposes, I might think, okay, this domain name may be compromised. I should investigate further. Maybe I want to contact this customer and I want to see if they know about this or what's going on.

But at the same time, if you look in that account and you see 20 other domain names that are also being used or likely being used for DNS abuse, that also paints a different picture. And that is part of your investigation that you should be doing.

So, I don't think that these two things are mutually exclusive. We can have this obligation to check for associated domain names, which doesn't require the registrar to do anything or take any action against those domain names, but it's part of their investigation. And then the registrar, as always, determines what they think is best. Doing a balancing test of everything.

FARZANEH BADIEI Yeah, absolutely. I totally agree with you, Marc and we need to cover the rest of this slide. We are not saying anything that like we are not blocking the process. We are just saying, hey, when you're doing these recommendations, think about these things in the back of your mind. So, let's go to the next slide, Andrea.

Accountability. So, this is another issue area. It's in the guideline for the human rights check. So, the associated domain check is

done by whoever has the data, registrar or reseller, depending on the model. And how does compliance happen? What does the audit trail look like?

And so, some of these, like these are the questions to think about, like are we going to kind of like implicate some sort of human rights when we are recommending certain means of investigation? Which I think that as the charter also says, the investigation should not be prescriptive. So that could be some of the mitigation mechanism. It could be that you give the registrars some kind of like a broad mandate that they could decide so that some of these human rights could not be implicated. Can we go to the next slide, Andrea?

And then we come to transparency, which is the last one. The domain is suspended following an associated domain check. Does the registrar know why? Do they simply see a suspension notice? And also, are we going to have transparency reports that these domain names were suspended because of associated domain check? Oh, we only have five minutes? Okay. Okay, great.

So, I'm going to go to the questions and then to the questions that we are recommending to ask, and then I'm going to go to Edmon and Margie and wrap it up. Let's go to slide six.

Okay, these are the five questions you should ask. Who is this acting on, like the associated domain check? Not just a bad actor. Could it implicate a registrant that is innocent? Does the required data actually exist? What happens when it goes wrong? Who

checks whether this is done correctly? Does the registrar know what happened and why? And that's about it.

And I see Margie's hand is down, Edmon's hand is still up. Go ahead. You have one minute, Edmon, and I'd really like to hear Margie too for one minute. Go ahead, Edmon. Oh, no?

EDMON CHUNG

Yeah, just very quickly. You know, I'm glad that human rights considerations are in PDPs right now. And I put my hand up to just say that the Latin Diacritics one, it's probably less sensitive on the human rights issue and it was done at the end. But I don't think we need to be prescriptive about PDPs, how they deal with the human rights assessments.

And for this one, maybe the right thing to do is to do it all throughout as the issues are being considered. But in the future, there may be PDPs that are more or less sensitive to human rights issues and I don't think we need to be too prescriptive about it.

FARZANEH BADIEI

Yeah, exactly. Margie, your hand was up and I saw your question in chats, which we missed.

MARGIE MILAM

Yeah, thank you. It's Margie Milam and we just wanted to talk about what I said in my chat, which is human rights also include IP rights under Article 27 of the Universal Declaration of Human Rights. But

yet the framework we've seen today doesn't take those into account.

So, I'm just wondering how we can get to a place where IP rights are also considered in the important human rights assessments? Because I think those rights are particularly implicated in the DNS abuse mitigation when it's typically IP rights that are used for, for example, phishing attacks, trademark rights, and copyrights.

And those sorts of things are often being misused as part of a phishing attack. So, I think it's something that we should try to weave into the framework as we do our work going forward. Thank you.

FARZANEH BADIEI We need to think about that. Reg, go ahead.

REG LEVY Thanks. Thank you, Margie, for that question. We're talking about DNS abuse, and my understanding is that IP rights are not part of DNS abuse. So, to the extent that the intellectual property rights that you're concerned about involved in the domain are part of a phishing, pharming, malware, botnets, or scam, or other DNS abuse, then they would be, as I said before, vindicated when the domain is suspended.

That said, we also do consider the intellectual property rights of the registrant when reviewing requests from IP rights holders that use the trademark in the domain name. Because very frequently it can

	be the case that somebody is using their free speech rights to speak about a trademark.
FARZANEH BADIEI	Yeah, and we need to have more conversation about this issue. Okay, we are done with this session. Thank you. This was just the first session. I'm sorry we had to go through it really quickly. We care about your feedback. We care about your comments. Nothing is set in stone. We are not going to block anything and we are going to just discuss. And thank you for attending.
ANDREA GLANDON	Thank you. You can stop the recording.

[END OF TRANSCRIPTION]