ICANN81 | AGM – GNSO: DNS Abuse Mitigation and Human Rights Impact Assessment
Sunday, November 10, 2024 – 10:30 to 12:00 TRT

ANDREA GLANDON: Hello, and welcome to the DNS Abuse Mitigation and Human Rights Impact Assessment session. My name is Andrea Glandon, and I am a participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace. And I will now hand the floor over to Farzaneh Badi. You may begin.

FARZANEH BADI: Hi, I'm, yeah, hi everybody, my name is Farzaneh Badi, I'm a member of non-commercial stakeholder group, which is the civil society arm of the GNSO. We work on advancing human rights, privacy, freedom of expression, and access to the internet and domain names at ICANN. So the reason we came up with this session in collaboration with the contracted party house DNS abuse working group was that as a stakeholder group, we emphasize the importance of having qualitative indicators for the DNS abuse mitigation success. So as well as having quantitative indicators, such as how much DNS abuse has gone down, we suggested that we should also look at the processes that we have in

place and see whether we provide due process and appeals mechanisms for the domain name registrants when mitigating DNS abuse. And so the framework that we have decided to use today in this session is a human rights impact assessment framework. We decided to use that framework to see if we can collectively, all of you I mean, we can collectively come up with suggestions on how human rights could be impacted when mitigating DNS abuse and what sort of remedies should be afforded, could be afforded to the domain name registrants, if any. So that's about it.

Some logistics, so if you don't have these papers, let me know and I will give you one. And also we are going to do, we are going to go over scenarios together and we are going to use those flip charts, so you're going to be very mobile during some part of the session. And now I pass it on to Michaela from Article 19.

MICHAELA SHAPIRO: Thank you, thank you. I was trying to figure out where to look. Maybe I'll just kind of swivel a little bit. But hi, I'm Michaela. As Farzaneh said, I'm here representing Article 19, so we're a human rights organization working at the intersection of freedom of expression and human rights. So hence, very excited to be here today. A lot of you are here probably because you may have heard of DNS abuse. Maybe you have a sense of how it works, what it could look like. Maybe you're trying to mitigate it yourself. So thank you so much for the work you're doing on that. What we're trying to do today is talk about the different areas of intersections of human rights, so as we put together up on the screen, and hopefully you can read it. But if not, you should have a handy dandy sheet. If not,

also please let us know. We'll give you one. We have plenty of printouts. But we'll be talking about what elements of human rights are relevant for this work so that we can make sure that as we try to address DNS abuse, that we are still ensuring that human rights such as the right to privacy, freedom of expression, the right to equal treatment, freedom of association, access to remedy, you name it, we can then make sure that it is also being addressed and that we don't overstep.

So this is an area that Article 19 has been working on through ICANN for quite a while now. As a lot of you know, it's a multi-stakeholder organization, so we are not the only ones doing this work. But Article 19 in particular has been involved in the development of the Cross-Community Working Party on Human Rights, which some of you maybe are members of or have attended a meeting of, and they're looking particularly at ICANN's role in corporate social responsibility, so this is right up our alley. So just to add that in addition to our work within the NCSG and the Cross-Community Working Party, there are a number of other groups, a lot of you are represented here today, who have been doing incredible work on this, within the context of the new bylaws that have been changed earlier this year in April, which should also, you'll see a copy of within your cheat sheet, so on the second page you'll see the text of the amendments, which is what we're working with today, or maybe the third page, sorry, numbers are not my forte, hence why I'm here at ICANN. So we have printed out a copy of the bylaws that are relevant for today that we're working to implement and to ensure that we interpret in a way that is human rights respecting. So a lot of you maybe are familiar with the bylaws, maybe not, so hence why we printed it out. We also wanted to make sure that we reference the

different human rights instruments that are relevant, so that way we cited our sources, you guys can take a look, we didn't print out the full text because they're quite long, but this way we have a little bit more kind of material to work off of as we go through this exercise.

Yes, and also, as Farzan has mentioned, we're going to make this a very interactive session, so please don't get too comfortable. We're going to have you do some work in groups, we'll be discussing different scenarios, we tried to make them not too, too tricky, but we want to make sure that everyone is thinking through these scenarios as in-depth as possible. Ideally, we'll have you each kind of take on a role, a persona, so get your acting skills, your improv skills out, we're really excited to try to think about this exercise and these scenarios in as many different perspectives as possible, because that's really what a human rights impact assessment is all about, making sure that as many perspectives are being respected and understood through these processes.

Maybe on that note, to not go on for too long, I can pass to some of my fantastic experts here who maybe can talk a bit more from the registrar or registry perspective. I don't know, whoever would like to go first? Reg or Dennis?

REG LEVY: My name is Reg Levy, I'm from Tucows. Typically, the registrar receives the first notice of some kind of DNS abuse. So, what we would do is make sure that there's evidence of the alleged abuse. If there isn't, we typically follow up with the reporter, and if the evidence checks out, we

either suspend the domain or we work with the reseller or registrant directly to mitigate the abuse, because it could be a compromised domain.

DENNIS TAN: I just want to take one step back, and for the purpose of this conversation, when we talk about DNS abuse, we're referring to the ICANN definition of DNS abuse, which is defining our contracts, the RRA and the RA, and that is the five categories of security threats, pharming, phishing, malware, botnets, and a span when served as a delivery mechanism. So, when we're talking about DNS abuse, that's the lens that we're using here, talking about these scenarios and all the processes.

FARZANEH BADI: All right. So, what we want to do here is to kind of look at how exactly in each process that we take, each step that we take in DNS abuse mitigation, what sort of human rights impact it could have. So, as I said, we use the human rights impact assessment that civil society organizations and digital rights organizations usually use in order to look at processes, like the impact of the processes in place. So, you have these papers that we discuss how each of these rights are relevant to the DNS abuse mitigation. For example, when it comes to right to privacy, and we didn't come up, we didn't make up these rights, these rights are based on the Universal Declaration of Human Rights and a bunch of other declarations that you will see references to it at the page number four. But, so, for example, right to privacy. If the mitigation

mechanisms for DNS abuse require disclosure of the domain name registrant private sensitive data to law enforcement or the person who is doing the mitigation, then it might have some privacy implications. It might not have always privacy implications, but there are certain scenarios that it might have. So, if the registrar is disclosing the data to law enforcement agency, there might be some sort of implications. If the registrar is disclosing it without receiving much evidence, that could also have some implications for privacy. And if the law enforcement agency requests can potentially lead to human rights violation.

So, and when it comes to freedom of expression, for example, the registrar duty to investigate reports of abuse and take appropriate action, which is in the contractual amendment, this requirement for registrars to take appropriate action to DNS abuse is vague. So, what sort of, and it could, if the registrar takes drastic measures that could also lead to the deletion of, we don't know, but if they do, to the deletion of the domain name registration and the domain name, then it could have possible freedom of expression implications. Then there is the right to equal treatment and non-discrimination. And people get a little bit confused here because these human rights framework is usually for like, you know, gross misconduct and like when courts do not treat people equally. But here in this context, in context of DNS abuse, the right to equal treatment, we simply mean that mitigation mechanism and remedies should be made available in the registrar service region. So, wherever the domain name registrant is, they should be afforded with the equal treatment. They should be, the same process should apply to them regardless of where they are.

And freedom of association, for example, it could be that the mitigation of DNS abuse could lead to, for example, lack of access to some of the services that we have online for meeting and also like gatherings and that could have an impact on the right to assembly. And also we have the access to remedy. So, when there is a DNS abuse mitigation and for example, when there is a false positive, whether there is access to remedy for the registrant if a mistake has happened.

Okay, and the last one is the right to fair trial and due process, which here the fair trial does not really apply here, but what we mean is due process of like whether there is the process is fair, there is a registrant gets to answer what happens and in case abuse happens and explain the situation and also be told why a decision was made that their domain name was suspended. So, these are the general human rights that we have enumerated that we believe that could be impacted, not in all cases, what we believe that could be impacted during the DNS abuse mitigation. And with you, we want to work on to come up with like situation and scenarios to think about in which under what circumstances there is a risk of impacting these human rights when we are mitigating abuse and what can we do to reduce the risk. And that's about it. I think Michaela, you wanted to talk a little about the scenarios and how we do, okay, go ahead.

MICHAELA SHAPIRO: Fantastic, yeah, and just to say, if the main idea behind a lot of this exercise is what are we trying to bear in mind? Transparency, accountability, those are kind of the underlying principles that we're trying to look at today. So, that's, if you can't remember the exact

terminology, don't worry, that's why we have the cheat sheet. But those are kind of the main ideas we want you to have in mind. So, Andrea, if possible, we could scroll to scenario four. Hello, nice to see so many familiar faces here. So, what we'll be doing, and apologies, the font is a bit small, but what we wanted to try to do is walk through a scenario today. So, maybe I'll pause just for a second, but I can also read through the scenario and we can try to, maybe we can get a discussion going to think about some of the ideas that are coming through here. So, oh, fantastic, thank you so much.

Yeah, who needs the last words, right? Ah, thank you, I might use this. So, I'll read it through, and that way we can just have a moment to reflect and kind of think through. So, a brand owner accuses a website that is being used during a civil protest of phishing and asks the registrar to take the domain name down. The domain name uses the brand's name to criticize the brand involvement in helping with oppressing people during the civilian protest. However, the website also engages with phishing. The registrar suspends the domain name, the domain name is being used for authentication on other websites, and the registrant cannot access the accounts associated until and if the suspension is lifted. So, the questions we're trying to think about here are where there could have been a potential to how could we have addressed this in a way that limits the potential human rights risks to the greatest extent possible while still addressing the issue. And so, one thing that, for me, when I read this, and I was trying to kind of think through what would be the first thing I would be thinking about is, okay, is it, in fact, DNS abuse? That would be the first question to ask yourself. Phishing falls into the definition of ICANN under DNS abuse, so, to me,

already, clear cut, there is clearly a DNS abuse. Now, the question is, how do we address it? So, there, we would see, okay, well, there's also freedom of expression involved here in the sense of there are people who are protesting, but at the same time, concurrently, you have phishing that is also taking place. So, was the suspension of the domain name without any kind of investigation as far as we're aware of, so, without an investigation, are we sure of the phishing? So, we have been told that there is phishing. We haven't done an investigation. That would be, potentially, where I would say, come in, okay, this would be the first step is let's investigate. Let's make sure that this is actually happening before we suspend. Let's give benefit of the doubt. So, that would be the first area that, that would be the second area that I would be looking at. And then, you have the issue of not accessing the accounts. So, there, you'll have issues related to, right, to access to information. There might be information on there that is relevant for people who are in the protest, so, they would want to have that information accessible. So, that's kind of the types of things that we'd be thinking of. And I know we ran through that a bit quickly, so, I also am happy to pause in case there are any others on the panel who'd like to come in on anything else with that scenario.

VOLKER GREIMANN: Yes, thank you. The scenario's interesting. However, it lacks certain information that would be required to make a decision. For example, is this some service where subdomains are rented out, or is this clearly in the control of the registrant? What kind of law enforcement are we talking about? Is it law enforcement that is of competent jurisdiction for

the registrar that is holding the domain name, or is it law enforcement in the country where we have nothing present? So, is it a standard abuse complaint, or is it an actual law enforcement complaint? Then, the question is, is the information necessary to, providing the information necessary? Do they have a legal request, or just an informal request, please send us the data? Do they provide a jurisdictional gateway to basically claim the data, or are they just requesting it on, please be nice? So, there's more that we would need to know, but ultimately, we would look at this request regardless. The question is just, do we disclose more than we would, if it's phishing and we can verify it, the domain goes down, yes, but do we do more or not, that's the question. That would depend on the additional evidence and the additional details of this.

REG LEVY: Where do you see law enforcement? We're looking only at scenario four right now. And I'm just curious, because all of the things that you've brought up with regard to law enforcement are correct, it's just not in this particular.

VOLKER GREIMANN: I thought we started with one?

REG LEVY: Nope, nope, we're starting with number four, just confusing everyone. We work backwards, that's how we like to do things. Counting down. Okay, thank you, sorry about that.

FARZANEH BADI: But Volker, your point is very valid. The thing is, I also want to know about, so if a brand owner brings that complaint, what would the registrar do? And would they treat that differently from if a law enforcement agency actually brings up the issue? So that's my question. And I saw some hands up here. Yes, okay, great.

VOJISLAV RODIC: Thank you, Vojislav Rodic from .rs, Serbian registry. A brand owner accuses a website, probably the owner of the website. The first distinction I would make is purely technical. The phishing pages within a website can be a part of the website. You can reach them through the menus. So you could presume that it was the owner of the website that put them there intentionally and covered all the activity with a political or environmental protest or anything like that. Or the phishing pages were inserted by an unknown player, so the owner is simply not aware unless someone sends him a link that starts with a domain name, slash, slash, slash, and then something that you cannot reach through the menus the regular way, but the phishing page actually tweets, shares through any means that particular address. So it looks like it's the owner of the website, not necessarily, he could actually be the victim of manipulation in order for the phishing pages to cover the tracks. So let's clear that up first. One more thing. You mentioned deletion of domains. What do you mean by deletion? I mean, you can suspend the domain name. You can keep it reserved until some legal process is finished, and then you can either return it to its rightful owner, or maybe if it was an intellectual property, you can transfer it to the side that complains, or you can reserve it for another 1,000 years. We had such cases. But when

you say deletion, people usually think, oh, you just backspace, backspace, or delete. It doesn't exist. No, it's ready for registration the next millisecond. Thank you.

FARZANEH BADI: Thank you. So my clarifying question is that, does deletion of domain name never happens in DNS abuse mitigation? It does? Okay.

VOJISLAV RODIC: But it has to be reserved. If it's not on a reserved list, it's free to register again by anyone. There is no such thing. Domains are not in the cellar of the registry. They are in our heads. Oh, this is free? I will register it. Someone suspends the domain, and then deletion means it's free to register again. So usually, when you have some problem, we had a problem. It's public, so I can say. What was the abuse? In the .rs government, gov.rs is delegated to the government. Someone registered the domain, [inaudible] gov.rs. Nothing wrong with it. It's not on the reserved list. Several months later, a page, copy of the page of MOD, Ministry of Defense, .dot qov.rs appeared, and that's a similarity case. Oh, it looks so much like government. What it was looking for? It was looking for someone who works for the Ministry of Defense, who can log in through this domain page under QOV. So what did we do? First, suspend it. Two hours later, it was reserved for an indefinite period of time, so that nobody else can repeat that.

BRIAN CIMBOLIC: Thanks, Farzaneh. Just to note that, because to the specific question, does deletion of a domain name ever happen for DNS abuse? I think the answer is yes, particularly from the registrar perspective, and maybe Reg or someone else can chime in on this. But during the first five days, during the add grace period, if a domain name is registered for phishing, oftentimes the registrar will delete the domain name. At the registry level, we primarily suspend the domain name. The gentleman's point is well taken, though, that deletion is sort of not necessarily the best remedy for DNS abuse, because especially if it's done within the add grace period, that domain name does become immediately available again for reregistration. So does it happen? Yes. Is it often the best remedy? Maybe not. But yes, it definitely does happen.

VOLKER GREIMANN: So this says, accuse the website, not a domain name. So here we would have to differentiate what kind of website. Is it the main website of the domain name? Is it a subdomain? Is it, for example, a domain name that's being used for subdomain hosting or URL hosting? Is it a domain name that just, that is in other ways multiple uses? Is this phishing the primary use or not? So there's, again, we need to look at this specific case of what the involvement of the domain name is in this illegal activity. Is it a hosting problem? Is it a compromised CRMS? Is it something else? That is a review that we'll have to make. If we find that the primary use is that phishing and everything else is just tagged on, then this is an automated takedown. But if it's not, then we tell the complainant to go to the hoster or go to the registrant and clean that issue up.

MICHAELA SHAPIRO: Fantastic. I was just going to say thank you so much for bringing these and just to say quickly that we deliberately made these quite vague, so these are exactly the kind of contingencies that we want to be thinking through and this is exactly the kind of thinking that we'd like to be doing through the remaining three scenarios. So just to make sure, I don't want to cut the conversation short, but I do want to make sure we have enough time to go through the remaining scenarios and we are going to do breakout groups and to try to facilitate that, we, in an ideal world, will have somewhat equal balance of perspectives in each group, so it would be fantastic and I don't want to put everyone on the spot, but it would be amazing if you, let's say self-identify as someone with expertise from the registrar and registry perspective, if you could raise your hand, that would be fantastic. Amazing. I know there's a lot of you here. Fantastic, fantastic, fantastic. Anyone over here on this side? No? Ah, fantastic. Amazing. So, we can try to kind of self-sort a little bit. I'm trying to think of, should we have people sit or kind of move around? Fantastic. So now, so try to remember who raised their hands and try to self-select if possible to kind of spread yourself out around the room by each of those flip charts, so that was the registry registrar perspective. If we have people with a bit more of a kind of legal, policy, human rights perspective, could we raise our hands, please? Fantastic, fantastic. Alrighty. Yes, and if there's anyone with the law enforcement perspective here? Amazing. So, if we could try to separate the two of you, that would be amazing. That way, we can have that perspectives right around the room. Yes, intellectual property, business, yeah, yeah. Some of you might wear multiple hats as well, but yeah, at this stage,

maybe we can try to, as quickly as possible, if we can kind of self-sort. So, how about we all stand up, if possible, that would be fantastic. So we have flip chart, back corner, back corner, and back corner, so three, is that right? Yes, we have three. Fantastic. Thank you so much for your comments. Thank you so much. All right. All right. All right. Thank you. Thank you. Thank you. Thank you.

FARZANEH BADII: We are going to tell you what the groups discussed. In my group, we discussed all the scenarios, including number four, and on number one, which is the national oil company website, this was a clear case of DNS abuse. But we had a little bit of a conversation about whether there's a human rights impact. It's a national oil company. If the registrar suspends the domain name, then there might be some kind of societal impact. People may not be able to access services of the company. So there might not be human rights impact, but if there are drastic measures of mitigation, there could be societal impact or blocking access to essential services in people's day-to-day life.

We also had a good conversation on what mitigation mechanisms registrars use. It seems like these scenarios don't reflect everything that the registrar does and we need to be mindful of that so that a registrar might not go straight and suspend a domain name.

Scenario number two was human rights activist who owns a domain name and gets hacked by a state actor. Basically, in number two, we talked about whether this is DNS abuse. Yes, it is. And there are freedom

of expression and association ... And depending on how the registrar mitigates the abuse, it could also have impact on access to remedy.

So, there were really interesting solutions here. The group mentioned that the registrar could contact the domain name holder and discuss it with her, and tell her that her website has been hacked, and then what to do and how to protect her website. So, and also it was mentioned that we need an appeals mechanism exactly for these situations, and then also we could suspend it, but then we could reactivate it after a while. So, registrar could, maybe they can do that as well.

And so, for the scenario number three, which is a global footwear company, is it DNS abuse? The answer was no, but if the scenario had like some phishing angles to it, or technical DNS abuse definition that we have in the contractual amendment, if it leads to that, then it might be DNS abuse, but this scenario, it was clear that it was not.

So, scenario number four, we re-discussed this, especially from the brand owner and what they do, and this was also scenario number four, the impact on human rights and assembly and access to [inaudible] But, one of the most interesting part that we discussed, I asked, okay, so in this scenario, if the registrant, because they said that the registrar should contact the registrant and to have a conversation about what is happening to the domain name, but I said that, so what if the registrant does not answer, because they might be in jail, or, you know, and it was mentioned that the registrant has a contract with the registrar, and it is their responsibility to respond. So, and this was a very interesting part of that as well. Thank you. I'm done. Who wants to go through their own group?

REG LEVY: Sure. We were in the very back there. We talked a lot about the jurisdictional issues in scenario one, in terms of where the oil company was, where the registrar was, and where the law enforcement that was making the request was. The answer is different if they're all in the same jurisdiction than if there are mixed jurisdictions involved. We also talked a lot about whether the request from law enforcement was a request or an order, because those are also treated differently, especially if the law enforcement has jurisdiction over the registrar, because there are times when they have a choice, and there are times when they don't have a choice in terms of what their response can be.

For the second scenario, we talked about how the state actor took control of the domain. Because again, a state actor can take control of a domain by issuing a court order to the registrar and getting control of the domain. Typically, they don't follow up with malware, so this seemed like maybe it was an account compromise, and we discussed with some of the other groups that that's not something that a registrar can tell, that is, that the account has been compromised, so we would likely take action before we know about the compromise, and would find out about the compromise when the registrar contacts us, because their domain's not working anymore.

For scenario three, we heard that this would probably not have been forwarded as a typosquat, because it is an actual word. Mellow shoes means something different, and it's not merely similar to yellow shoes. That said, there might be issues where there were active MX records and evidence that it was being used for, for example, spear phishing, so we

went over that one as well. I think we talked about scenario four as a group, but...

MICHAELA SHAPIRO: I would just add, quickly, the only other thing we discussed in scenario three as well was just clarifying that this is not, in fact, trademark infringement, or at least, from the information we have, it does not sound like it is, but even if it were, in terms of how the response from the registrar would take place, that would be a different kind of response mechanism, so depending on the type of DNS abuse, and whether it even is DNS abuse, there will be a different process within the registrar and registries, kind of, there would be a different process that they would take in terms of how to address what this would be, and we discussed, kind of, across all three scenarios, we discussed where access to information would be a relevant part of the discussion, data privacy, anonymity, particularly in the case of scenario two with the human rights activists, that's a particular area of concern, where you want to be very careful about how you treat information requests, or sorry, that wasn't scenario one, that was scenario one, in terms of how do we treat requests versus, as Reg mentioned, a request versus an order is completely different, but even just what kind of information are you willing to give, depending on who is asking, that's also something that we kind of ran through, but yeah, maybe I'll turn it over here to Dennis.

DENNIS TAN: Yeah, thank you, Dennis, for the record, I agree with all your findings, I think our group is consistent with your findings or learnings, in scenario one, yes, different answers based upon who the actors are, you know, within the country or outside the jurisdiction, and in scenario number two, different questions about, you know, who's controlling that domain name, if we assume the state actor fully controlled the domain name, the registrar was not able to really talk to the registrar, but in order to minimize that impact, then the registrar, you know, the rightful registrar will have a process to reach out to the registrar and provide all the information, documentation, that they are the rightful owners and reinsert that domain name back to them. And in scenario three, yep, agreed, not DNS abuse, so fairly, quite simple, so, yeah.

FARZANEH BADI: Great, does anybody from the participants want to add anything to this? Okay, no. All right, it seems like we add to the participation, okay. Great, so what are the next, so first of all, we need feedback on these exercises, whether they were useful, whether they were not, how can we improve them, and if this exercise gave you some kind of like a better understanding of what we mean when we say we need to do human rights impact assessments for the mitigation of DNS abuse. One of the interesting issues that I heard in our group was that the mitigation mechanisms that registrars use in DNS abuse are more granular than we have in the scenarios. So it is not that the registrar just goes and suspends the domain name when they receive a DNS abuse report. If you want to mention your point on that, like how we should go about like talking about mitigation of DNS abuse?

UNIDENTIFIED SPEAKER: Yeah, I think that was the first scenario, yeah, where we were talking about those subdomains, and everybody was talking about, yeah, should the domain be suspended or not, and then I brought the scenario itself up, so yeah, we don't know what the name server is. We want to get the subdomains down, and the way to do that is via the DNS zone and the name servers, so yeah, we have to be specific when taking stuff down, so to reduce collateral damage.

FARZANEH BADI: Okay, great. So one of the points that also, like the overarching points that we kind of discussed was that the registrar has to also, I keep saying has to, please forgive me, I mean, it's better for the registrar to contact, like the registrant has like a line of communication, but also contact other actors, so hosting companies, if they know which hosting company it is. So mitigation of DNS abuse is a very complex matter, and I found out that it's not just about suspending or not suspending the domain name and there are many other steps that registrars use in order to tackle DNS abuse. And that could have an impact on human rights. It could, like with the mitigation mechanisms that registrars use, they could reduce the risk of human rights impact on the registrant. And so one of the issues that NCSG is very interested in is to look at what sort of practices registrars already do in order to—

REG LEVY: I didn't mean to interrupt you, I was just trying to get in the queue. One of the things that was helpful for me about this exercise was

underscoring the diversity of registrars. The reason that the DNS abuse amendments are vague, as Farzaneh mentioned earlier on in the session, is because there are so many different types of registrars and each of us might do something different when presented with a particular case. We don't conduct human rights impact assessments every time we receive a DNS abuse complaint, but we do care about our customers and we are trying in almost every case to protect our customers. If that means suspending a domain while the phishing is resolved by the customer, that's what we do. But again, we think about our customers in the actions that we take. We don't call it a human rights impact assessment. And again, I say we. Registrars do different things. There are different business models, there are different registrars, there are different jurisdictions, there are different things that each of our systems are capable of doing. The gentleman at the back talked about NS records. We don't actually have the easy ability to go in and edit those, so that's not something that we typically do. Other registrars might have set it up differently so that they can very easily and quickly make that change. So again, there is a diversity of what people do and this exercise really underscored that for me, so thank you.

MICHAELA SHAPIRO: Thank you so much, Reg, for that. And I would also say something that came out of the discussion for me as someone who is not, you know, has never worked in the context of a registrar or registrar, sorry, in a registrar or registry, is there's an element of, for example, we were talking about scenario two, the activist domain gets taken down and

from my perspective, from the human rights view, is, you know, like that's really a shame, we've lost that aware, you know, we've lost that information, we've lost the ability to get, you know, whatever issue that person was reporting, but at the same time, you can't blame the registrar because in that case, without knowing, without them being aware of the situation, they can't remedy it. So from the outside, right, we look, or at least I'll speak for myself, you look at registrars as kind of omnipotent, unknowing, and I think that's where there's a lot of space for us to do work together to talk about how can we ensure that registrants know what they're entitled to and how they can work with registrars and registries to ensure that if something does go awry, that they can, that they have avenues for support, and that's really great. I'll turn to you.

FARZANEH BADI: So I think that, but what you said is very important, Michaela. So we should not put, like, as a result of, like, all the DNS abuse mitigation and a lot of the, like, you know, the pressure that we put on the registrars to mitigate, mitigate DNS abuse one way or another. I think that we need to be careful and more nuanced in what we want from the registrars, because then what the registrar, I'm not talking about the registrars in the room, I'm talking about the registrars somewhere else, but, like, some of the registrars don't have the resources, they can't handle in a nuanced way, and the thing that they do is they, they just go with the easiest way, which is the suspension of the domain name, which can have an effect on the, on the domain name registrant and on human rights. So this is why we are talking about, we are, we keep saying that

a successful DNS abuse mitigation program and, and then the success, success of the contractual amendments does not depend on the, on all the DNS abuse that has been tackled and, like, I don't know, 3,000 domain names were taken down and stuff like that. It also depends on how we went about it, and if in the process of doing that, did we have an impact on the human rights of domain name registrants and on access to services, as we saw in scenario number one.

So it was a great conversation. As I said, this is the first time we are doing this, so we are open to, I mean, we are not the first time we are doing this human rights impact assessment, but first time we are doing it in the context of DNS abuse, and we are open to feedback and suggestions, and if you have any kind of, like, feedback on the scenarios or how these sessions should be run to be more interesting and more constructive, please let us know. The next steps are to discuss more and talk about and focus on each human rights. For example, here in these scenarios, we did not get to talk about privacy and how privacy can be impacted, so we will go back and we will talk with Reg and Dennis, and we will see what the next steps can be, or may potentially have, if you found, found this useful, potentially have another session in Seattle.

DENNIS TAN: You just stole my thunder. Yes, next steps, Seattle, and looking forward to keep working well for you guys. This has been a great exercise, I think raises awareness as to we contracted parties do in terms of mitigating DNS abuse, we care very much. We don't control the bad actors, I mean, unfortunately, but when we are aware of the issues, we take action, right, in a meaningful way that balances collateral damage.

FARZANEH BADI: Thank you so much, everybody. I just wanted to make another point now that I have the floor. I think that, so, with coming up with strict timelines, and for the registrars to take action, as a result of this session, I just found out that that could actually have an impact on human rights, and we have to be very careful when we talk, when we are suggesting that there should be swift action taken, so we have to be detailed and say in what circumstances those swift actions should be taken, and think about it more clearly, and yeah, that's it. Thank you so much, you can go to your break now. Oh, it's lunch break. Thank you, you can stop the recording.

[END OF TRANSCRIPTION]