ICANN67 | Virtual Community Forum – At-Large Policy Session: Tools for Wholistic Contract Compliance
Monday, March 09, 2020 – 13:45 to 15:15 CUN

JONATHAN ZUCK: It's kind of funny because one of the challenges I'm seeing with these virtual meetings that you're in front of your laptop even more, which means that there are five different ways that people are able to communicate with you during a session. Sometimes, that's the case in a public session but I feel like less so. That's one of the challenges to take note of, is the fact that there are too many ways for people to reach out to you in a virtual session.

CLAUDIA RUIZ: Yes, it's a lot going on. I agree.

UNIDENTIFIED MALE: And especially if you are on a board, right, Jonathan?

JONATHAN ZUCK: Exactly.

CLAUDIA RUIZ: Okay, if we could please start the recording? Good morning, good afternoon, and good evening, everyone. This is Claudia Ruiz from At-Large staff. Welcome to the ICANN67 virtual meeting and the At-Large policy session, the Tools for Wholistic Contract Compliance, on Monday the 9th of March 2020 at 20:30 UTC.

The audio room is in English. In order to access the French or Spanish audio, please join the French or Spanish streaming via the link on the main ICANN67 website. All details were sent out on the ALAC [announce] with all relevant links. Details for these connections can also be found on the ICANN67 At-Large Wiki agenda pages.

We will not be doing a roll call today for the sake of time but ALAC members, RALO leadership, and liaison attendants will be noted. If you would like to ask a question or make a comment in English, French, or Spanish, please type it in the chat by starting and ending your sentence with "question" or "comment."

French or Spanish questions will be translated into English and read out loud by our remote participation manager, myself, Claudia Ruiz, or Gisella Gruber. Staff will put periodic reminders of this process in the Zoom chat. If you are in the Zoom room and wish to speak, you may also raise your hand and staff will manage the queue.

A kind reminder to please state your name when speaking, not only for the transcription purposes but also so the interpreters can identify you on the audio streaming. Please also speak clearly and at a reasonable speed to allow for accurate interpretation.

Finally, this session, like all other ICANN activities, is governed by the ICANN expected standards of behavior. I have put a link in the chat for your reference. So, without further ado, I pass the call over to you, Jonathan Zuck.

JONATHAN ZUCK: Thanks, everyone. By the end of the day, you're going to be well and sick of my voice, but we're going to continue our discussion of DNS abuse. We just got done with a session that was kind of a DNS abuse 101, the first draft of a DNS abuse 101 discussion and some of the issues of concern to the At-Large, in particular, about DNS abuse and some of the challenges that are faced within the ICANN community.

So, this next session is specific to contract compliance, and we're honored, here, to have the head of ICANN contract compliance to be one of our participants, along with James Bladel, who is the head of policy for one of the largest, if not the largest registrar, GoDaddy.

I guess I'm buying time until the slides appear on the screen. We had a previous session two meetings ago with Jamie and Graeme Bunton from Tucows in which we discussed some of these issues. In that session, we talked quite a bit about the DNS abuse framework that has been created by a number of the contracted parties that began as 11 but is now 48 in number, so that's great to see that grow.

What we wanted to do was get to the notion of how to go after the bad actors, in particular, so that's the purpose of this particular session. Next slide, please.

So, when we think of the At-Large and DNS abuse we consider this to be the number one issue facing individual end-users. Just day-to-day users trying to use the Internet aren't paying that much attention to what's going on inside the ICANN community, and frankly, even when I was a software developer, a fairly technical person, I wasn't paying attention to what was going on in the ICANN community either because you just come to expect things to just work, but DNS abuse is something that has large downstream consequences for folks that are, as I said, just trying to use the Internet.

The At-Large, if you were watching the last session, has resolved to combat DNS abuse both through end-user education on social engineering and computer hygiene, as well as advocacy within the ICANN community. We're advocating for increased research on predictive analytics, new mandates to compliance, and then potentially modifications to the agreements that ICANN has with registries and registrars, so this is the most controversial part, if you will, of what we're trying to propose, and that's the reason for this discussion. Next slide, please. Next slide? Oh, yeah. Thanks.

And so, one of the things I wanted to do – and it's perhaps a little too cheeky of me so I'll give folks a chance to clarify their positions rather than just steam-rolling over this, but in broad strokes what came out of the previous session we had, in which James also participated from the audience, which is why I asked him to participate in this session—thanks, James, for doing it—Jamie's point was that compliance is rigorously enforcing both the registry and registrar contracts and that it's really up to the community whether those contracts are enough or not.

And so, I think we're constantly trying to put Jamie in a position of making that assessment, and he wants to throw it back to us but I'll give him a chance to clarify in a second if he'd like. And as for James, if I sort of recall some of his points from the previous session, one is that he's concerned about—and this probably applies to the signatories on the best practices pledge that's at dnsabuseframework.org—the distinction between DNS abuse versus content abuse, and where that line needs to be drawn, and where ICANN's role might be limited. We'll be, actually, addressing some of those scenarios in this discussion.

As far as current contracts, James has stated that he thinks that contract compliance has tools that they're not using. This comes up a lot with regulation; rather than adding new regulations, let's enforce the ones we have. So, he'll talk a little bit about that. There are some industry-led efforts. They are proposing that instead of new policy, which includes this framework to address DNS abuse that we've had some discussion about, and there has been some talk of financial incentives from ICANN to encourage contracted parties to adopt these best practices.

And so, James also made the point in the last session that sometimes when you write down or set in stone the practices you actually limit the flexibility of contracted parties in what is a constant arms race with the DNS abusers. And so, leaving some of this at the discretion of contracted parties can be superior.

So, before moving onto the next slide I wanted to open the floor to both Jamie and James because I am trying to zip through their positions and speak for them. If they want to make any clarifying remarks before we dive in, I wanted to give you the opportunity to do so. Jamie, go ahead if there is anything that you want to say by way of introduction.

JAMIE HEDLUND: Sure. Thanks, Jonathan, and thank you again for inviting me to participate on this panel and engage directly with ALAC. As you said up above, we like to believe in contractual compliance that we vigorously enforce the agreements that we have with the contracted parties. Sometimes in the community, there is a misunderstanding about what's actually in the agreements. And so, these types of conversations are helpful in elucidating what types of provisions exist and what types of provisions do not exist.

In terms of the additional tools that may be out there, traditionally contractual compliance has applied individual provisions that apply to individual complaints. And so, we have WHOIS inaccuracy provisions, we have the 318 that you mention, investigate and respond, etc.

We have not taken an—I hate to say it—Wholistic approach toward enforcing any of the agreements. And so, I know James and others have suggested that there are tools that we might have under the agreements writ large that we haven't used to date. It is true that, in section five under the termination provision, that's something we have looked at being enforced by others against registrars and then implementing it.

We're very open to any kind of creative ideas. The last thing I would point out is one thing that's often missed is that the data that we have, from DAAR primarily, is that a very small number of registries and registrars are responsible for the vast majority of DNS security threats: phishing, malware, botnets. Most recent month that I saw, 90% of the abuse was being perpetrated by 20 or fewer registries.

The challenge we have is, how do we make sure that we have tools that allow us to go after the worst of the worst without unduly hampering those who do way more than the agreements require in terms of mitigating DNS abuse? With that, I'll turn it over to James.

JONATHAN ZUCK: Thanks, Jamie. James, go ahead.

JAMES BLADEL: Thanks, Jonathan. Thanks, Jamie. Hopefully, you can hear me okay.

JONATHAN ZUCK: We hear you fine.

JAMES BLADEL: Great. First off, I just wanted to say thanks to you, Jonathan, and ALAC for putting this together, for putting together the previous session as well, and keeping the conversation regarding DNS abuse front and center. I think at this stage in the game the entire community could use a break from talking about privacy so this is a welcome change of subject.

I think I agree mostly with some of the points Jamie made, that it's important to recognize the complexities around DNS abuse, and in addressing it, and in mitigating these issues, and making a dent in some of these global problems/global challenges.

It is important, I think, for everyone in this community because we're supposed to be the experts, now. It's important for us to evangelize those complexities and to ensure that folks are not tempted by over-simplistic ideas or solutions like "compliance is just not doing enough," and "registries and registrars are hiding behind their contracts," and things that ascribe negative motives to other actors in the community and in the ecosystem who are all, really, trying to do their best with the limited tools and authorities that they have.

So, with that in mind, I think I wanted to reference some of what Jamie pointed out, that ICANN's scope in this regard is somewhat limited by its contracts. Those contracts can be changed—I saw one of your bullet points previously—but there are legitimate pathways to pursuing those changes and they must be done according to those prescribed processes.

It is also important to note that the bad guys are very well aware that ICANN conducts its work at a certain pace and out in the open, which is one of the reasons why, and I know others have put forward the idea that industry cooperation and initiatives like the framework to address DNS abuse can be more flexible, more dynamic, and also to some extent more confidential in sharing those types of inter-industry efforts and can be more effective in addressing abuse.

I think it's very important. I know you did it in the previous session and I think that it's front-and-center in the framework, as well, to try to establish where the boundary lives between DNS abuse versus just general content abuse. I think it's tempting, again, just one of those overly-simplified arguments, to say that since all bad things on the Internet require the DNS, or nearly all of them require the DNS, that therefore the DNS is the appropriate choke point to look at combating that abuse. I think that's something that we need to view with some degree of skepticism, particularly given ICANN's limited role.

I also would agree, and I think raised this in Montréal, that it's not just a matter of enforcing the letter and the law of each of these contracts and contractual provisions between the registries and registrars, but also important to have an overarching perspective of habitually bad actors who are either negligent in their practices or possibly even complicit in some of the abuse that's occurring on their platforms, and to bring to bear all of the tools in compliance's toolbox against those folks.

Yeah, I think that covers everything. I do note that financial incentives is something that has come up fairly recently. I think it was part of the CCT report. As a registrar, I would say, "Fantastic. Please give me money for things that I am already doing." I would welcome any type of plan that results in getting paid for things that are already happening.

But as a participant in the community, I think we also have to ask the questions of, "Where is that money coming from?" and, "are there ways for those types of incentives to be gamed or abused themselves by folks maybe not operating in good faith?"

I'm happy to just leave it there, leave it relatively informal, and we can address the questions as they come up. I'll turn it back over to you, Jonathan. Thanks.

JONATHAN ZUCK: Great. Thanks, James. Thank you both for participating and for keeping the introductions brief because I think we wanted to just get an informal conversation going. It seemed like the best way, potentially, to do that is to look at some scenarios. I think, ideally, we regard them all as hypothetical scenarios and try to get a sense of how we think the process would work today. That might help to reveal where there might be deficiencies in the tools that are available.

So, next slide. Yeah. So, this was the other positions recap. There are many of us that think that this current status quo is not enough despite the efforts of, as Jamie said, the majority of the contracted parties. There has got to be a way to deal with the bad actors better since the incidences of DNS abuse are going up.

There is a belief on the part of all of us that contract compliance is not empowered to deal with what might be called "systemic abuse," the idea being that they're only able to respond to complaints in a piecemeal fashion, as opposed to being able to look at contracted party as a whole, either the registrar practices or the registry itself, which is what allows something like .science to have the problems that it did, for example.

But being reactive is not enough and compliance need new tools and maybe a mandate for some of its existing tools such as its audit function and things like that. That's the end of my introduction. Next slide.

So, the scenarios that I wanted to use for the basis of a conversation could be real or hypothetical but the point is to treat them as hypotheticals and delve into what the best approach would be. And so, what I'm hoping to do—and I hope this works as a format—is present a short scenario and then ask the both of you how you believe this should be handled today.

What tools should be used for that to handle that particular scenario? Do we think the use of those tools would lead to favorable outcomes, which in some cases might be a behavioral change on the part of the party that is in question or would lead in a reasonable period of time to a breach notification and/or suspension? Those are kind of the questions for each one that I'll want to pose to both of you as we go through these scenarios.

Again, we're looking right now at whether compliance has the tools it needs. I think that the best practices question is an incredibly important one, and how to get more people to sign onto that framework or even look at how that framework might be enhanced is worthy of its own session. I don't mean to be dismissive of that at all, and all the work that has gone into that thus far, and the work you're already doing on DNS abuse mitigation. Next slide.

So, here is the first scenario. Two names are registered with actual Facebook identity information. In other words, their name, their address, etc. That's what's in what was previously WHOIS records and now is registrant data records, etc., but they're using Facebook's information. Those domains are used actively for abuse.

Tens of thousands of end-users are targeted through messenger using those two names, and so it is reported to the registrar and contract compliance that that's what is taking place. And so, then, my question is for both of you. What should happen? What should compliance do? How long should it take for this to be resolved? I'm interested in hearing from both of you what you believe the tools are to take care of a situation like this. I don't know who should go first, but maybe Jamie.

JAMIE HEDLUND: I'll go first.

JONATHAN ZUCK: Sorry.

JAMIE HEDLUND: No, I volunteered first. This, as far as I can tell, sounds like a WHOIS inaccuracy complaint with a possible abuse report, as well, but on its face, it looks primarily like a WHOIS inaccuracy.

What happens with those is someone submits a complaint to compliance of inaccurate WHOIS records. We first make sure that there is evidence to support that there is an inaccuracy, evidence like a bounce-back of an e-mail address, and assuming that that evidence is there we then go to the relevant registrar under the agreement, under section 378, another WHOIS accuracy program specification.

They have, I believe, 15 days to investigate and take action is there is inaccuracy. It can go back and forth a few times so that if it's not done we send a second notice, and eventually a third notice, and potentially a breach. So, it can go three days or longer before inaccuracy is adequately addressed. There is no … No, I'll leave it at that. So, that's the standard approach.

JONATHAN ZUCK: So, just to clarify, Jamie, you think it's probably, at minimum, a 30-day process to get to those names being taken down. How would that happen? What would lead to those names getting pulled?

JAMIE HEDLUND: It doesn't have to extend to 30 days. Lots of registrars do it even within the 15 days that they have under the agreement to investigate. And then, if eventually they don't respond it, again, escalates to first, second, and third notice, and then the formal breach notice. They are expected to, if it doesn't have the correct information, either to get the information corrected from the registrant or suspend the domain.

JONATHAN ZUCK: Thanks, Jamie. James.

JAMES BLADEL: Jonathan? Can I jump in here?

JONATHAN ZUCK: Yeah, please.

JAMES BLADEL: Great. Hey. First off, I should apologize in advance because it's going to sound like I'm picking apart your scenario and I'm not doing that. I think this is a really valuable exercise but I do want to go back to what I was saying about being careful not to oversimplify because I think there are some really crucial details missing in order to describe how this is currently or should be addressed.

First off, when we say that domain names are registered with Facebook information in their WHOIS but they're being used actively for abuse, I'm not 100% clear on how the domain name fits into this type of abuse. Can we say, for example, that we're phishing for Instagram or some other service credentials, or WhatsApp credentials, and so someone thinks it's coming from Facebook so it sort of has some credibility?

JONATHAN ZUCK: Yes. Yeah, that's a good idea.

JAMES BLADEL: So, in that particular case … I mean, first of all, I should come to Jamie's defense a little bit here that the ICANN process, as he illustrated, there is going to be a bit of a back-and-forth between the registrar and compliance and the registrant on giving them a window to update and correct obviously false, or incomplete, or out of date WHOIS information. So, that's probably not the fastest path, particularly for something where the harm is being measured in hours. Giving someone seven days to update their WHOIS information is just too big of a window if you're dealing with a truly bad actor.

Instead, reporting to the registrar, and if it's a large registrar and it's also a hosting provider, for example, like GoDaddy, you're going to have a lot of different avenues to file and submit a complaint. And so, for example, saying that "this domain name is being used in conjunction with a phishing attack that's targeting users of Facebook Messenger, and here is the domain name," one of the first things a registrar is going to do is try to figure out if they are actually managing that domain name as a registrar, and then also hosting that phishing payload content as a web host, because that gives them a completely different avenue, perhaps, and a different toolset to bring to bear that might be able to detect and address this faster.

I know that in some cases they're not, they're one or the other; the registrar, for example, and not the web host. I know that sometimes that's perceived as a bit of a pass-the-buck exercise but, really, what it's saying is that "I understand and appreciate that abuse is occurring but it's not occurring on a platform that I can control.

But stepping back from that, let's say that they are one and the same. Then, the registrar and the web host probably have some active measures that can be brought to bear with their own anti-abuse policies in terms of service, so that they can either suspend or shut down the website that this fraudulent domain is luring users to, and perhaps get that done in a matter of hours rather than some of the stuff that Jamie was discussing, where it's measured in days.

I want to say that if it's the case where the registrar doesn't have a clear method for reporting those abusive activities or if you report those activities and the registrar, essentially, just is radio silent, then I think it's time to get ICANN contractual compliance involved because, while ICANN contracts with registries and registrars are not overly prescriptive on how to address abuse, it is very clear that we do have to have procedures available and that we have to publish the entry points for those procedures, as well.

I think there was a very good blog post, recently, that outlined what the expectations are from ICANN of its registries and registrars in having abuse mitigation processes.

So, I'm not trying to overly-complicated your scenario, here. I think this is a good exercise but I think in the real world what we see is, the closer the proximity to the content that we are as a provider, the faster we can act and the more tools and processes we can bring to bear to shut these things down.

As a web host, we're very close; as a registrar, we're arm's length. I think poor Jamie is over there – contractual compliance is several arm's lengths. But if the first two are absolutely non-responsive then I think ICANN compliance is our only and most appropriate step to bring to bear and ensure that registrars are taking this responsibility seriously.

I don't know if that's helpful or if I've just taken this conversation off the rails but I think it is important to recognize the different layers of the ecosystem and how they all have a different perspective and a different approach to dealing with this kind of a scenario.

JONATHAN ZUCK: Thanks, Jamie. I really appreciate that context and perspective. This, in fact, was a true scenario. There were two domain names and both contract compliance and the registrar in question were contacted. The turnaround time for the resolution of this was 60 days. It took two months for two domain names to be taken back after the abuse was reported and 30,000 users were targeted with the phishing attack.

Just to give some context, I don't mean to say that complainants shouldn't reach out to the closest party but that is part of the difficulty, I think, that we'll find, that, again, how can compliance better deal with bad actors? Obviously, contacting you with this problem would have resulted in it being taken care of more efficiently than what happened with the registrar in question. Fabricio has his hand up, I think, with another example of this. Fabricio, why don't you go ahead?

FABRICIO VAYRA: Thank you. Can you hear me?

JONATHAN ZUCK: Yes, I can.

FABRICIO VAYRA: Perfect. Thank you, Jonathan. Yeah, I just wanted to jump in, here. We've done enough of these that I'm not sure if it was this exact example or another one exactly like this but the more you describe it the more it sounds like our exact example. I just wanted to chime in because I know James said, “In the real world there are ways to get out of this.”

In the real world, we recorded exactly this: two domains with a brand being used for fraud. We reported it to the registrar. The registrar acknowledged that they were fraudulently registered, acknowledged that the brand owner’s name had fraudulently been used to register domains, but refused to take the domain names down.

When we went back and invoked the RAA and told the registrar—in this case, it was OnlineNIC—and asked them, “Well, if you’re not willing to take the domain names for fraudulent registration then you have to acknowledge who is in the registrant field,” which was the brand owner.

“Under that, you’re acknowledging they are the registered name holder and you need to transfer the names or drop them at their request,” at which point the registrar came back and said, “Well, no. They’re fraudulently registered.” So we said, “Well, which is it? They’re either fraudulently registered and you need to act under the RAA and drop them,” and they actually acknowledge they’re fraudulently registered to scam people, “or you have to transfer them because the rightful registered name holder as listed is the brand owner.”

When they refused to do anything, we contacted ICANN. I'm happy to provide the correspondences if people want to refresh their memories but I believe that myself and Jamie's team had a long back-and-forth, at least two months. At the end of the day, ICANN just continued to close the ticket; "Well, we think the registrar responded to you." We said, "Well, no, they haven't because they violated the RAA in two or three different instances. And so, now you need to do compliance on them and you need to take care of the domain names."

And so, in the real world where a registrar has acknowledged that two names have been fraudulently registered under a brand owner's name and used to phish that brand owner's users, that registrar did nothing and argued with us. When we pulled in ICANN in the real world what compliance did was continue to contact the registrar then close the ticket. This happened for months.

I guess in the real world what we're seeing under this example is that there is just this vicious loop. And so, I think this is actually a really great example where … We've had a lot of talk about, I think, a dichotomous argument of "the agreements can't be too narrow because then that ties our hands, but then if they're too broad, well, we can't interpret them that way."

I don't think there was much issue in this scenario, which matches what you have on the board, and yet it took months to do anything. At the end of the day, the registrar was never reprimanded or compliance put on them. I don't believe that ICANN actually acknowledged anything that we asked them to do.

The names, I think, at the end of the day, just ended up dropping but by then, as we talked about, as James admitted, we're measuring these harms in hours, not even days. It took months to take care of two domain names that were being used, acknowledged by the registrar, as fraudulently registered for fraud purposes, and they did nothing and ICANN did nothing.

I just thought that it would be good to have context of the real world because I was actually involved in one of these. Anyway, thank you for that.

JONATHAN ZUCK: Thanks, Fabricio. Yeah. I think it's right that it does raise an issue of, when the contracts are vaguely worded, it says, "You must have a policy in place," and if that policy becomes more of a checkbox then it becomes difficult for ICANN compliance to go further because whatever policy was in place was followed but that policy wasn't sufficient. James, go ahead.

JAMES BLADEL: Yeah. Thanks, Jonathan, and thanks, Fabricio. Just to respond, I actually know we've had incidents in the past where we have simply done a transfer or a change of account of a domain name that was either involved in phishing, or infringement, or something like that, because the registrant information was that of the brand holder or the target of the phish.

So I think, in that case, you are correct. The registrar had a decision to make; either this is a name that was fraudulently registered or it is not fraudulently registered and it's the property of the brand and it needs to be transferred to them for them to do with as they please.

Sitting in the middle like that, I think it is appropriate to contract compliance. Not to put Jamie on the spot, I am curious why compliance wouldn't force them to choose one or the other, but not both and not neither. I think that, in our experience, we've been put in that situation and we've said, "Fine. These domain names belong to the complainant."

JONATHAN ZUCK: Jamie, did you want a chance to respond? Okay.

JAMIE HEDLUND: Yeah. It's o putting me in a difficult position because I don't have the complaint before me and I'm not familiar with it but I'm happy to go over it again with Fabricio and review whether or not there was something more we could have or should have done.

JONATHAN ZUCK: Yeah. I'm not trying to put you on the spot for something you might not have … These are meant to be more hypotheticals. I feel like the conversation is going well so let's make a note to follow up on that one.

Steiner mentioned that there would be a possibility of the registry being able to take action in addition to the registrar, so I just wanted to make a note of that comment from the chat. Let's go onto the next scenario. Alan, I see your hand is up. Do you want to say something before I move on? Alan Greenberg?

ALAN GREENBERG: Sorry, someone muted me on Zoom.

JONATHAN ZUCK: Okay. Go ahead.

ALAN GREENBERG: If you were taking questions after the first section, where Jamie and James made their presentation, I would have made a comment saying, "It's really encouraging to hear representatives of both sides, as it were, saying 'there are problems and we are looking for tools to fix them.'" Nobody mentioned "it's not a problem," or "it's so vague we can't address it," or "it's outside of ICANN's remit or outside of contracted parties' remit." That was really positive.

Now, you have your hypothetical case which clearly wasn't just hypothetical. It's clear that the processes in place don't necessarily work. Now, they may well have worked if the registrar had been James or another one of the people who get it, but clearly, it doesn't work in the general case.

I really think going forward—and we'll go back to your cases—we need to figure out how we can accept the reality that it's not always working despite the best of intentions, and how do we put a process in place, whether it's frameworks, rules, or whatever, or contracts, so that we actually can address these real problems?

I think when we're looking at these cases we need to think that if it's not working today for whatever reason, be it bad will or simply we don't have the right tools, we need to think about what do we really need to move forward and tackle this.

JONATHAN ZUCK: Yep. Thanks, Alan. I think, hopefully, the whole purpose of this conversation is to help percolate up to the top some of the things because we know it's not bad will on the part of most people involved. You mentioned the general case that it's not working but I think we can see it as the exception case. It's still widespread enough that we need to find the best way to resolve these things going forward. James, you wanted to respond briefly to Steiner's point, so go ahead.

JAMES BLADEL: Yeah. Thanks, Jonathan, and thanks, Steiner, for the question regarding the registry operator. I just wanted to note that, at least in the gTLD space, registry operators should not be viewed, necessarily, as some sort of a point of escalation. They are even further removed in terms of proximity to the abuse than the registrar and certainly do not have the relationship with the customer the way that the registrar does.

So, I would caution folks about holding up the idea that the registry is an alternate pathway to getting something done when the registrar is not responsive, and I think that the appropriate role for the registry is to continue to monitor whether or not the registrars have anti-abuse practices and policies in place, and whether or not they are living up to those.

I think PIR, for example, with .org, is a good example of a registry that monitors their registrar's performance in this area without actively intervening in specific cases, just because I think they recognize that that is fraud with the problems, as well.

I just wanted to address that because I think it's a good point and I think it is a perception that, "Well, I didn't get what I need from the registrar. Now, I'm going to go to the registry," isn't always the right approach. Thanks.

JONATHAN ZUCK: Thanks, James. Next slide, please. So, the next scenario I call whack-a-mole. I don't know with an international audience if this is completely familiar but it's a game you play in an arcade where these little moles pop up from their holes and you have to whack them with a hammer. And so, you're in a process of constantly trying to whack the moles as they appear. And so, it has become kind of a metaphor, in English at least, for having to solve the same problem over and over again. Next slide.

In this particular case, we have a situation where a registrant has registered 1,000 domains and 10 have been reported and taken down by the registrar but despite, requests by a business and/or government agency, the registrar will not take down all 1,000.

The question then becomes, is there a way to get to a point where a particular registrant has demonstrated sufficient ill intent that these takedowns can happen in a less piecemeal fashion? And so, that was, again, "Is there something compliance can do or instruct registrars to do in this particular case?" Jamie, I'll put it up to you first, again.

JAMIE HEDLUND: Thanks, Jonathan. So, I guess it would help to clarify what the interaction with compliance has been. If there were ten complaints submitted, or complaints about ten domains submitted, and they were taken down or an action was taken against them, that's the beginning and end of the complaint. We don't have authority under the agreement to say, "Well, these are ten complaints by registrant X, and so, therefore, you must take down the other 990 also registered."

We sometimes, for a complaint involving 1,000 domains, don't necessarily require 1,000 separate complaints, but the information and evidence in support of the complaint for each of those domains is necessary for us to pursue them.

I know that in some instances registrars on their own will see a pattern and go beyond the scope of compliance's interaction with them and, on their own, take down the remainder or take down many other sites/domains registered, but that's done on their own initiative and not because of the complaints or the agreement. Thanks.

JONATHAN ZUCK: Thanks, Jamie. James, what's your feeling on this? Again, obviously, if it came to you it might be easier to twist your arm to get the rest of these taken down or you might do that automatically, but what do we do in a situation where the registrar is resistant to taking a broader response to what is clearly a malicious registrant?

JAMES BLADEL: Yeah. I want to, I guess, back up a little bit what Jamie is saying. I think one of the points he made was ICANN doesn't necessarily have the authority to take down the other 990 just because ten had been suspended, but we do as a registrar and it's one of the first threads that we would pull as part of this investigation to determine what other domains are associated with this registrar account and what they are doing with them.

But we may decide not to take all of them down or some of them down. We may have a situation where the registrant, unbeknownst to the reporting party, is actually a boutique web designing firm with 990 innocent clients or blogs and ten bad guys, or grey actors, or whatever, that have been taken [action apart].

Registrars need that level of discretion to conduct those investigations and to not have these sorts of all-or-nothing tools, to be able to act with some degree of precision and say, “I'm taking down the names that have been actively involved in abuse and I'm not taking action on the names that have not.”

It really situationally depends upon the circumstances that are involved. I think if it is, in fact, the case that you have 1,000 domain names and each and every one of them is involved in some sort of abusive activity then it might necessitate 1,000 separate complaints or it might necessitate a complaint to ICANN about each of the ones that the registrar did not act upon that it could clearly be demonstrated that they should have.

But it sounds like, overall, that the concern here is that the registrar has some degree of discretion in how broadly or how narrowly their sanctions will fall on the registrant. I would argue that we need that level of discretion and, while it may not always satisfy those who are filing the complaints, that doesn't necessarily mean that the registrar has done something wrong.

JONATHAN ZUCK: Thanks, James. Great point. Again, we find ourselves making a distinction between the good actors and the bad actors. Once that position is made with the registrar and they’re not able to point to the fact that they’re a boutique website creator or something like that then, what could happen next, I think, is the question, again: "What do you do with a registrar that isn't as proactive as you are?"

JAMES BLADEL: Well, can I build on that for just a second?

JONATHAN ZUCK: Sure, yeah.

JAMES BLADEL: What it assumes is that that distinction that the registrant is a good guy whose account, maybe, has been compromised or a bad guy who is actively involved in the abuse, sometimes that's not obvious.

What I'm maintaining is that it's important for registrars who do their diligence and are effective at addressing abuse that have the ability to act according to the circumstances and not be tied to some one-size-fits-all policy, or rule, or some edict from compliance. I'm not picking on Jamie here but it's just it is discretion that we have and that we use to be as effective as possible and to account for all of the different circumstances. It's not a cop-out, it is something that we try to use effectively.

JONATHAN ZUCK: Yeah. I'm not accusing of copping-out, it's just a question of given—again, back to Alan's point and the point of the session—that if there are failures that are occurring now, what if anything can we do, or can compliance in particular be empowered to do?

And so, you're saying you think that empowering compliance in this particular case with some new power would have downstream consequences for your ability to protect a registrant that had a legitimate issue that you'd be solving through other means, it seems like.

Let's go onto the next slide. Here's another one where I've used Facebook as an example. If a registrar allows privacy proxy registrations of the following domains – you can see there is Facebook, there are Instagram ones, there are WhatsApp ones. Some of these are just typos, some of them use IDNs, etc.

And so, the business in this case, the hypothetical business, is Facebook. They come to the registrar and ask for information about the registrant behind these somewhat fairly obvious abuse-oriented domains and the registrar refuses to share that information, what do we think should happen in this scenario? I'll go to Jamie again, first.

JAMIE HEDLUND: Thanks, Jonathan. Maybe I didn't say this earlier but I'll look at this as hypothetical and not about any …

JONATHAN ZUCK: Please, yeah. I don't mean to put you on the spot of a particular case.

JAMIE HEDLUND: There are obligations around privacy proxy providers and we enforce those. Specifically, they do need to post what their terms and conditions are. And then, once those are posted, they're supposed to implement them. When we get a complaint, we look to see, first of all, how they posted their policies.

And then, the next thing we look at is whether they have enforced it. The agreement does not require anything in particular to be included in their policy and so, typically, the provider maintains full discretion to interpret, apply, and take down or not, as they judge best.

It does create a frustrating position, I'm sure, for many who are unhappy with potential fraud being perpetrated under these domain names. That's, in a nutshell, what we do when we get a complaint.

JONATHAN ZUCK: Thanks, Jamie. James, do you want to share thoughts on this scenario?

JAMES BLADEL: Sure. Just so I understand the scenario, this is just the privacy service has simply allowed these registrations to occur, or is there something …?

JONATHAN ZUCK: Yeah. They've occurred and then they've been contacted by a company and asked for the registrants behind them because they were flagged as potentially abusive in some cases and actually abusive in other cases. Let's say that that's the scenario, and the registrar has refused, then, to share the underlying registrant information.

JAMES BLADEL: Well, first off, I think, a couple of distinctions I want to make. The first one is that I wanted to be sure—thanks for the clarification—that the concern wasn't that these weren't somehow screened, blocked, or detected at the point of registration because that is, as we have indicated for a number of years now, both operationally challenging and also … Okay, are we done?

JONATHAN ZUCK: Way to go, James. You broke it.

JAMES BLADEL: I broke it. Okay.

JONATHAN ZUCK: James!

JAMES BLADEL: Yeah. I have that effect on machines, apparently. But the second point I wanted to raise is that [cross talk] may or may not be an independent entity with its own terms of use, which could potentially be brought to bear on these types of registrations. So, filing a complaint with the privacy proxy service is one approach, one avenue, that might bear fruit.

And then, if it is in fact affiliated with a registrar or the registrar record has underlying customer information that is distinct from the privacy service, then I think that filing a complaint with the registrar next is the next step. And then, finally, if there was a clear case where that's failing then maybe there is an avenue with compliance.

I just want to point out that in all cases … I think, now, part of this, we want to maybe poke some holes in the privacy proxy PVP that's kind of on hold, and then the temporary spec/ePVP, which is also wrestling with some of these issues. So, I want to be careful to not make blanket statements that undermine years of work and some of the very complex issues in play, here.

I think that generally, if there is for example a URS or a UDRP file, in almost all cases that cuts through the clutter fairly quickly and gets to the underlying customer information, even if it's just simply releasing it to the panelists, or it gets these names suspended quickly. Alan says, "it doesn't say a privacy proxy service was used, it says 'scenario: privacy proxy service,'" so I apologize if I have misunderstood.

JONATHAN ZUCK: That was the hypothetical, yeah.

JAMES BLADEL: All right. So, that was my assumption, as well. The privacy proxy service introduces another actor which may or may not be affiliated with the registrar, which may or may not have its own anti-abuse policies. But certainly, only the registrar would be subject to a complaint to compliance, not the privacy proxy service. I'll cut it short, there. Thanks.

JONATHAN ZUCK: Thanks, James. Fabricio.

FABRICIO VAYRA: Thanks, Jonathan. Can you hear me?

JONATHAN ZUCK: Yes, sir.

FABRICIO VAYRA: Awesome. Thanks. Cutting through a lot of the … Once you contact the "privacy proxy"— I guess I'm doing air quotes here because we don't really know if it's a privacy proxy or someone just saying that they are to mask their fraud. Let's say you contact whatever information you have there and you get no response, and then you go to the registrar and you get no response.

Shouldn't you be able to go to ICANN under the 2013 RAA where it explicitly says, under 3.7.7.3, that if someone's contacted a registered name holder—which by definition is who has listed themselves in the registrant field, so be it a privacy or proxy service that has decided to do that and provide a service, or otherwise—whoever is listed there is the registered name holder?

And if that registered name holder is provided information of actual harm and does not release that information within seven days of who is the underlying registrant, they're liable, right?

Either ICANN or the registrar should be able to take direct action or the aggrieved party should be able to sue that person directly because they're not saying anyone's underneath and, frankly, we don't have a policy to ensure that they are or aren't an actual privacy proxy or anything else. All we know is that they are listed as the registered name holder and they refuse to let you know something else.

I guess my question to compliance is, or the registrar to James, under that scenario, don't we just default to 3.7.7.3, mark you up as the registered name holder, and take action against you, as you would have to under the RAA for using your services for abuse? Or, isn't it appropriate for, in this instance, the brand owner to just go ahead and sue the "registered name holder," whether they say they are privacy proxy or otherwise?

JAMES BLADEL: Jonathan, I can respond to Fab, if you like.

JONATHAN ZUCK: Yeah, go ahead.

JAMES BLADEL: Yeah. So, I think you've got a couple of points, here. One is that you were talking about 3.7.7.3 and the statement, I think, that says the privacy service, if it is affiliated, that the registrar should acknowledge that, otherwise they'll take legal responsibility for the use of the domain name.

I think that another, and perhaps more appropriate, way for ICANN compliance to get involved would be enforcing the Temporary Specification on privacy proxy registrations, which is what's attached to the 2013 RAA. In the absence of any permanent policy, we just keep renewing this agreement that is not as strong, I think, as some proposed policies but does say, essentially, that the privacy service, if it's affiliated with a registrar, should have a point of contact, should have clear terms of service to address these types of issues, and should be responsive to outside complaints of abuse.

But I think, going back to your first point, we also have to determine if this privacy proxy service is indeed a privacy proxy service or just a bad actor pretending to be one. If it is a legitimate service, is it affiliated with the registrar? There are a couple of different threads we can pull on this scenario. Thanks.

JONATHAN ZUCK: Thanks, James. I guess I'll make a general comment to everyone who is speaking up. I know this is really tied up in contracts and that there is a lot of legal complexity associated with it, but with our 139 participants, I suspect that no more than 120 of them are lawyers. And so, for the other 19 of us, just be careful not to get too deep into the legalities, and we'll try to keep this discussion at the level of, maybe, instead of quoting a provision just say briefly what it is or something like that so that everyone is able to follow, as well.

But thanks, everyone. I'm really appreciating the discussion a great deal, and everyone's willingness to dig in. I just wanted to speak out on behalf of those of us that cap our syllables at two. I appreciate the simplification. Next slide. Oh, that was the rest of that one. Sorry. Next slide after that.

This one is about public interest commitments or PICs. This is one of the interesting things that came up in the context of James' introduction but it has also come up quite a bit in these kinds of conversations. And so, I wanted to get a hypothetical in place for this, as well.

So, the idea here is that an applicant applies for and is awarded a contract for .creditunion, which is considered to be a highly regulated space. The PICs that are in that contract, I was trying to find a way to use the least number of words. This is one of the most interesting challenges associated with this, that in each case the only requirement is that the next person down the contract chain have a policy about X. And then, all they need to then do to respond to a complaint is say that they have a policy.

And so, what the complainants have difficulty with, the victims of DNS abuse, is how to actually get to whether that policy is effective or whether it's actually being followed. In this case, the PICs that are in place are that registrars will ensure, via their contract with registrants: that these things are true and that these are PIC specs from the registry, that the registrants are all licensed or authorized credit unions, they'll comply with applicable laws, including privacy, consumer protection, fair lending, etc., that they have appropriate data security for private and sensitive information, and that these are registrants who will report changes to those authorizations or licenses if they occur.

So then, you have a situation where ICANN compliance gets complaints from both victims and some government agency within a country in which this is taking place, that there are a number of these .creditunion registrants that are actually engaged in criminal behavior, both in doing identity theft and also in publishing private information that they shouldn't, etc.

Someone has informed a government agency that it is one registrar in particular that just isn't doing this screening and is allowing anyone to register these domains, regardless of whether they have the proper authorizations or the proper bylaws in place to adhere with local laws.

So then, the question becomes, what should happen? What should a government agency or a victim of fraud do in this context to get a domain taken away from one of these fraudulent credit unions? Jamie, I'll let you go first.

JAMIE HEDLUND: Sure. Thanks for this interesting hypothetical. Just to give a little bit of background, there are a number of these types of new gTLDs that, unlike .creditunion, have actually submitted an application as a community applicant. As a community applicant, they have a specification 12, which really includes the criteria for eligibility for a registrant.

.Creditunion, in my understanding, is not a community gTLD, but instead still, as you point out, is a TLD in a highly regulated space. And so, the GAC safeguards apply to it. What you've listed here are the specification 11 3(a) requirements, and you are correct in the logic of how those apply.

The obligation in those—and there's a similar construct for non-sensitive gTLDs with respect to the legal behavior of registrants—is for the registry to include in its agreement with the registrar prohibitions that would be included in the registrar's agreement with registrants against prohibitions against engaging in illegal activity.

If a complaint is brought about that—we kind of explained this in a recent letter sent to the business constituency—compliance will look to see whether or not the registry has, in fact, required in its agreement with the registrar to include those prohibitions.

We do not have a way through spec 11 3(a) of reaching the registrar or the registrants but in this instance, I think, there is not the risk of harm that I think you describe because there is also a further provision in specification 11, in the section four of this particular gTLD agreement, which spells out the eligibility requirements for registrants, and that is enforceable directly by contractual compliance against the registry.

So, if there are registrants who are not credit unions or don't meet the criteria for registration in that instance, presumedly if they're engaging in these kinds of frauds they would not be licensed credit unions or associated with them so we would be able to go directly against the registry. I hope that makes sense.

JONATHAN ZUCK: It does, Jamie. I guess the issue is that the government agency complains to the registry, the registry says, "It's not our problem. Our agreement requires registrars to have this requirement in their agreement with registrants and our agreement does so." The agency complains to a registrar, the registrar says, "That provision is in our agreement with registrants," and the government agency complains to ICANN that neither the registry or the registrar is meaningfully implementing the PIC.

So, you just have this situation where everyone has checked off that they’ve got this policy but it doesn't seem to be anybody’s responsibility to ultimately enforce it.

JAMIE HEDLUND: Again, as a practical matter, it would seem that any entity engaging in those kinds of activity is not going to fulfill the eligibility requirements in order to become a registrant. And so, to the extent that parties can enforce against the bad actor in their local jurisdiction for engaging in this conduct and going after the bad actors directly, then a fallback would be—and probably an effective one I would think—going after the registry for allowing parties that don’t fulfill its eligibility criteria.

JONATHAN ZUCK: Thanks. James, is there anything you wanted to add, there?

JAMES BLADEL: No, very little, Jonathan. I agree with Jamie. You mentioned like, at this point, nobody is responsible. As I understand the scenario, both parties are responsible and both parties should be the subject of complaints to compliance. Thanks.

JONATHAN ZUCK: Thanks. I’ve got a question from Dean Marks in the chat. Dean, are you able to make an audio remark here or do you want your question read? Are you able to speak up, Dean? Yes, I can hear you.

DEAN MARKS: My audio is pretty bad. Could you read it, Jonathan?

JONATHAN ZUCK: Yeah, we can hear you.

DEAN MARKS: Would you mind reading it? I've lost my screen, so if you wouldn't mind reading it.

JONATHAN ZUCK: "What if the action is not illegal but not in compliance with the PIC in question?" is the question. I think that's sort of what was answered by Jamie.

DEAN MARKS: No, actually it was a different question.

JONATHAN ZUCK: Oh, I'm sorry.

DEAN MARKS: So, my question had …

JONATHAN ZUCK: “How does compliance and GoDaddy interpret—”

DEAN MARKS: [cross talk] accreditation agreement.

JONATHAN ZUCK: Is it this one, here? Yeah? Sorry.

DEAN MARKS: Yeah.

JONATHAN ZUCK: “How does compliance and GoDaddy interpret and apply the following provision of the RAA? Well-founded reports of illegal activity submitted to these contracts must be reviewed within 24 hours by an individual who is empowered by the registrar to take necessary and appropriate action in response to the report. If a report of illegal activities, such as pervasive copyright infringement, is made and reported with evidence, what is considered the appropriate action in response to such a report?”

DEAN MARKS: That’s that, thank you.

JONATHAN ZUCK: Not at all, Dean. James and Jamie?

JAMIE HEDLUND: So, I can start, and then James, please chime in.

JONATHAN ZUCK: Thanks, Jamie.

JAMIE HEDLUND: First of all, the first half of this is about what the requirements are for reports from law enforcement. So, registrars have to have a separate [use] contact for law enforcement. They have to acknowledge those within 24 hours.

The second part of the question applies to all abuse reports, which is, "What if the report is about something that looks really bad? What's an appropriate action?" This was also the subject of the recent BC letter and was also something that compliance had blogged about previously.

Under the RAA, under section 3.18, registrars have an obligation to investigate and respond to all types of abuse. So, whether it's copyright infringement, trademark infringement, fraud, things that are well outside ICANN's remit, still, the registrar has an obligation to investigate and respond.

The agreement, however, does not create requirements for what the investigation is supposed to look like or what the response is supposed to look like. And so, it is left to the registrar to determine what type of response is appropriate. A lot of times, there will be reports of abuse where it is not clear to the registrar what the law is in the jurisdiction either or the reporter, the registrant, or where the abuse might have taken place.

Different countries/different jurisdictions have different rules on what is a copyright violation. And so, there is a lot of discretion left to the registrar to determine in its best ability what the appropriate response is.

To address this issue, particularly with pervasive copyright infringement, some registries have, as many of you on this call know, entered into trusted notifier programs with NAs in the content industry. Under those notification agreements, which happen outside of ICANN and outside of the registry and registrar agreements, a trusted notifier will identify the domain name associated with pervasive copyright infringing content and will provide that over to the registry with whom they have the trusted notifier agreement.

The registry, presumedly, trusts the provider of the information and the veracity of the information and then takes action against it. That seems to be an effective means for dealing with the pervasive copyright infringement and it leaves ICANN out of the business of regulating content, which our bylaws prohibit in any event. James, anything you'd like to add to that?

JAMES BLADEL: Thanks, Jamie. I think that your answer was fairly comprehensive. I think you mentioned these but I just want to echo the point about the distinction between the time clock that's ticking upon receipt of a request from a law enforcement channel versus other types of complaints that could include a copyright infringement, even if it's pervasive.

In the second case, copyright claims can sometimes result in the response which, as I mentioned earlier in the call, is that this is occurring outside of our network, "Can we direct you to the web host, for example, that can maybe help you address this?"

I say that because from an ICANN perspective that is a response. It's not, maybe, depending upon the nature of the complaint, a satisfactory response, but it is an investigation that resulted in a response. I think that's where we get a little tied up in what sort of outcomes ICANN is enforcing versus the enforcement of the existence of a process, and that that process is followed. Yeah. Otherwise, I think Jamie covered this fairly comprehensively. Thanks.

JONATHAN ZUCK: Thanks, James. I want to call on Laureen Kapin from the FTC. Thanks.

LAUREEN KAPIN: Thanks, Jonathan. I'm also speaking in my capacity as co-chair of the Public Safety Working Group. What I wanted to ask Jamie, in terms of what you mentioned about the registry enforcing the eligibility requirements, as I understand the commitment, all the registrant has to do is represent that they have the proper credentials, and that is the obligation under the public interest commitments in terms of the eligibility requirements.

So, my question to you is, do you see a gap in the tools that one might need to make sure that players in highly regulated domain namespaces like a .creditunion, that there would be a gap here? Because, once they represent that they have the right credentials, one could make the argument that the registry has complied with its obligation.

But you never get to an obligation to actually make sure that the representation is, in fact, accurate, which was a higher standard that was originally advised by the GAC and the subject of a lot of repeated GAC advice that, by diluting the request by the GAC of making sure that these representations were verified, you would, in fact, have a scenario where people like. That’s my question to you. Does this scenario point to a gap in the tools you would need to make sure that folks are what they purport to be in these very sensitive domain namespaces?

JAMIE HEDLUND: Thanks, Laureen. I'm looking at section four of specifications 11 for the .creditunion RAA.

LAUREEN KAPIN: I was looking at that, too.

JAMIE HEDLUND: "Registry operators shall only permit the registration of names to registrants that meet the registrant eligibility policy. The current registrant criteria limits registrations to those entities with a meaningful nexus," etc.

I don't see the scenario that you're pointing out where they say there is nothing they can do because they got a representation that they, in fact, met the criteria. If later it turns out that there is evidence that they don't then we would provide that evidence to them and ask them to explain how, with this evidence, they still meet the criteria.

LAUREEN KAPIN: Right. Well, that's actually good to hear. But of course, that point four, the public interest commitment, was a voluntary one. It wasn't required to be part of the contract. So, if I change my scenario and we're not dealing with the actual .creditunion contract but we're dealing with another highly sensitive domain that, regrettably, didn't take this extra step, wouldn't we be in hot water then?

JAMIE HEDLUND: I suppose it's possible. The "credit union" has this and "bank." That was the other one? .Pharmacy have their community applications. Up until now, we haven't had any complaints that I'm aware of, for example for .lawyer, or /accountant, or .cpa. I think .cpa is community, as well. I'm not sure. I can't remember but I believe so.

I think my memory of the issue for the ones where there were these additional voluntary commitments were made was a concern that there wasn't going to be enough preregistration vetting, which I think is a different issue than, under false pretenses, getting the registration and then engaging in bad behavior, in which case we would be able to go back to them and ask them to review whether or not this entity met the eligibility criteria.

JONATHAN ZUCK: Thanks, folks. We're running out of time. We're checking to see if we can get a few more minutes with the interpreters. This virtual meeting is a lot stricter on timeframes than some of our calls are so we may get cut off fairly quickly. I apologize. I'm really appreciating the conversation.

One of the scenarios that we wanted to try and address was just the notion that there is a registrar that has been engaged in continually having a very high percentage of the registrations being used for abusive purposes, and that goes on for a very long period of time. So, Alpnames is one of those. I was going to pass the microphone to Fabricio to very quickly make that tie-in and see if we've got an opportunity to discuss it a little bit. Fabricio, go ahead.

FABRICIO VAYRA: Thank you, Jonathan. Can you hear me?

JONATHAN ZUCK: Yes, sir.

FABRICIO VAYRA: All right, thank you. Yeah. I was looking at the screen, here, and I saw this: "Many registrants were engaged in criminal behavior. One registrar is doing no screening at all." Listening to the conversation, Dean asked—in the context of PICs but I think it's relevant to the Alpnames and that scenario—"What if it violates the PICs or the RAA generally, the behavior, and what does ICANN do?"

My understanding, paraphrasing from Jamie, is that we obviously reach out to the registrar to find out, "Are they in compliance? What are they doing in response?" etc. My recollection of our discussions, Jamie, on this, under the guise of the ICWP, the Independent Compliance Working Party discussions we had, was that in the context of Alpnames ICANN was doing that right. ICANN was reaching out to the registrar, and then the registrar said, "We checked it out and we canceled that one domain name."

But big picture, here, and high level, Alpnames basically ran aground and left ICANN holding the bag. That, I think, brings up a really big problem, here, which is that level of deference, of, "Let's check with the registrar per ticket," basically going on a ticket system, and they get to, per ticket, tell you everything's okay, and then you're left, basically, telling us you can't do anything per the contract, your hands are tied, doesn't this raise a bigger level?

When you're in persistent, consistent, and documented violation of the RAA, where is ICANN compliance's hook to deal with that registrar? I think, hopefully, my colleagues on this call, James, and Graeme, and others who we've talked this through with, will agree that this is a problem and we've all thought that there's something in the contract that you can do but it seems like not.

I guess I'd love for you to just answer that broader question, Jamie. What can you do that hasn't been done, or what's the plan to fix that gaping hole so that we don't have another Alpnames, or that we address those that are like Alpnames right now that are continuing to move from ticket to ticket and never actually get compliance?

JONATHAN ZUCK: Thanks. I know Jamie has got another session right after this one. I don't know, Jamie, if you are able to address that briefly?

JAMIE HEDLUND: Sure, yeah. First of all, I don't agree with some of the characterizations, Fab, you made about ICANN or compliance being left with a bag. Be that as it may, as I tried to say in the beginning of the conversation, our approach in compliance has been to enforce the provisions as they are in the agreement. We do that in response to complaints, we do that through audits, and we also initiate discussions based on things that are out there in the media, blogs, or industry information.

So, I think the question was raised in the CCT and elsewhere about whether and what ICANN compliance can do against allegations of systemic abuse. There are lots of questions implicit in that, including, “What is systemic abuse? What is DNS abuse? Should ICANN compliance be enforcing beyond what’s listed in spec 11 3(b) of the registry agreement?” and how to establish what is systemic.

I will say we do have the ability to escalate in our compliance efforts against recidivists or repeat offenders. We’ve done that in the past, where parties come in, and are then found to be not in compliance, and remediates. They come back again. Rather than having to go through our normal first, second, third notice, we go immediately to an escalated notice, in which case they have five days to respond or we go to a public [inaudible] breach.

So, we have those tools. And then, James and others in the community have suggested that there may be other ways that we can go after the truly bad actors, however defined. I'm eager to hear those. We are all eager to look at other creative ways there may be to go after the few truly bad registries or registrars. I hope that helps. Thanks.

JONATHAN ZUCK: Thanks, everyone.

JAMES BLADEL: Jonathan?

JONATHAN ZUCK: Yeah?

JAMES BLADEL: I know we're over time, I just wanted to respond really quickly.

JONATHAN ZUCK: Yeah, I think we're just about to lose our interpreters, that's all, so I've got to …

JAMES BLADEL: Yeah. I just want to not I think that Jamie makes a good point. I actually do think that ICANN should be more aggressive in these types of scenarios because we make investments. If it's not clear by some of my answers, we do take our responsibilities seriously and make investments in terms of people and tools to crack down on abuse.

And so, it cheapens those investments if other registrars are allowed to skate on by. And so, I do want to see a more aggressive approach from ICANN in these types of cases of ongoing and continuous abuse, as opposed to just sending more tickets to our folks because GoDaddy answers them promptly and addresses them.

I think last time I pointed out that there is a provision in the contract, the RAA, that I think is a huge trapdoor that says to ICANN, "You don't have to be in this contract with a party if you believe that party is involved in illegal activities." Maybe it's time to look in those truly, truly egregious cases where ICANN has tried consulting and trying to coach these folks up, making sure they completely understand their obligations.

Sometimes, it may just be a function of the RAA is not available in a local language, maybe, but if all of that fails and you're just going round, and round, and round with a bad actor it's time to pull the plug.

JONATHAN ZUCK: Thanks, James. I appreciate that perspective. I'm really being told I've got to pull the plug, Mason, I'm really sorry. It's just the beginning of this conversation and we're going to try to keep this going. As you've seen from our last two sessions, the At-Large is planning to really take this issue on to advance. I appreciate everybody's participation on this call and I realize that everybody that has been speaking has the best intentions. And so, we're trying to keep going. I just got note that we could have nine more minutes. Mason, I can actually let you speak up if you're still there.

MASON COLE: I am here. Can you hear me, Jonathan?

JONATHAN ZUCK: Yes, I can.

MASON COLE: All right, thanks. Good. It's good to know we've got a little extra time and I appreciate you working me in. Look, I think the discussion on these examples are really useful because they bring things down to the real-world level. I was encouraged by James' most recent intervention on Alpnames. I'm not sure that we totally answered the question about what you do from a community point of view or from a compliance point of view on Alpnames-level abuse, but hopefully we'll get an answer to that question soon. I wanted to bring the whole discussion back around to the "Wholistic" nature that I think we talked about before we started.

I just want to say a couple of things. I applaud the framework that the contracted parties have put together. I know I said that in Montréal during the session on DNS abuse, and I think it's a fantastic move and I'm glad to hear that so many others have signed onto it.

The problem, of course, with that is that it doesn't encompass the 20-or-so registrars and registries or the other contracted parties that we know are responsible for most of the abuse. Abuse rates, I'm afraid I have to point out, are still going up. The framework is great; it clearly isn't going to solve the entire problem. It seems clear at this point—and I don't say this lightly, coming from the many years I spent on the contracted parties side of the house—that we need new tools.

We were asked on the BC how to interpret contracts for greater efficacy but we just received a reply from the board that shot that down. There is some fatigue in hearing that the contracts are insufficient, I know, but our ask is that we do something to come together as a community to strengthen those agreements in a way that gives compliance actual teeth and real tools either to stop the increase of abuse or bring that rate down.

So, I just wanted to say that we're going to continue to be vocal on this. I hope that we have further discussions on this in the spirit that you've outlined here, Jonathan, because it has been very productive. I hope that everybody will come together and we can have a constructive and productive dialog on how to do that without retreating to our usual corners. Thank you.

JONATHAN ZUCK: Thanks, Mason. That is, in fact, our intention. We have many more conversations ahead of us on this issue and I would, again, want to thank everyone who participated and we will keep these conversations going. The At-Large is happy to take a lead in getting some of these conversations going across the community.

I really appreciate so many participants signing on for this meeting. I hope you found it useful and informative. I think that it did raise some issues that the status quo is insufficient and we're going to have to figure the best way to address it. Thanks, everyone, so much.

Thanks very much to the interpreters for going over by a few minutes. We really appreciate it. I know we get excited about this stuff and always go over time, and so we really appreciate your effort. Thanks.

Everyone join me in thanking the interpreters. Thanks, everyone, for participating. Thanks a lot.

CLAUDIA RUIZ: Thank you all for joining. This meeting is adjourned.

[END OF TRANSCRIPTION]