ICANN68 | Virtual Policy Forum – At-Large Policy Session: DNS Abuse: Setting an Acceptable Threshold
Wednesday, June 24, 2020 – 10:00 to 11:30 MYT

[JONATHAN ZUCK:] I'd say go ahead.

MICHELLE DESMYTER: All right. Thank you so much. Okay. Well, good morning, good afternoon, and good evening to all. Welcome to day three of our At-Large session of the ICANN68 Virtual Policy Forum on Wednesday the 24th of June at 02:00 UTC: "DNS Abuse: Setting an Acceptable Threshold."

My name is Michelle DeSmyter from At-Large staff, and I am the remote participation manager for this session. Please note that this session is being recorded and follows the ICANN expected standards of behavior.

We will not be doing a rollcall during ICANN68 but will note attendance for all sessions. During the session, questions or comments submitted in chat will only be read aloud if submitted in English using the proper form, as I've noted in the chat.

I will read questions and comments aloud during the time set by the chair or moderator of this session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, we will kindly unmute your microphone and you may take the floor. Please state your name for the record and the language you will speak, if speaking a language other than English.

Please note this session includes interpretation in French and Spanish. To hear the interpretation, you will need to download the interpretation application. More information can be found in the session details on the event schedule and instructions will be posted in the chat.

We have also posted all the details on the At-Large ICANN68 Wiki page. The link is posted in the chat, as well. A friendly reminder to please speak clearly and at a reasonable speed to allow for accurate interpretation and, again, to state your name each time you do take the floor. With this, I will hand the floor over to Jonathan Zuck. Please begin.

JONATHAN ZUCK: Thanks, Michelle. This is Jonathan Zuck, vice-chair of the At-Large Advisory Committee, specializing in policy, and so also co-chair of the Consolidated Policy Working Group inside the At-Large.

The At-Large are the principal advocates of individual end-users in the Internet ecosystem. And as such, DNS abuse is something that is a dominating issue for the At-Large. And so, it's something that we've held a number of different sessions on in the last few meetings, and this one is no different.

But here, what we're going to try to do in this session is really drill into one particular concept, rather than having a more overall type of conversation. So, we'll see how that goes. So, if you would, can you bring up my slides? Okay. They're not really filling the screen. I don't know if there's a way to make them bigger. Not to make your life difficult or anything like that. Well, I'll continue on.

So, I'm always thinking about how not to have bullets in my slides. I guess that's the first thing. I was thinking about a kind of visual metaphor for the discussions that we've been having about trying to combat DNS abuse.

The way I see it, here, is that this guy in the background is like a sheriff. And so, that's the governments, trademark owners, consumer protection agencies, etc., that are about to have a duel with … Sounds like somebody has got to be muted. About to have a duel with some bad actors in the DNS ecosystem. And one would hope they'd be quicker to the draw. Next slide.

There is this other problem where community members are sort of walking in and out in between us and it's very difficult to fire at the bad guy without just hitting the townspeople. I think that's part of the challenge that we face; it's tough to just shoot the guy across the square when there are people coming in and out of the square all the time. Next slide.

It's the end-users that are ultimately suffering in this battle between the parties inside the ICANN ecosystem. Next slide. And we know that there are still some bad actors out there. While we are only hearing from the good ones, there is a lot of news just recently about GalComm and what was happening with a registration of over 60% of malicious domains with that registrar. Next slide.

So, there's a famous line from Star Trek, where we need to draw the line: "The line must be drawn here, and no further." Let's see if this works. All right, there you go. Next slide.

But the question, of course, is, and the question for this panel is, where to draw that line. So, next slide. What we heard from both Graeme and Keith Drazek, in the first DNS session, is that we need to determine the characteristics of the bad actors, and then we can deal with them. Next slide.

So, what do those characteristics look like that we'd want to use? What sort of metrics do we want to try to use to figure out whether or not we're dealing with a bad actor or just somebody that we need to work with more? Is it a percentage of abusive registrations, as a percentage of the total registrations?

Because we don't want to punish people for being successful, but get a sense of how their operation scales. Is it complaint percentage? Is it the average resolution time? Do they wear a black hat? We don't really know. But we want to figure out those characteristics. Next slide. Owen, I see your question about defining abuse, and we're going to define it very narrowly for this discussion. Drew is going to do that, and he's going to be the next one to present.

So, that was my introduction. I'm sorry, Michele, about any thoughts that [there was liable]. We'll have to have a conversation about that. We're honored to have on our panel David Conrad, who is senior vice-president and chief technology officer of ICANN, and Drew Bagley, who does a lot of things for SecureDomains and for CrowdStrike. So, without further ado, I'd like to pass the microphone over to Drew Bagley.

DREW BAGLEY: Thank you, Jonathan. Are you guys able to load the presentation I sent? Perfect. There it is. Thank you. Yeah. So, today I'd like to start off the conversation by discussing some of the characteristics from work that the community has already done that relate to us defining metrics for DNS abuse specific to the systemic abuse that Jonathan was referring to, with regard to some of these operators like the one he showed and, in general, the ones that don't show up at ICANN meetings. Next slide, please.

And so, I was a member, like Jonathan and like representatives across the entire community, of the CCT Review Team. When we were doing the CCT Review Team analysis and looking at the safeguards that were implemented as part of the new gTLD program, as well as all the issues that were identified prior to the implementation of the new gTLD program, one of the key issues that we focused on measuring was DNS abuse.

And so, as part of that process, ICANN commissioned the Statistical Analysis of DNS Abuse in GTLDs, which is sometimes referred to as

SADAG. This study looked at both new gTLDs, as well as legacy gTLDs, and did a breakdown by registries and registrars with regard to abuse levels.

In general—and you can look at the report itself as well as the CCT Review Team's report for more information on the methodology—the researchers looked at a three-year time horizon, and then used multiple blocklists—next slide, please—to conduct the analysis.

And in doing so, they relied upon the DNS abuse definition you see here, which is the same DNS abuse definition that the CCT Review Team used, which we called DNS Security Abuse, and which relied upon common, consensus-based areas, based upon the literature that we cited in our report, on where there are areas where DNS abuse is highly technical and related to cybersecurity, even though we all know that DNS abuse can, potentially, go beyond this, depending on which party you're talking to. But in general, this is what we focus on, and this is what the research itself focused on.

As it related to these parties that Jonathan was alluding to, where there are these high levels of abuse and where abuse is concentrated, the CCT Review Team, as well as this particular study, found that there really are these particular either zones, certain TLDs, or specific registrars where the levels of abuse can be more than 50% of their total registrations.

And so, these high levels of DNS abuse are seemingly not random, nor are they universal so that every zone faces these same levels.

Nonetheless, there are these very particular, identifiable places where this is very problematic.

And so, with this, the other interesting thing is that these high levels of abuse could go unabated and sustained over several quarters, and sometimes over several years, without there being any sort of action being done.

And so, in other words, a registrar that might be deriving its profits from having a portfolio with more than 50% abusive registrations would still be in business with that and there would not be an action taken from ICANN Compliance to mitigate that abuse or suspend them if they weren't mitigating that abuse. And similarly, there would be no action from this registrar to do something about these registrants. Next slide, please.

And so, in addition to several other recommendations related to abuse, one of the CCT Review Team's recommendations, recommendation number 15, focused on this systemic, unabated abuse. And so, while other recommendations that have already been discussed previous … ICANN's focused on certain incentives.

This recommendation, really, was focused on ensuring that these operators, with these extremely high levels of abuse, and where you would have people being victimized and data breaches happening, could not just be sustained without anyone having any ability to do anything about it.

And so, here, the recommendation, which all of our recommendations in this report were very long, so that's why I didn't put the whole thing on the slide, but the gist of it was that ICANN Org should ensure that it has this power for ICANN Compliance to do something about high levels of DNS security abuse when then they cross certain thresholds.

And while the CCT Review Team was not prescriptive in mandating what thresholds should be, the CCT Review Team did suggest thresholds. And so, in this, the thresholds that were suggested were that, if there was a trigger of 3% of registrations being associated with high levels of abuse, then that's where you would, at least, instigate some sort of investigation by Compliance. Whereas if the threshold reached 10%, then that's one where a party would be presumed to be in breach of its agreement. And so, this was based off of the data that we saw in the study. Next slide, please. Next slide, please.

[MICHELLE DESMYTER:] One moment.

DREW BAGLEY: Okay. No problem. And so, these thresholds were based off of what we were seeing with these extremely high levels. So, here are some examples. So, there were two registrars managing an AlpNames that were particularly egregious in looking at this data, and that operated for years with these extremely high levels of abuse.

And so, for Nanjing, they had it so that 93% of the new gTLD registrations associated with them for a period of time were actually appearing on blacklists. Eventually, Nanjing was suspended, but it wasn't suspended just based off of this level of abuse.

Instead, it was a series of things. And ultimately, one of the most damning things was that they had a failure to pay ICANN fees. And so, Nanjing, looking back at the data, had operated this way for years.

Similarly, AlpNames operated until 2019, when it was eventually suspended. But it was operating with extremely high levels of abuse, and some of that abuse was associated with specific TLDs such as .science and .top.

And so, these are two clear examples of where you have these parties that don't show up at ICANN meetings. They aren't the ones trying to play by the rules in general. And yet, they were getting away with being a source where cybercriminals could go register domain names and use them for all sorts of purposes related to that definition we discussed at the beginning of this session. And yet, that alone was not enough for anyone to do anything about it. Next slide, please.

And so, here are some of the charts that you can see in the SADAG study itself that highlight this. But you can see Nanjing, here, at the top, with a 93.36% rate, but there are several others with these high levels of abuse.

Similarly, when you get to these registrars that are dealing with particular zones that have high levels of abuse, too, then that's where you can really see that overlap that, if you're going either to register a domain name for malicious purposes or to compromise a legitimately registered domain name, there is a very high correlation between certain zones and certain registrars with the success that these cybercriminals were having and being able to sustain those high levels of domain name registrations without anything happening. Next slide, please.

So, here is an example of the zones for which registries had domain names with … That have more than 10% of their domain names associated with high levels of abuse. And so, here, .science, half of the .science registrations were abusive at this point in time. And .stream, similarly, almost half.

And so, that's where this concept of a threshold came about on the CCT Review Team where, when you're looking at this and you're thinking about the contracted parties—who are doing a lot about abuse and making sure that their domain name registrations are overwhelmingly legitimately registered to begin with and that, to the extent domain names are being compromised, they're doing something about it—they're not showing up on this list.

However, when you have parties, whether they're registries or registrars, where it seems that they're either doing nothing about it or turning a blind eye and profiting from it, you end up with these extremely high levels of abuse that are above 10%. Next slide, please.

And so, here is more data from the study that highlights some of these that I just went over. You can see here that, with some of these like .download, you have really high levels of abuse where you have 20% of all registrations being associated with some sort of abuse. And so, that's the issue, here, that thresholds really can address. Next slide, please.

So, what this data tells us, and what the work of the CCT Review Team in this area really tells us, is that there really are some parties that are either used by cybercriminals or specifically targeting; for example, if you have legitimately registered domain names being compromised by cybercriminals.

And yet, if there are no incentives or disincentives for these parties to do anything about the abuse, then this abuse can really sustain itself over very long periods of time, while people can continue to be victimized from the same sources, whether you're talking about particular TLDs or particular registrars.

And this whole, entire concept is completely incompatible with ICANN's remit with regard to protecting the security and stability of the DNS. And so, that's why, on the CCT Review Team, what we looked at was a way in which you could, at least, get ICANN Compliance engaged with looking into and investigating something if there was a threshold going high.

And so, sometimes, if you had some sort of active campaign focused on a registrar and the registrar itself was a victim, that's something where that can come out when ICANN Compliance is investigating this.

But if you have something where levels get to the point that you have 10% and they're sustained levels of abuse, similarly, if the registrar is the victim, then that can come out in the investigation.

But that's where, if you're operating at that high of a level, it should be assumed that you should be doing something about that to mitigate that. And if a party is not doing something about that, then that's where it's really problematic for that party to remain accredited. And instead, that's where suspension would be necessary if there is no mitigation of the abuse.

And that's where coming up with thresholds as a community is really an important tool that we can use to, at least, address these particular registrars that are being used and exploited by cybercriminals for these purposes in a way that is incompatible with the security and stability of the DNS, but also is something where it's really a poor reflection of the Domain Name System when it's this concentrated level of abuse, when you have other parties being responsible and doing something about it.

And so, to get these bad actors to either be incentivized to actually comply and mitigate abuse, or to get them to no longer be parties, it's really important to consider this threshold recommendation.

And so, the CCT Review Team has several other recommendations related to abuse, but I just wanted to focus on that for purposes of this discussion, as we're discussing, as a community, how to move forward. But it's important to remember that there really is a lot of data supporting this notion that some registries and registrars really are associated with levels of abuse that we don't even hear of from the parties that show up here at ICANN meetings.

And so, when we had this cross-community group of the CCT Review Team look into this, this was something that was very troubling to us and that, I think, we can really do something about. And with that, I'll pass the baton.

JONATHAN ZUCK: Thanks, Drew. We obviously have a heated discussion, again. I was hoping it would be less heated, but a heated discussion again, in the chat. David, I guess it would go to you next, and then I'd let Graeme go last. Go ahead, David.

DAVID CONRAD: Okay. Thank you. I was asked to talk about the information that we have available within ICANN Org, specifically within OCTO, related to DNS abuse. And we have, right now, two primary projects. One is the DNS Abuse Activity Reporting project, DAAR, which I'm sure everyone here has probably heard of one way or another. And we have another project called the Identifier Technologies Health Indicators.

The sources of data for our internal research use zone files from CZDS and reputation data from a set of DNS reputation providers. We documented the methodology by which we chose those providers, and they are that list that's provided there.

DAAR reports, currently, are a point in time. I believe they are the last day of the month. We, basically, take a snapshot and generate a report off of that. And ITHI are a time series that are based on monthly averages. Next slide, please.

So, in the DAAR report that you can find on the ICANN website at the URL that I've provided, there, you can see a series of graphs, a number of charts of various forms. And one of the points that is probably worth making, here, is that over time—and the DAAR reports have, basically, a six-month rolling window of the abuse that we track within these reports—it appears that the abuse has been, generally, going down.

Of course, you get spikes every now and then, whenever a campaign is run of one form or another. But if you sort of eyeball the data that's presented, here, you see that over time the numbers tend to be decreasing.

One other observation that I would make is that the magnitude of the abuse, here, is sometimes surprising to people. If you look at the figure 12, there, the average percent of abuse per gTLD type is around 0.5-0.6% of all the registrations. Similarly, if you look at everything but spam, everything is under 1% of the registrations.

So the numbers, here, in the grand scheme of things, are relatively small compared to the total number of registrations, and these are only registrations that show up within the zone files.

This isn't registrations that are made or that are held that do not get populated in the zone files, because DAAR generates its data based off information that's published in the zone files that are obtained via CZDS, the Centralized Zone Data System. Next slide, please.

We also provide a number of dot charts/scatter plots. These show everything from the raw counts of domains that are resolved in gTLDs versus the raw count of security threats. And you can see, in each of these, that there are occasions where you will see some outliers.

For example, in the malware chart over there on the upper right, you can see one blue dot, which represents a new gTLD, which sticks out from everybody else. I actually asked my team, Samaneh, the researchers primarily responsible for this, to dig up some information.

She gave me a snapshot of the DAAR statistics, and it turns out that that is a single … Well, actually, it's two registries that have had a relatively high amount of malware, in the sense that they had a total number of registrations of, I believe, seven, and one of those registrations was actually used for distribution of malware. So, the percentage of abuse showed up quite high.

Similarly, in domains, the Botnet C&C, you do see little spikes here and there – little indications that there are outliers that may be of interest to explore. And that's one of the things that my team is beginning to look at. We are identifying these outliers, and then we actually go and talk to them, try to understand why they are outliers.

We've had some reasonable success in this where we've interacted with the registries. Because right now, DAAR only deals with registry data and, specifically, gTLDs. We do have six ccTLDs, but the CCs are not included in these statistics. As yet, we're trying to figure out how best to incorporate their information into the DAAR reports.

But we go and we speak with these registries, and we've had reasonable success. The data that Drew was showing was from three years ago, if I understand correctly. The SADAG study, I believe, was published three years ago.

And today, looking at statistics that Samaneh generate for me earlier this morning. There are no TLDs that are showing DAAR statistics of over 20% abusive. There are five, I believe, that are above 10% abusive, and that's including all of the categories of abuse that DAAR looks at, which is botnet, command and control, malware distribution, phishing, and spam.

If you drop spam, because spam is sort of an annoying outlier in and of itself, you get into much, much smaller numbers. The highest right now is only about 1.4% of abuse that doesn't include spam, and it drops down pretty quickly beyond that. Next slide, please.

The other source of information that we use within OCTO is the ITHI DNS abuse statistics, which is category M2. If you go to that website, you will see a beautiful example of 1990's web design. But within that, you will have quite a bit of data associated with DNS abuse.

The statistics, there, are aggregated over a month, and the "high and low" are the historic highs and lows from since the point where ITHI were initiated.

So, again, one important item to note is that the absolute magnitude numbers, here, are actually quite low; less than a tenth of one percent, in most cases. And the total numbers of TLDs that account for 90% of the abuse are actually quite small, but that shouldn't be surprising because of the market concentration.

There is one registry that accounts for more than 50% of abuse, but I don't think anyone here would suggest that that one registry is actually doing anything wrong, or bad, or they're a bad actor in any way. The issue is that the amount of domains that are published has a highly correlative effect to the amount of abuse.

There are outliers, as I mentioned before, but they are the … Oh, the graph went away. Can I have the slide back, please? But in general, one of the things that we're trying to figure out within OCTO is trying to identify the thresholds that have been discussed, what thresholds actually make sense, and how they can actually be applied. Could I have the next slide? Or any slides. Oh, there we go. No. Getting there. One more slide, I believe.

[MICHELLE DESMYTER:] Actually, that is the last one.

DAVID CONRAD: Oh, interesting. Okay. Well, if you go to the ITHI website you will see a set of time series, and that goes back to when ITHI was first started. And again, the general trend that you will see is that the abuse is decreasing over time.

I, personally, don't have data for this, but I personally think it's because of the increased attention that various parties have been applying to DNS abuse. But it is, as far as we can tell, sort of a long-term trend that the DNS abuse is decreasing over time. And with that, I will hand it over back to Jonathan.

JONATHAN ZUCK: Thanks a lot, David. I guess I want to go ahead and let Graeme go ahead and talk. There are, obviously, a lot of things to talk about, given the chat, and the presentations, and [we've lost our recording]. Graeme, go ahead.

GRAEME BUNTON: Thanks, Jonathan. Thank you to the ALAC, and thank you, Jonathan, for having me join the panel. It's looking like it's going to be quite contentious. So, I'm now reasonably trepidacious.

Let me start with, maybe, thanks for the quote you shared relatively early in this presentation. I think that still holds true, and I'll come back to this at the tail-end of what I'm going to talk about, here. I don't have any slides. I'm just going to talk to a few issues for a moment.

So, this topic is at the nexus of some things that I think about quite a bit, which is data, data-driven policy development, and DNS abuse. Oh, we get to read other slides while we're doing this.

Maybe for a little bit, for the context of myself, I, up until very recently, ran the data practice at Tucows; very hands-on in collecting and processing data. So, this is not a casual perspective for me. This is something I've really been involved in in the past.

So, I'm going to start, maybe, with a little bit of a couple of thoughts on what data looks like from inside a registrar, and maybe that's worth sharing. There is, maybe, also, a piece that's worth sharing, here, and it is unfortunate the move to virtual meetings has pushed this plenary session off.

But contracted parties have been trying to get a session in front of the ICANN community about the actual business realities of running a registry and a registrar, and what that looks like, and what the economics of that looks like.

Because I think it would inform a lot of this discussion, and I would really encourage those who really don't understand the economics of how the industry works to do a little research and thinking on that. I won't go into it here, but suffice to say, this is a domain registration.

From a registrar perspective, it's a business of scale. It requires a high volume and it has low margins, and that impacts the data we collect and how we respond to issues. That's not to bemoan our position. I think it's just a business fact that we need to recognize.

So, where I think that impacts registrars, especially, is that we optimize our abuse queues for throughput, and being able to definitively close and issue, and not to collect statistics on what's happening.

Reg, the director of compliance and Tucows, and I discuss this all the time. We love data at Tucows. This is, as I said, really important to me. We would love to begin customizing our Zendesk, which is the platform we use for managing our abuse queue, to be able to collect more data about what types of issues we're seeing, how we close them, what the outcome of that is, because I think it would really inform discussions like this in important ways.

But that work, for us, always falls behind more important work. Most recently, responding to COVID abuse. And if you go back to some of the things that Tucows has produced, we have some really excellent blog posts on the statistics related to requests for access to registrant data that I would encourage everyone to go read. All of that was built by Reg, essentially, by hand, and collecting that data.

And so, it's really hard for us to inform some of these decisions from an inside perspective, where that data really isn't just being collected at an enterprise level. And I suspect that's true for just about every registrar, and the same is true for our work on COVID.

I was talking about that in the Contracted Parties House webinar that we held, I think, on the 11th. The statistics that I presented there were, again, essentially collected by hand: putting stuff into spreadsheets and manually reviewing.

All of this is to say that, as we're collecting and thinking about the data, we need to be exceptionally careful about how we're doing so because the end results, and the impacts on registrars and contracted parties, greatly depends on the quality of that data.

I don't want to talk for too long, so maybe let's go right to the idea of thresholds for a bit. So, first of all, for definition purposes, I know we don't want to belabor this conversation because we've had it about a bajillion times.

I will reiterate, here, that the Contracted Parties House has, as formally as possible, agreed upon a definition of DNS abuse. It is very similar to the CCT one, except for aside from "high-volume spam" it says "spam where it's in service of malware, botnets, and phishing," in short.

I would encourage everybody to … I'm sure we can find a link for that. It is taken from the DNS abuse framework. Thank you, Sarah. Please go take a look. That's where we would like to work from. That is where, the companies that are taking down domains for DNS abuse all day every day, we are working from currently.

And to an extent, that is a floor, not a ceiling. Every single contracted party is free to take that as their definition, that is their floor, and then go above and beyond as they see fit, and address issues as they see fit. So, let's start there.

Part of the issue, and some of the concern I'm seeing in the chat, and I know the contracted parties have with the idea of thresholds … And going back to this issue of data quality, what was really highlighted for me was the quality of lists that we were seeing reporting abusive registrations.

Those lists were, by and large, terrible. They would have had me take down the official South Africa COVID response website, websites for hospitals. There was a lot of very poor information, and we need to be very careful as we're treating these feeds.

Others who are closer to DNS abuse in a technical sense than me, I think, will tell you that a lot of the feeds that people use are reported abuse, not necessarily verified or investigated [reviews]. And hanging a lot of these very important decisions on those facts is, I think, really difficult.

There is sort of, also, I think, real concerns about what thresholds might do. One, and I think I saw, maybe, Rubens referring to it, is that they could, in a sense, be weaponized against contracted parties, which is maybe an odd concern, but not beyond the realm of possibility.

And then, the other is that … And this is, I think, called Goodhart's Law. It's where, by setting a threshold, you actually set what becomes a target, and you don't necessarily incentivize, but what you've signed is, "You can be this bad until you get into trouble," and it allows people to figure out exactly what that means. Maybe there is a better way to come at this problem than incentivizing that.

Thresholds in general. How would we enforce these things? Registrars, I think, across the board—and I'm just about no longer chair, but I think I can say with some reasonable confidence—would much, much, much prefer being creative with our existing contracts and working with ICANN Compliance to go after these bad actors in a meaningful way.

The small number of bad actors that I think have been … And maybe how they're identified is an important thing we should talk about. But my sense is that OCTO is doing some really great work, and I loved that presentation from David.

Seeing that DNS abuse is going down is wonderfully heartening. But figuring out how OCTO and Compliance can begin to work together to find creative ways to use the existing contractual language that we've got to go after bad actors.

There are a couple of things in there that may be contentious. I would be really curious to hear from ICANN Compliance. I don't think they're here, but it is … What is it? Oh, I don't have the reference in front of me. I think it's like 5.5.71, or something, where you can de-accredit a registrar for material impact to the security and stability of the DNS, something like that.

Are there circumstances where that would apply? I would be really curious to hear from Compliance what that would actually look like for them. Have they tried a hypothetical example?

And so, maybe just to bring this in for a close, we need to be really careful about the quality of the data that we're using. It can be so impactful on this industry, and the data, as we've seen, can be sensationalist and, also, wildly inaccurate.

I'm going to pick on you, a little bit, Jonathan, here. You put up a slide earlier this week that said, COVID-related domains were 50% more likely to be abusive. Well, 50% more likely than what?

And if you actually go back to that report, it was for a week's worth of domains that was actually captured, I think, in late February, well ahead of where we saw the bulk of COVID registrations, and it was comparing it to domains that that particular company happened to look at in that week.

And if you were to take that, "Oh, if they're 50% worse than domains in general," and look at David's presentation about what the rates of abuse were where it's going from, that would mean something abusive might have gone from the likelihood from … What was it, like 0.1%, 0.01%, to 0.015%, or 0.15%? For a small registrar, that might not actually add up to a single domain name. And so, we need to be exceptionally careful in how we approach this problem.

So, going back to the quote that Jonathan Zuck shared from me—I guess it was from 2008—I'll reiterate that, which is … I think we've got a definition, now, at least, from the CPH, that I would like us to use, and I think it's important that we do.

Now, let's work with OCTO, who are doing really interesting work right now, to use that definition to really define or to understand what the bad actors are doing and how they're doing it.

Let's identify their attributes and characteristics. Once we understand what they're doing … Because I don't understand. I don't spend my days figuring out how to get around ICANN Compliance or how to … I don't know there is any really good way to build a business on abusive registrations, but that's not a thing I try and do on a regular basis.

So, when we have a really solid understanding of those characteristics and attributes, from there we can figure out what tools we need to address them, and that could be creative interpretations of existing contracts.

It's not impossible it's new contractual amendments. But we really, I don't think, can say definitively what this is going to be set at until we have a better understanding of what's really happening out there. I think I'll end with that. Thanks.

JONATHAN ZUCK: Thanks, Graeme. I'm happy to be picked on for my data. No question. I guess the question I have is, is there a … I come back to AlpNames, or some of the other parties that Drew mentioned in his presentation, that long after … It seemed, by any measure, it was obvious that these were bad actors.

It seemed impossible for Compliance to act until they didn't pay their bills, basically, and that feels like bad optics for the organization. And so, I, too, believe that the contracts are sufficiently vague that it's almost ICANN's responsibility to put out an advisory interpretation of the contract and make clear what their expectations are of contracted parties.

And I guess I also feel that a sustained percentage of unaddressed complaints, or whatever form that makes over some period of time, could lead to an investigation that involves the verification of the information, as opposed to just a reliance on a blacklist that might just be based on reports, or something like that.

So, I guess some of this might just be a process question that could lead to a more thorough investigation. But then, even at the end of that thorough investigation, we need to make sure we have the tools in place to allow Compliance to take action.

So, nobody is suggesting that, somehow, you're going to come up with some algorithm and automatically de-accredit registrars based on that data or anything like that.

But the question is, is there a workflow that could be put in place that doesn't catch too many dolphins in the tuna net, so to speak, and figure out how to move forward on some of these bad actors?

So, that's where we're trying to go with this. So, I wanted to pass that back to you, Graeme. My understanding is that the notion of a threshold like this isn't even a new concept to you, and it came up before and was something that you had some favoritism to, at least at one point.

GRAEME BUNTON: I don't know that I would have described my position in that way.

JONATHAN ZUCK: I'm not trying to get you in trouble, either. I'm just—

GRAEME BUNTON: Sure.

JONATHAN ZUCK: Vague recollection on this, on my part.

GRAEME BUNTON: And I apologize. I'm terrible at saying my name for the transcript. I'm not opposed to the idea in principle. But I think, in practice, it's going to really require a lot of work. And maybe a bit going back to the Compliance piece, because I think it's probably worth mentioning.

As we think about how to be creative with our contracts and ICANN Compliance, this is something we talk about inside the DNS abuse team inside the Registrar Stakeholder Group, which is, how do we work with Compliance? Can we look at our contracts and suggest to them tools and mechanisms that we would be supportive? And those discussions are pretty early days but my hope is that, out of those discussions, we have something to offer the community, there.

But we're in a kind of funny spot re. Compliance, which is we want them to go after the bad guys. They make us all look bad, they bring down the industry, they're a pain in our ass. Sorry for swearing. I'm surprised that's the only time so far.

And they drive people within the ICANN community to attempt to achieve policy goals that they say are going after bad actors, but really they're trying to get to apply to everyone, and we don't want that. I don't think that's a secret, right?

So, what we don't want to do, though, is have Compliance sending out, I think someone described it as "parking tickets," to registrars constantly, hitting everyone in the hopes that the bad guys trip up enough times that they can get up with the three-strikes rule that exists.

Because that wastes our time, and registrars would much rather be responding to real, substantial problems. In the past WHOIS, WHOIS inaccuracy requests were eating up [scads] of time for almost no value.

We would much rather that Compliance … We find ways to identify material, substantive issues, and I think that's going to require hard looks at our contracts and support from the community to do so. Thanks.

JONATHAN ZUCK: David, Drew, do either one of you want to come back in based on the things that have been raised thus far, both by other speakers and also by the chat, to the extent that you've been able to follow it? I'm happy to open up for questions.

DREW BAGLEY: I'll go first because I think, building off of what some of Graeme said, it will be natural for David to jump in and respond with what DAAR is already doing, or not doing, or looking to do, and whatnot.

I think that, here, you really have a lot of interests aligned. Because as you stated, Graeme, reputationally, obviously, none of the parties that show up at ICANN want to be associated with parties like AlpNames or others when it comes to, probably, anything, but especially when it comes to discussions about abuse.

And so, that's where, I think, this notion of creating thresholds is something that's really important, despite that fact that, as you stated, you have to make sure the data is valid, and the data piece is critical, and that's where I'd love to hear more from David on that.

But essentially, this data is used all the time in the field of network security, internally, when people are figuring out what they're going to block for their own networks. It's used, additionally, by researchers who look at this data and find it to be valid enough to use for those purposes.

So, the existence of false positives at all is not, necessarily, indicative of all of the data being bad, or of a registrar like Nanjing, with a 93% registration rate, not being associated with a super-high level of abuse. Even if you said, "Okay, not all of that data is real," they might still be associated with 50% that's you'd agree upon.

And so, either way, these things can still be used, for sure, as indicators. And so, with the CCT recommendation, the CCT made a recommendation and then, in the details, just made a threshold suggestion and a suggestion of how the process would work.

But to the extent there is a better process and a better workflow, like Jonathan's talking about, I think that that's where it's important for the community to get.

Because if the first indication, or the first thing that happens, is ICANN Compliance merely has a conversation, the fact that they are even obligated to have a conversation with a party that's meeting a certain threshold of abuse is still, I think, a terrific step for the community.

And then, you can build in with that threshold. Once it reaches a certain threshold over a certain period of time, and after however many attempts by ICANN Compliance to work with the party to do something about it, then maybe that's where there's further action.

And ultimately, you end up where, if you have a party like AlpNames or Nanjing, they could be suspended for the abuse itself, rather than having to find several other things, or rather than it taking years and years.

And then, at the same time, if you have a party like the ones who show up at ICANN, where, maybe, there is a temporary spike in abuse or something, or they can actually call out something with the data used, you're not actually having any real sort of issue.

But I think that's a great thing, because you're able to still do something about this abuse, particularly when we're talking about the registrar is mentioned, or even entire zones, if you're finding this problematic with the zone and with the registry.

So, I think the threshold tool is a very important one that could be helpful, and I think the incentives are aligned. And obviously, it's a matter of getting the details right, there.

But I think the overarching goal still goes back to one of the goals identified at the outset of the new gTLD program, even though we're speaking broader than that, which was to make sure you didn't have bad actors operating registries, and it should similarly be you don't want bad actors operating registrars, either.

And so, I really think that it's important—and I want to hear David's opinion—to get the data right, but it's also important not to ignore data that is, overall, good, merely because it has some false positives, and that should be factored in, of course.

And then, again, the workflow itself. You can factor that. You can factor safeguards into the workflow itself, but I think we really do have a lot, as a community, to do something about this. And so, David, I'd love to hear your thoughts, because I think DAAR can be an important tool with this.

DAVID CONRAD: Sure. One of the challenges that we have, given the data sets that we currently have at our disposal, is trying to identify what's actually relevant. So, with just taking, for example, the CCT suggestions in terms of thresholds, that would mean, based on the snapshot data from DAAR that I obtained this morning, that there would be 11 top-level domains that would cross the 3% threshold.

Those 11 domains represent a total of about 10-11% of all the abusive registrations that are currently seen by DAAR. So, a total of about

622,000 abusive registrations. So, the total that we're talking, here, is relatively small. It's on the order of about 70,000-80,000 abusive domains.

And one of the real challenges there is that, because spam is so frequently used, it skews all the percentages. It skews all the statistics that we gather. So then you say, "Well, okay. Let's ignore spam. Let's focus on all the abuse, so phishing, malware, command and control, that doesn't include spam."

Then you get sort of a different problem in that no one would reach the 3% threshold. In the existing statistics, that tops out at 1.4%. So, okay. Then, you lower the threshold, and then you get into different questions.

And this is making an assumption that you don't want to really care about domains that have fewer abusive registrations than some arbitrary number, like maybe 1,000, or something like that, because you don't want to go after the tiny registries that have one or two registrations that blow their statistics right out of the water.

I think part of the reason that the way we've been trying to look at this as identifying outliers … And then, trying to work with outliers to figure out, A, why they're outliers, and help them, hopefully, mitigate. If they choose not to mitigate, that, in and of itself, is interesting information that can feed back into the community discussions.

If there are actors out there who are aware that a certain business approach that they are taking results in them becoming a home for, basically, a target for all the bad registrants out there, then maybe that is something that the community can undertake as something to explore. Maybe that particular business practice may not be something that is viable if you want to actually have a healthy DNS ecosystem.

So, I am a little reluctant to buy into the model of arbitrary thresholds, just fixed numbers, because there are so many variables that play into what actually is abuse, how the abuse impacts the registries/the registrars.

The one reality is that there are a number of bad registrants, and those registrants are taking advantage of whatever mechanisms they can to be able to be bad, to make money fast, as used to be said back in the day.

And my impression has been that those bad registrants are a relatively stable set of individuals that happen to bounce across registries and registrars where it fits their particular malicious business model.

It isn't usually the case that they are targeting a particular registry or registrar, although that can happen. There have been cases where there are clearly what appears to be malicious registries or registrars. The ones that I'm thinking of don't actually exist anymore.

But the reality is that you have these folks that are sort of bouncing around, doing bad things, and you need to figure out how to make it less enticing for them to do those bad things, and that isn't a function of threshold, per se. It's a function of the policies and the processes by which businesses operate. And just to be clear, this is my personal opinion, not reflecting any position of ICANN.

JONATHAN ZUCK: Thanks, David. We do have some questions. So, if you see questions that are directed to you in the Q&A pod ... And I think, Drew and David, there are questions aimed at both of you. I can read them, or you can type out answers to them, either way. In the queue, here, Brian Cimbolic has his hand up. His unmuting has been enabled. I don't know if he's unmuted yet. Go ahead, Brian.

BRIAN CIMBOLIC: Hi, everyone. I hope you can hear me. Thanks very much for this. I think it's a really thought-provoking session. The only thing I want to say … And here at PIR, we're very committed to fighting abuse, DNS abuse, in all its forms. The only thing I would say is that third-party providers, even if well-intentioned, often can lead into some orders of magnitude to false positives.

So, if you track one TLD's abuse rates month over month, you might see a two, three, four, five-fold increase in "abuse percentage," without, actually, any underlying increase in abuse, like raw, abusive domain names.

And so, there is very little insight into how the third-party providers work. There is little transparency. And so, you'll end up seeing large spikes in percentages across the board with no underlying increase in abuse.

This also sort of reared its head with the spike in COVID registrations where, for .org, for instance, we saw 14,700 domain name registrations related to coronavirus or COVID. A total of 13 of them were actionable for either DNS abuse or website content abuse, limited strictly to selling of fake cures or vaccines. So, that's less than one-tenth of one percent.

And then, we were handed lists that had, essentially, every domain name related to COVID or coronavirus being "abusively registered," including domain names registered by the United Nations that were really serving proper purposes.

So, my point is that, to the extent anyone is relying on third-party data, which I understand because it's sort of all that's out there, we have to be very careful as far as what we rely on and our understandings of the benefits and the potential faults of those lists.

JONATHAN ZUCK: Thanks, Brian. That's certainly something that has really come out in chats in all the sessions this week, about those lists. And so, maybe, part of this is we need to work with some of those list-makers to get things broken out in a more granular way, or something like that.

There was a conversation in the chat going on. Steve DelBianco made the point, I think, more articulately than I was trying to, which was that

I don't think there was ever a sense that there would be some sort of automatic de-accreditation.

As Jeff Neuman said, that shouldn't be the goal, certainly. But when there are limited resources in Compliance, using a persistent high percentage of abuse as a means to have conversations, as David mentioned …

But then, when those conversations don't go anywhere, potentially, being able to do your own investigation but still have the means to dis-accredit a registrar, if there is just a failure or an unwillingness to address the issue that was pointed to by some of that data.

So, again, I don't think anything automatic should happen from the data, but it could provide a pointer, in many respects. Brian, is that a new hand?

BRIAN CIMBOLIC: Sorry, nope. Sorry about that. Thanks.

JONATHAN ZUCK: Thanks. So, in the chat, Fabricio: "[inaudible] measures are a good start, i.e. the Domain Abuse Framework. But is there a way to add transparency so that the community knows that these measures are working and that the signatories are abiding by their stated commitments?"

Thanks, Fabricio, for your question. I think I want to, probably, let Graeme answer that. But part of what we were trying to do was figure out if there were objective measures, here, rather than trying to dictate to contracted parties how they do their job, because that's where there has been a lot of pushback.

The CCT Review generated a lot of very specific recommendations. We've had discussions about bulk registration, for example, and some of the issues associated with that.

And so, what I was really trying to do in this session was see if there was a way to step back from practice recommendations, or regulations, if you will, and find if there were some objective measures that could be used, and leave registries and registrars to their own devices to address the issues that they face.

So, that was the idea behind that. But Graeme, do you want to address Fabricio's question about compliance with the framework? If it becomes the new SEC or something, a kind of self-regulation, is there some way to tell, or metrics to tell, if these frameworks are actually being followed just because somebody signed onto it? Thanks, Graeme. Over to you.

GRAEME BUNTON: Thanks, Jonathan. I don't know that I can speak on behalf of the entire framework signatories, and I know Brian's in the call, so he might chip in, too. We are not set up to have, currently, a compliance team enforcing that voluntary framework.

What we do when people say, "Hey, I want to sign on," is we state pretty clearly to them that we think this should be a meaningful choice. We don't want this to be window dressing. And we state that pretty clearly, and it is our sincere hope that people follow it sincerely.

If someone was really treating that as window dressing and, essentially, abusing the goodwill of that group and the good work that we have done by putting their name on it and doing absolutely nothing, would I be upset if they were called out for that in some fashion?

And I don't collect data on what other people are doing, so I don't think that's going to be me. That would not break my heart, is probably how I would respond to that. Thanks.

JONATHAN ZUCK: Thanks, Graeme. There has always been a reticence, and it is just a fine balance. There has always been a reticence on the part of Compliance to do what people call "naming and shaming," or calling people out, etc.

And so, there is complexity associated with that because, as Jeff mentioned, the goal isn't to be de-accredit anybody, but to actually change behavior. And so, it's certainly understandable that there is a hesitance to do that.

And the question is, where is the threshold after which you do do that, and then information becomes available for the purposes of people making decisions about with whom to do business. Fabricio, I assume you have a follow-up. Go ahead. Fabricio, I don't hear you. I don't know if you have been enabled to unmute yet. Yes. So, now you can. Go ahead.

[FABRICIO:] Can you hear me? Can you hear me now? Oh, perfect. Hey. Thanks. So, I just want to say I think this was one of the most productive sessions that I have attended so far. I just want to thank, in particular, Graeme, to join the Graeme cheerleader squad, here. I've always enjoyed his candor in the conversation we have.

So, I thought it would be helpful to follow up to the discussion, my question about transparency. I think transparency would go a long way to have the community trust what those are signing onto.

And the reason I want to follow-up is because I put in the chat, here, a letter from 2008 that we started a communication with Jamie Hedlund in Compliance that took on the acronym of the ICWP, the Independent Compliance Working Party.

And really, if you take a moment to just read the initial letter, and feel free to read the others, we basically had this exact conversation that we're having here on proactive, data-driven approaches: transparency, everyone agreeing on what the data is, making sure that we cast the net only far enough to catch people like AlpNames that are just obviously egregious to anybody, and not accidentally grab people who are just having variances in registrations, etc.

And I want to hark back, particularly, to a conversation. After this letter went on, I proceeded to sit at a table with Graeme, and Brian, and so many people on this list.

I think we had over a year-long conversation about, how could we come up with, or put out to the community, a discussion about the right triggers, the right net-casting, ensuring that the burden doesn't always fall on all these good parties that are putting money behind DNS abuse and curtailing DNS abuse, and getting constantly painted bad by the bad AlpNames of the world?

And so, I wonder … We had really, really great, productive conversations. We, before Marrakech, had actually gotten to a place where people were saying, "Yeah, it sounds like we could start to think about thresholds and understand what it is we're trying to target so that we're not talking past each other."

And then, that conversation sort of dissipated/disappeared. It seems like it's coming up here again. And I'm just wondering, is there a way that we could all get back to that conversation to the point, here, that the contracted parties are coming up with their own standards and it's something that the community can trust the people are abiding by, and that we're all trusting on the same reports, Transparency of Data by ICANN, etc.?

Because, unfortunately, what I keep seeing is that we have a lot of people who are trying very hard—Graeme and his group, among others, kind of leading the charge, there—and you have a bunch of people in the community wanting something to happen.

And any time we go to Org, Org just throws the pressure back on and makes it the responsibility of the registrars. They take no responsibility and they come up with a lot of data, but they're not willing to stand behind it. They're not willing to engage in any way. It's always someone else's issue.

And I'm just wondering, if it's our issue, can't we just all talk and come up with something that we can enforce, make sure it's transparent as a community, and that we can all agree on, the basis of data, and things like that? Because that's what the conversation was for a year, and then it just sort of, like I said, fizzled out.

So, rather than revisit 2018 and 2020, and then have this conversation again, 2024, when something else comes up, can we just kind of continue this conversation and come up with something that the community can all kind of sink their teeth into and agree to?

GRAEME BUNTON: I'll jump in quickly. I agree, those conversations were good. I see Crystal Ondo in the chat saying that some of those conversations were organized by Bryan Schilling, and maybe it would be good to see some of those revived. I don't think that's a bad idea.

Let's get in the room. Let's think about these creative solutions for Compliance. Let's see if we can move this ball forward in a material way, and not just in the ICANN way have perpetual conversations about the same stuff. Thanks.

JONATHAN ZUCK: Thanks, Graeme. Thanks, Fabricio. Michele, you're next in the queue.

MICHELE NEYLON: Can you hear me okay?

JONATHAN ZUCK: We can.

MICHELE NEYLON: Perfect. Good morning. Just a couple of things. So, there has been a lot of talk about the DNS abuse framework, that a reasonably large number of us, who actually account, I think, for more than 90% of all gTLD registrations globally, signed on for. And I think this is where there is a kind of a conflation of concepts which people really need to be careful with.

Registrars and registries are businesses. The way we function and the way that we are able to function is, obviously, by selling products and services and making money, because capitalism isn't such a bad thing.

So, [they get to be] very careful how a lot of this is framed. And I share a lot of the concerns that others have voiced around some of the blacklists and some of the other sources of data, because they are not all equal.

And just because a domain name is on a blacklist does not mean anything, realistically, because some of the blacklist providers, literally, will throw things onto a list because they fell out of bed in the morning or were in a bad mood.

Or in some cases, they will try to, actually, extort both registrars, registries and registrants, in order to get domains removed from their blacklists. So, I think there are a lot of these conversations that could be had, and I think some of us are happy to engage.

But it needs to be a conversation, not this kind of hyperbolic rubbish which we've seen so often in the last few months, where people take one badly written study or one badly researched article and hold it up as if it were, somehow, fact-based, which, in many cases, it is not.

And those of us who work in this space on a day-to-day basis can point out a lot of the flaws and very, very dangerous assumptions that a lot of these "reports" and "studies" make.

Be very, very careful how this is framed. Be very careful what you wish for. Because it's very easy to tip things over so that you end up where the bad actors, which I hate as a term, are just able to weasel their way around things, whereas many of the businesses who just happen to have attracted one bad customer end up suffering. Thanks.

JONATHAN ZUCK: Thanks, Michele. I think those are all very good points. In fact, that was sort of the thinking behind this session, to get out of the business of trying to dictate practices on the part of registries and registrars and, instead, look simply at results.

And so, the problems with the data are, obviously, extremely important, and we need to figure out what the best way is to address that. But if it's a pointer to facilitate investigation more directly, or something like that, that may be the way to go.

But then the problem becomes, also, once that's established, is there sufficient basis in the contracts? And I guess I believe there is, and, if I heard him correctly, I believe Graeme believes there is – that once you really do have a sense of what the business practices are, there is enough in the current contract to go forward.

It may just be a question of trying that. I don't know the answer, but that's the idea, here, to get out of nit-picking our way through a bunch of practices and building those into the contract, but instead do an interpretation of the contract that suggests keeping things under control, so to speak. I think Fabricio is next. I think these are in the order they're supposed to be, so go ahead, please.

[FABRICIO:] Hey. Yeah, I just wanted to follow up real quick, Jonathan, and you teed it up perfectly. Yeah, that was, actually, the crux of the conversations we had for that, over a year long, which was just trying to find some very high triggers where Compliance could take action.

I'll say it, hopefully, not putting words in Jamie's mouth. It seems, though, Compliance just kept saying, "We really wish we could act, but we're told we can't," or, "we don't see a position," and flank to left and right where folks like me from IPC and folks from the Contracted Parties House are both looking back at Jamie going, "We see things in the contract that allow you to enforce. What's holding you back?"

And that concept of a trigger, a threshold … I don't want to weaponize it, but that concept of when it's so apparent and there is no question, it should trigger, at least, an investigation or something where the conversations were going.

And so, yeah, throw me on that list of those who agree with what you're saying. And what you were saying you think Graeme agreed to, I'll outright say I agree to it, as well, because I think that's what's missing, instead of using that data to trigger when it's really obvious.

What I'm hearing the contracted parties say, and what we're seeing, is that, instead, the Compliance group gets into this low-hanging-fruit ticketing system where it just runs around and [nits] at everybody for things that don't really matter, and it's a huge waste of contracted party time, money, and effort.

It does nothing for the community and people like us, who are asking to bring down the levels of abuse, and that effort could be going somewhere else to take down things like AlpNames, which you rightly pointed out. I think the letter that I put out there quotes the DAAR report that we've heard Conrad talk about this whole session.

They were noted for over, I think, 38% of abuse coming out of this little island, yet they basically operated until they couldn't pay their bills, not because Compliance did anything.

And when we asked why it was Compliance didn't do anything, it was because they were engaging in the exact practice the contracted parties can't stand, which is just shooting off random little compliance tickets, and then closing the tickets when they were saying, "Oh, well, that domain name is now gone," as opposed to addressing the bigger issue based on the data. It will sit right before them. And so, a proactive, data-driven approach with some level of obvious thresholds would do a good service to everybody involved, here.

JONATHAN ZUCK: Thanks, Fabricio. I guess I wasn't watching the panelists tab, and so I don't know how these things work out order-wise. But Graeme, do you have your hand up actively?

GRAEME BUNTON: I do.

JONATHAN ZUCK: Okay, go ahead.

GRAEME BUNTON: I'll be very brief. Thank you. Just a piece on the contracts. I really want there to be something in the current contracts. That would be my preference. And for context, contractual negotiations with contracted parties are long, expensive, drawn-out affairs.

I think the 2013 round, and it's a little bit before my time, took something like 18 months. I think something focused on DNS abuse would take even longer. And so, I think we want to get in front of this faster. And so, I would say that that's probably not going to be the most expeditious way of doing it. Thanks.

JONATHAN ZUCK: I'm inclined to agree, Graeme. I also see Göran's hand up. Göran, go ahead. Sorry I didn't see it before.

GÖRAN MARBY: Thank you. As being the head of ICANN Org, and I hear a lot of comments about my dear friends Compliance and from the … Well, first, I want to state that Compliance and OCTO, of course, work together.

Some of the things that have been said that we are doing with what you would call "bad actors" has been said without knowledge. We believe strongly, and we've done that, that we're trying to work with the outliers, and we're trying to change their behavior.

And while there have been bad actors that we have focused on, we have done that. I really don't know why this discussion goes this way. So, what we've said from …

First of all, we think, from ICANN, that many of those discussions belong in the community. We believe strongly that discussions about abuse mitigation or abuse is something that the community should discuss, which you are doing.

Which means that, when you ask us for our opinions, of course, the answer will be, "We believe this belongs in the community," because ICANN Org and the board is actually prohibited to participate other than from a factual standpoint in the discussions with itself.

There is always something you can develop. There are always things we can do better for us and Compliance. But I'm taking it a little bit of a … There are a lot of things that Jamie has said or ICANN Org has said.

Yes, we have contracts, and I agree with a contract is something done between two parties. And we are engaging with the contracted parties how to understand some of the provisions that are in the contracts. Some of the provisions, by the way, don't come out of policy-making process, which is something that we have to work through.

So, I think that I would like to just … The only question is, do we have enough tools? What I think Jamie has been trying to say … First of all, we have very soft tools and a very hard tool.

The process that is set up for those tools is something we have to go through many different … It's not as easy. We have to go through. And I think that, in its very transparent way, we have to go through many different parts of the process to be able to achieve a result.

And when the discussion ends up in a sort of way saying that we have, already, contract obligations: Jamie hasn't done a job, or I haven't done my job, or we don't have the right things.

What I think is important in this discussion is what [I would have come here] to discuss. How do you find, from the community perspective, the abuse? How do you see abuse evolving? How do you see the effects of the abuse that you've seen from COVID-19, but also the things that David presented?

Our job, there, is very much to help and facilitate that discussion. And then, what Compliance is is, basically, the place where we [check] that the policies are in the contract and we're actually following what the policies have [set forth] from the beginning. That is the role of Compliance.

So, for some of the speakers who made those accusations about the way Compliance works, it feels like you are on the wrong avenue. You are having a good discussion, I think, and it's in the right place. It belongs in the community.

And to some extent, then, after that, it also belongs in the discussion between implementation in the contracts. But please, please, let's not make this into if Compliance has enough tools or not. It has to come from the community.

JONATHAN ZUCK: Thanks, Göran. I think everyone agrees. That's why we're trying to have these conversations. Because I think there are people that show up for meetings, show up for Zoom calls, etc., on these conversations, and there are those who don't, and I think that a lot of the actors we're talking about in this particular session are those who don't.

And yet, there is a lot of, as Graeme said, concern over everyone's reputation being painted with too broad a brush. So, I think there is consensus about trying to find a way forward with those, and that is something we're trying to work out in the community. Brian, do you have something, quick? I think we're running out of time, here. Cimbolic?

BRIAN CIMBOLIC: Yeah. Thanks, Jonathan. Just a couple of quick things. The provision that Graeme was mentioning in the contract for the RAA is section 5.5.2.1.3, which, for those DNS operators out there, would be equivalent to a fifth-level domain, which says that ICANN may terminate if it gets a declaratory judgment, if a registrar is with actual knowledge, or gross negligent permitting illegal activity, or, essentially, DNS abuse. So, that is one tool in the registrar arena that ICANN has.

I just also wanted to touch on the framework to address abuse. It's a voluntary agreement. It's non-contractual. It includes ccTLD operators, including some of the biggest ccTLD operators in the world.

It's not something that you want to discourage participation in, and if you make it some sort of Contractual Compliance tool, that's exactly what would happen.

The only thing I would say, too, I would encourage, if you were finding a registry or registrar that has signed its name up to the framework to address abuse and it is not living up to its obligations, then that should be known. But there are instances where people reach out to us under the auspices of the framework to address abuse, with things like copyright infringement and claiming it's phishing, when clearly not.

So, don't let a good deed go punished. The framework to address abuse is a good thing. I think it's a very positive step for our industry, and I hope more registries and registrars sign up to it in good faith. But to the extent you're finding that that's not the case, let that be known.

JONATHAN ZUCK: Thanks, Brian. I guess that's a good note to end on. Before I leave, I just want to say that my attempts at dark humor at the beginning of the session might have offended some people, and if they did, I apologize. That was not my intention, just to mix things up for people in all these different time zones.

So, appreciate you participating in this conversation. And I really want to thank David, Graeme, and Drew for being on the panel. I appreciate everyone's participation and for being a part of this session. Thanks. And with that, we'll close.

[MICHELLE DESMYTER:] Thank you all very much for joining.

[END OF TRANSCRIPTION]