MONTREAL – At-Large Policy Session: DNS Abuse - End User Concerns
Sunday, November 3, 2019 – 13:30 to 15:00 EDT
ICANN66 | Montréal, Canada

JONATHAN ZUCK: Welcome everyone. If there was a subtitle, whenever you go see a movie poster, you see the name of the movie and then there's often a subtitle, you know, Back Again With A Vengeance, or something like that. And so this being the 65th sequel to ICANN the movie, this is ICANN66: DNS Abuse, right? It comes after the colon. If there is a theme to this ICANN meeting, it's probably this discussion of DNS abuse.

And so this particular session is really meant to be a kind of inside At-Large session to table set some conversations about a statement that we might try to come out with by the end of this meeting about DNS abuse and recommendations and there's a lot of recommendations floating around and there are also some activities that are already happening in this regard. And so we're trying to level set this and have an open conversation about this concept of DNS abuse, how it's defined, and what's best to be done about it, so that the At-Large can more easily form its own perspective on that.

And so to help us with that discussion, we have three guest speakers, two of whom are here so far. So, the first is Drew Bagley, and he served with me on the CCT review team that made a number of DNS abuse related recommendations, so hopefully he'll be here to talk about those recommendations. We have Graeme Bunton, that if I understand correctly, was sort of the shepherd of an effort by a subset of the contracted parties, registries and registrars to come out with a proposal, a framework for improving response to DNS abuse and that has also with it a component definition of DNS abuse, and so I've asked him to come and share what that looks like and what the thinking is that went behind that.

And then finally, Jamie Hedlund, who is head of ICANN Compliance, began his work for ICANN just as a lowly lobbyist and was pressed into service by Fadi to be a member of the CCT RT, the CCT Review Team, along with me, and Drew and Kali. And rather than waiting for all these processes to work their way through the bureaucracy of ICANN, he took the initiative when he took over the compliance to begin trying to make some reforms within his organization to deal with some of the issues that we found out about as part of the CCT Review.

And so we're really appreciative of that and I wanted him to get a chance to discuss some of those reforms, again, to provide the context for the discussions that we're having I mean, it should come as no surprise that this is an issue of particular interest to the At-Large, because we are tasked with representing the interests of individual internet users. And while there's a lot of talk in the community about the interest of registrants, the people that register for a domain name, there's another 4 billion people that aren't registrants that are just trying to use the internet and are concerned about DNS abuse in its many forms and many definitions.

So I think the best way to get started is probably to go to Graeme, and Drew is just showing up here, so we'll go to Graeme first, no, you know what, let's start with Jamie, if that's all right, because that's something that's already happened, right, and then we'll do Graeme and then Drew as an overview, and then let's have an open discussion about it. Alright, thanks, Jamie.

JAMIE HEDLUND: Thank you, Jonathan. So yes, I did start as a lowly lobbyist. I'm still a lobbyist. I'm from Cook County, Illinois, which is famous for its politics, so I'm a lobbyist and I'm proud, but I'm also here in my role as heading up contractual compliance and consumer safeguards and happy to talk about some of the other things that we're doing related to DNS abuse. But first on the CCT Review, during the deliberations of the review team there was a lot of discussion about data and granularity of data and reporting abuse, and we were very happy to implement a lot of the recommendations even before they had gone to the Board for approval, because we're all about reporting and transparency.

The compliance puts out a lot of reports, I would refer you to our page, and we put a lot of work into these reports and reporting the different types of complaints, as well as not just abuse, but laying, listing particular types of abuse and what we're seeing, and how they're getting resolved and when along the process they're getting resolved. The problem is we don't get a lot of visitors to the website and so we want to report information because it's important to be transparent, but we'd also like to report information and data that people want to see.

So a plea I think I've made here before, but will repeat again is, if there's data that you are not seeing that you want reported on, please share that with us. We will continue to turn out reports, as you know there's a separate project going on, open data platform, which will eventually roll out and all the compliance data will feed into that and so people will be able to make their own custom reports, but we'd also like to continue to create our own reports that tell a narrative that's true, but also that people are interested in. So I hope that's responsive to what you were looking for.

JONATHAN ZUCK: So Jamie, you would say the majority of the things that you've implemented thus far were just about data availability and not the other aspects, you haven't changed audit practices or anything like that, that were related to those recommendations.

JAMIE HEDLUND: Not directly related to the recommendations. We did have a DNS audit of registries recently on DNS abuse, I'm happy to talk about that. There is an indirect relationship between that and the CCT report, along with others, really highlighted abuse as an issue. And so we, for the first time did a sort of risk based approach to the audit and focused on DNS abuse exclusively and the obligations to the extent that they are in the contracts.

JONATHAN ZUCK: This is Jonathan Zuck again for the record, I guess I should keep saying my name. One of the primary findings of CCT was the lack of tools for compliance to deal with these things in a kind of a holistic manner, in that it's very complaint driven and without putting you in a difficult position in the job that you're in, it's still the case that you are more driven by complaints than you are, you're not better able to be proactive in saying, finding a dot science or something that had 50% DNS abuse registrations and doing something about that. That's still not something you're empowered to do, is that right?

JAMIE HEDLUND: What we do is we enforce the contracts and we enforce the contracts as they exist. We don't have the ability or authority or frankly the bandwidth to enforce things that are not included in the contracts. Our remit is what's in the contracts. There are discussions in the community that are ongoing right now about DNS abuse.

We have a separate discussion with the registry stakeholder group about one individual provision. A lot of work is complaint driven. We do audits, but as was just the case, the audit that we did for the registries on DNS abuse was limited to what's in the contracts. Graeme, go ahead tell us a little bit about the document that you just released.

GRAEME BUNTON: Sure, my name is Graeme Bunton, I work for Tucows. I also happen to be Chair of the registrar stakeholder group, although what I'm about to talk about was not a registrar stakeholder group initiative, so I'm sort of taking that hat off for the moment. First, I guess, thank you for having me. I don't think I've actually talked in an ALAC panel before, so it's nice to be here and see some new faces.

So a number of registrars and registries, I think there were 11 of us could hear some of the grumbling within the community in recent months around DNS abuse and we were sort of talking amongst ourselves and feeling what I would describe as frustration with some of the lack of progress on this issue, especially because it felt like we just kept dancing around different definitions of what DNS abuse meant. Some people want to keep it strictly as narrow as possible, some people want to have it so broad, as it includes every unpleasant activity on the planet.

And we felt like, as people who operate the DNS on a daily basis, that we had some real expertise we could bring to the table. And a bunch of us happened to be in DC for a separate meeting but we scheduled some time to get together and see if we could come up with something that we felt was a framework on DNS abuse that provided a definition that we could rally around and help us to move forward and allow us to really sort of default to action.

And so that's what we did. We published a framework on DNS abuse, I think we put it up on Circle ID. I don't have a shorthand URL for it which is gently ironic, as a registrar, and we'll look at getting that.

What this document does is it really lays out, and I don't think this is really a secret, it lays out the things that we think we're doing already, and the things that we think the entire industry should be doing, but we'll leave it for others to adopt as well.

And so that is, on DNS abuse, I'm going to make sure I have this in front of me and I don't screw it up, the things that we feel like we must action are going to be malware, bot nets, phishing, pharming and spam, insofar as spam is a vehicle for any of those other above things, and that to us is the core pieces of DNS abuse that the registrars and registries that have adopted this framework will action. I was asking our head of compliance, Reg, who may or may not be in the room, just how many of these things we're actioning on a daily basis and it's something like 100 domains a day that Tucows is taking down for these sorts of activities. So these are prevalent, they're common, and they're something that we are all tackling right now.

The document also does something kind of interesting which is we expanded from the things we must do to the things we should do as well, and included some areas that are outside of DNS abuse that RE content abuse, that we think is so harmful to humans that we will act at the DNS layer. And boy, is that a narrow number of things, because we take our position as internet infrastructure very seriously. And we want to ensure that when we're acting at the DNS layer that we're being careful responsible and thoughtful in these actions and that the actions we take, especially the DNS layer where we do not have a lot of granularity, are proportionate to the harms.

So on the list of things that we should do is See Sam Child Sexual Abuse materials, human trafficking, the sale of opioids, and I'm missing one more thing, oh, Specific Incredible Incitements to Violence. Those are things that are outside of DNS abuse that the people who signed on to this framework will also action. And we think that this is a real positive step. It again sort of captures what we were doing already and provides I think a really nice place for us to get more people on board and keep pushing this forward.

So I should probably offer some apologies to people who weren't in the room as we worked on this. We knew that Montreal was coming up very quickly and definitely wanted to get this done as quickly as possible and we're still working at ways that we can ensure, other people can adopt this framework and join us in tackling these issues, and so I look forward to that, and then we're going to figure out what other edits and changes we need to make to that framework too, going forward.

So I think that's sort of the bulk of that initiative, I'd encourage people to go read it and have a think and we can discuss that definition that we've proposed and see if that helps move this community forward as it talks about DNS abuse. Thanks, Jonathan.

JONATHAN ZUCK: Thanks, I guess I'm going to hold questions until we're done, even though I grilled Jamie, that was really more for fun. Drew, go ahead, talk a little bit about CCT and the recommendations we made there and then we'll get the conversation going.

DREW BAGLEY: Absolutely, thank you, Jonathan, and thank you for having me. This is Drew Bagley, for the record. So as Jamie alluded to a bit and as I know I've discussed with this group in the past, the CCT review team looked holistically at the new gTLD program and many things that were within our mandate, and within that was a close analysis of the safeguards put in place as part of the new gTLD program to mitigate against types of abuse that were identified by the community prior to the expansion of the DNS.

And then looking at that, the CCT review team took a data driven approach in which we analyzed the actual safeguards put in place, but then we also commissioned a study that looked at the degrees of abuse, which were defined very similar to the way in which Graeme just explained in the framework because we were looking at security related abuse which, abuse is naturally much broader than that, but we looked at that with the study and took a data driven approach to that and the study showed that despite the safeguards put in place, there was still widespread prevalent abuse both in gTLDs as well as the new gTLDs, but that it was not just random. Instead, DNS abuse is highly concentrated and seems to correlate with things that we as a community can take action to mitigate.

And so consequently the CCT review team came up with a series of recommendations aimed at fixing the current broken model with regard to abuse and providing three categories to help with abuse. So one was data driven and another was incentive driven, and another one was intended to actually enable ICANN Org to take action where necessary. And so among our recommendations we recommended that ICANN Org regularly publish abuse data related to these more security oriented types of abuse and so that way we can see where the infrastructure really is within ICANN's remit of being in charge of security and stability of the DNS, as well as have data driven policy discussions and see how we're moving the ball going forward.

Additionally, we recommended that incentives be explored, including the potential for financial incentives to incentivize proactive anti-abuse measures being adopted by registries and registrars so rather than merely waiting until there is a complaint and therefore there is likely a victim of a form of security abuse, to take some basic steps at hygiene in the beginning to help facilitate abusive domain name registrations not persisting in a zone for very long or persisting in an account for very long at a registrar.

And then we also proposed that the agreements be amended to include mechanisms whereby infrastructure providers cannot tolerate certain levels of abuse, but should be expected to take actions at certain levels. We did not mandate what those levels should be, but we did put some suggestions of what we thought, based on the data we were seeing, would be helpful to explore. And so the key there was to give ICANN Compliance the tools to go after systemic abuse.

So as we echo time and time again and echoed when we were discussing the CCT review team findings, from what the data shows and from what data shows in reports often published, generally speaking, even though abuse is prevalent everywhere, it's not the registrars who show up to ICANN who are the facilitators of this sort of systemic abuse. Instead, it's the party's not here. So while parties here might think of ways to take action outside of any policy changes, there's still a need for policy level action for all those parties who don't show up.

And so the poster child for some of our recommendations was altnames which many of you may be familiar with, but we saw these characteristics where you would see either the allowance of bulk registration or DGAs or different things like, that combined with systemic levels of abuse that would be 50% of all the domains being registered by registrar or even higher percentages within an zone of a specific TLD.

And so that's why we took this approach of recommendations that hopefully would provide incentives for good actors and then provide a means for ICANN compliance to take action against those who either weren't good actors or might be good actors, but just not have the means to deal with that abuse without, you know, a little corralling.

JONATHAN ZUCK: Okay, thanks. So, just to mix it up a little bit, let me go to Graeme and since you said that the document was more about here's what we're doing, why don't the rest of you do this too sort of, right? Are there things that you're not doing that you think would be good ideas or that you're exploring doing, and what was your reaction to the recommendations made by the CCCRT when I'm sure you read those when they came out, or heard about them, or whatever, right? Because they dealt with you directly.

So, I'm interested in sort of both those things because they're related, right? I mean, those are some specific recommendations, do you like those, hate those, and are there other things that you would like to see your industry doing on DNS abuse that you're not already doing?

GRAEME BUNTON: Thanks, Jonathan, this is Graeme for the transcript again. So, I'm going to defer to one of my other colleagues who I'm pretty sure are in the room on the CCT stuff because I was not dialed into that, and I can see James and I bet Brian's back there somewhere, other people that worked on this, and so maybe they have input on that. So, this document, though, is what I would consider to be a floor, not a ceiling, and so in that we leave unlimited room for registrars and registries to take the action that they might want to do above and beyond that, and would encourage people to do that, as well.

So I think setting this, I would love to see everybody get in the same place, as this as their floor and I think, boy, we can spend a bunch of time working on that and getting everybody up to where I think they should be, and then we can talk about what's next. But let's make sure that we've really hammered home this core set of principles, and maybe James has some CCT bits.

JAMES BLADEL: Thanks, James speaking from GoDaddy, and yeah, I think we were also participating in the development of the framework as setting a jumping off point where we have common overlap for all of our practices. I was encouraged, I think Drew, that you pointed out yet again, and for folks who are new, that the abuse is focused primarily on the registries and registrars who don't regularly attend ICANN. It is marginalized within this community.

So my response to the CCT was, I thought it was very informative, the report, I thought it was probably a little overdue in some respects, but I am a little less enthusiastic about the conclusion that new policy is necessary, particularly when we understand that, for example, I think registrars in particular understand that the RA has provisions for ICANN to act against registrars that are involved in illegal activity and I think that perhaps could be more aggressively enforced, and I'm kind of looking in Jamie's direction here, I know he has other constraints and equities that he has to answer to, but I think from a registrar specific perspective, drawing that line a little more, making that distinction a little brighter between the good guys and the folks who are clearly operating on the margins, is valuable.

And I also think that creating additional obligations is somewhat chasing our tail, because we have to create those things through a

PDP process that's out in the open, that takes years to develop, and anti-abuse practices to be effective have to be somewhat less transparent than I think the ICANN community is used to, or the expectation of, because you don't want to telegraph to the bad actors what your practices are and how to evade them and how to skirt around the edges of detection, and we also don't want to assume that the bad actors are at the table participating in the policy process, that could also be a scenario.

So it's something that I think that non-standardization is maybe a good thing and we should we should consider that registries and registrars working to develop something that's specific to their customer base, their geography, their business model, might be more effective than a blanket ICANN policy. But otherwise, again, very supportive of the CCT and its recommendations, I'm just concerned, I stop short of we need new policy.

JONATHAN ZUCK: Jonathan for the record. I just want to give Drew a chance to address some of this. One is what is your feeling on the definition question, I guess, a little bit, and also, why do you think that new policies are necessary, what are the holes that you think need to be plugged in a global way if it really is just marginal players that are the problem?

DREW BAGLEY: Sure, thank you, and thank you for that reaction So, first of all, just for clarification, and this is Drew Bradley for the record, that's the clarification, now for the confusion. So, there's nothing mutually exclusive about the CCT review team's recommendations and the ability of registrars and registries to design anti-abuse measures that are appropriate for them. Instead, our recommendations are tailored over means by which ICANN Org has tools to go after systemic abuse, as well as building in incentives for operators to adopt proactive anti-abuse policies, rather than being prescriptive about either.

So, just for clarity, those things are not incompatible, nor is it incompatible for innovations to take place in parallel with regard to anti-abuse. But where there is a current gap now is with regard to this notion that the entire universe in which we operate is a very reactive one right now, whereby you have to wait for the victim or someone on behalf of the victim to file a complaint, even for these cybersecurity related areas of abuse, which are ones where you can find out relatively quickly whether or not a domain name is associated with something being used for what we in the CCT review team report call DNS security abuse and like I said, very similar to the definition you're using, Graeme.

And so that's where that's just really problematic at the speed at which cyber threats occur. If you look at ransomware that was enabled by DNS, you can look at a million things enabled by DNS and that's why not only is this approach outdated with regard to those categories of abuse, especially, but it's also something that's not really sustainable going forward, and so that needs to be turned on its head and it's certainly a gap where there needs to be a policy solution.

So even though the systemic abuse, that's the one where I think that's something where, like I said, what we saw with the data, it's the actors who don't turn up at ICANN that tend to be associated with the systemic abuse. That doesn't mean, right now there has been a means to proactively go after that. Again, that's very reactive in terms of being complaint driven by domain name. And so that's a thing that we identify where that doesn't really account for these issues of high percentages of abuse being associated with a single actor. So that's where we thought that was absolutely necessary from a policy standpoint to build those tools.

And with regard to your question, Jonathan, about the definition, I think that the definition for DNS abuse obviously is one where if you say DNS abuse, there are several different categories of abuse but what seems to be some good news right now is that at least now that we can start dissecting those categories of abuse and identifying consensus around certain areas of abuse, we can start taking actions against those areas, whereas I think just a couple years ago people were throwing up their arms and saying, oh, since we can't define all areas of abuse, we can't take action against any areas of abuse.

So I think that this is absolutely a positive development to see some consensus around that and from the CCT's report what we actually found to come up with our definition we looked at a decade's base of consensus around the security oriented definitions of abuse, including in the community work that went in place before the new gTLD program in order to create safeguards that were baked into the new gTLD program. So the consensus for security related DNS abuse has existed and I think that this is a very positive development now to see some baby steps of action being taken around that.

JONATHAN ZUCK: I can answer the question I guess perhaps more directly, Drew and Graeme, and maybe Jamie, but it may be harder for Jamie to be in a position to answer, do you think the definition as it's currently proposed either by the CCT or by this document, I don't know the best way to talk about the group, so I'm just calling it the Graeme document for now, but do you think that it's sufficient to encompass all that's considered in the contracts?

In other words, because Jamie said we're limited by the contracts, et cetera, so there are things about legal activity, et cetera, is the definition of DNS abuse, et cetera, that's being bandied about enough, does it encompass all that's envisioned by the contracts as they currently stand? And I was going to ask I guess all of you.

GRAEME BUNTON: Sure, this is Graeme. I guess I would not call this the Graeme document, I would definitely call it the Brian symbolic document GC for PR, he did all of the heavy lifting on this, I just showed up and smiled pretty. I think the framework that we put together encompasses everything in the contract, and I would say goes above and beyond that, too.

UNKNOWN SPEAKER: So in the registrar accreditation agreement there's 318 which is the obligation to have an abuse contact and investigate and respond to abuse which is not defined and when we get complaints about those, we make sure that the registrar actually did the things that they're supposed to do. In the base registry agreement that was developed for the new gTLD program which Drew recommended, there's Specifications 11-3B which imposes a requirement on registries to scan their zones, and monitor for specific security threats, phishing, pharming, malware and bot nets to create a report and make that report available to ICANN and in the reports which also include actions that the registry may have taken, that's Spec 11-3B is what this most recent was mostly about. And in terms of DNS abuse, that's the way it's being talked about now that's pretty much the universe of obligations that exist in the contracts.

UNKNOWN SPEAKER: I think it's compatible with the language used in Specification 11, as far as the types of abuse identified, but then with regard to what those technical measures are, how that's defined, that's something that could, depending on the operator, they could go broader than that, and interpret their obligations under the agreement, or depending on your interpretation of their obligations under the agreement, Jamie, they can go broader than that, but the definition I think seems to be compatible there, whereas with the registrar agreement I think it's compatible with what you often see in registrant policies that a registrar imposes in terms of certain prohibited activities but naturally things can go broader than that.

So I don't know that it's the same, but I don't know that it's different either, certainly not incompatible, just as Jamie mentioned, just because of the distinction in language used there. But again, what I think is a positive development is this identification of a specific category of abuse and therefore, then the ability going forward to discuss that and do things about that and then hopefully in other areas of abuse to also ensure there's positive steps going forward to mitigate it.

JONATHAN ZUCK: I guess one last question from the Chair here, there was part of the Board's response to the CCT Recommendations and the data that's reported, it talked about the actual name of the domain name that was involved and it sort of left open the fact that it was still being considered, whether that information will be disclosed, which would facilitate end user choices around the vendors they used based on complaints that they've received, et cetera, and again, Jamie, without putting you in an uncomfortable position, is there anything you can share about the progress of that thinking, because that's something that I think folks have been interested in for some time.

JAMIE HEDLUND: So, that's one of the recommendations that remains pending...

JONATHAN ZUCK: It's an accepted recommendation, but said that that particular data element was still being discussed, so that's why I just want to know if there's anything you could share about that.

JAMIE HEDLUND: Right, right, so, there's not a lot that we can share, one of the dynamics that we face, not just with this, but in transparency around complaints in general, is right now when we get complaints, they enter in the informal inquiry stage and at that point they are confidential and they're confidential for two main reasons. One is when they are confidential and there is a naming and shaming, there's often a greater chance that the registry or registrar who is complained about is going to cure more quickly than if exposed to the whole community.

The other big reason is about 75% roughly of complaints that we get are invalid. So, there is no value in making transparent something that didn't happen. When you get past the informal inquiry stage and there is a refusal to cooperate or to cure and it's a valid complaint, at that point we do issue a notice of breach and that is public, and that would probably include the domain name, depending on the specific complaint. But I think we are looking hard at what point does it make sense, does this tradeoff between transparency and compliance and making it available for consumers to view, when does it tip on the side of disclosing the name?

JOANNA KULESZA: We go to the audience, sir, you've been waiting for a long time, the mic is yours, go ahead.,

MARK SEIDEN: Hi, Mark Seiden for the record. If I read Brian Krebs' column last week correctly, there was a big data breach at multiple registries and these things are reported to ICANN under the agreements, but ICANN has been so far reluctant to publish anything about identity breaches at registrars. Have you made progress on that in terms of transparency? And do you have any intention of performing postmortems for the improvement of overall security in the community so that other registrars will not be similarly affected?

JAMIE HEDLUND: I can't talk about any pending complaints, but you are absolutely right that there is an obligation to report data breaches related to the DNS, and those initially go to GDD and then to Compliance for enforcement.

MARK SEIDEN: But that's not something you report on currently to the community?

JAMIE HEDLUND: I'm not sure if we have ever reported on that in the past.

MARK SEIDEN: I can tell you, you haven't reported in the past, and have resisted reporting on it, claiming that you can't tell what in those reports are confidential and what is intended to be republished, and my suggestion is anything in breach reports which, by the way are often reported to the public by requirement of statute in the place where the registrar is, should also be reported by ICANN to registrants for their protection.

JAMIE HEDLUND: Thank you.

JOANNA KULESZA: Thank you, we are going to go with the audience first, and the mic is yours, but I have the flags queued up here, so we will go to the flags, next.

ANDREI KOLESNIKOV: Okay, a short question, straight to the subject, Andrei Kolesnikov for the record. ICANN provides the DAAR report to the registries where quantitative and qualitative measures of the current abuse levels for the registries. Do you see any feedback from the contracted parties? Because that's regular reports available through the API and how does the registry respond to that? It's not on a contractual obligation, this report is not the part of the contractual obligation as far as I understand, so it's kind of voluntary from the ICANN side. So, is there any reaction? Is it betting better after the service became available?

JAMIE HEDLUND: DAAR is not a Compliance program, it's run by OCTO, the Offices of the CTO, and it was undertaken as part of our commitment to reporting on the security and stability of the DNS. My understanding is that there's a session this week, meetings with the contracted parties and OCTO to talk about DAAR, there has been discussion about ways to improve it. But OCTO is not doing it because they have a contractual obligation, they're doing it as a matter of research that they think is important for security and stability.

ANDREI KOLESNIKOV: Great, no answer. No answer is an answer, good.

JAMIE HEDLUND: Tell me what your question was, I'm not trying to be evasive.

ANDREI KOLESNIKOV: My questions was, after this report became available, was it getting better as a reaction from the registries?

JAMIE HEDLUND: I think you'd have to ask Registries that question.

JOANNA KULESZA: Alright, one more question from the audience, sir, and then we go around the table. Go ahead.

UNKNOWN SPEAKER: The name is Jean-Philippe [inaudible] for the record. If for example a powerful outside entity would come at DNS abuse, for example, governments, billionaires, whatever, registrars will take action against this entity and that entity would retaliate. Would ICANN offer any kind of support to the registrar to help them fight this retaliation?

JOANNA KULESZA: Is your question directed at any of our panelists?

UNKNOWN SPEAKER: No one in particular, I just want to have an idea what would be ICANN's policy in such a case.

JOANNA KULESZA: Perfect. Is anyone willing to pick that up? Graeme?

GRAEME BUNTON: This is Graeme for the transcript. It's kind of an interesting scenario. My hunch is that we'd have to talk about it with ICANN, but my company is essentially constantly under DDoS for any number of reasons, and I would suspect that's true for just about every major registrar and every major registry, and I think that's just part of the cost of doing business at the moment. If it were ever to, and it does occasionally, it has happened in the past, where it has escalated beyond our capacity, I don't think we've ever taken that to ICANN, but as a threat to the global DNS, it's probably worth having some conversations.

UNKNOWN SPEAKER: Yeah, I'm just to make it clear, I wasn't necessarily talking about DDoS but also talking like lawsuits and such

JOANNA KULESZA: That is an interesting question Thank you, sir. It's fully taken on board. I don't think we have a readymade solution, but it's an interesting question Thank you for posing that. I have a list of speakers from around the table I have Seun, I have Tijani, I have Alan and Holly. We'll start with Seun and we'll start with a question and answer. We have plenty of time so ask your question, and then we'll go to the answers. If times are scarce, then I'll collect the questions. Go ahead, Seun, the floor is yours.

SEUN OJEDEJI: Thank you, this is Seun for the record. I just wanted to mention first that at the table, I don’t wear any special hats. I was listening to the speaker from GoDaddy and that was when I had to put up my card and looking at the report that was mentioned, that was referred to by Graeme, I saw that GoDaddy is actually part of the participants in that reports. But it begs the question, is there a real intention to solve a problem here?

The question is, are you actually seeing registers or registries seeing the abuse as a business for them because if they are seeing it as a business then simply means that it will be difficult to solve the problem. If they are seeing it as a business model, then solving the problem simply means that we shouldn't even waste our time in trying to get a solution. So the question is, I have no intention, I mean, I don't intend to pick on GoDaddy, but I think that from the response I got from them It does seem like they don't want the problem to be solved in a way that actually makes this abuse go away, to some extent. And I'm speaking as a typical end user here, and I hope to be seen as such. Thanks.

GRAEME BUNTON: This is Graeme for the transcript. I'll let James respond because you've picked on him a bit and as much as I enjoy picking on GoDaddy, I don't think that's probably fair. DNS abuse is bad business, so the reality of being a registrar is that anytime you need to look at any specific domain name, you are never making money on that domain name ever again You're making probably a dollar or two dollars, that's the economic reality of this. And so having a clean platform is a profitable platform And so there is no good business in serving lots of abusive registrations.

UNKNOWN SPEAKER: If I may chime in once real quick and then I'll defer to you. Along the same lines, there's actually a report that one of the organizations I'm affiliated with, the Secure Domain Foundation did several years ago on the cost of domain name abuse and it was based off of surveys with registrars and registries and it goes into charge backs and all the other costs associated with DNS abuse. I would just encourage you to look at that and I think that that echoes a lot of what Graeme is referring to.

JAMES BLADEL: So just to respond, this is James again from GoDaddy, just to respond to the previous speaker. I'm not sure which part of my previous intervention left you with the impression that you raised. We have probably between 20 and 40 individuals working full time, we've invested significant amount of dollars and time and developing tools to combat abuse.

Our digital crimes team is probably on par with any private entity cybersecurity team that you could imagine in this space. So I guess I'm confused. We don't make any money, we don't get any really a lot of credit for doing these things, it's just a necessity to keep the bad stuff off of our platforms, as Graeme mentioned.

I think that if you heard any concern from me, it was a question of how effective can this space, can ICANN be in addressing some of the problems that we've raised, and I think what the framework that Graeme and I and our company participated in and developing, what the framework says is that there are some areas where ICANN can be effective that are specific to DNS security and stability and then there are some particularly egregious content type issues, but beyond that, consensus policy coming out of contracts enforced by Jamie and his team are probably not the right instrument to address this, that we have to look at other areas and other efforts.

so I don't know, I apologize if I left you with the impression that it wasn't profitable to take these steps. We certainly incur those costs and bear those burdens on our business to keep a clean platform and to maintain a high standard and a good reputation in this industry So I hope that helps your perceptions. Thanks.

JOANNA KULESZA: Thank you, that's an exciting discussion we're having. Tijani, you're next.

TIJANI BEN JEMAA: Thank you very much, Tijani Ben Jemaa. Thank you for this certification and thank you, Graeme, for introducing the document. I read it and I agree with the definition. Nevertheless, since we are in ICANN, we are ALAC, so ICANN, you are a registry stakeholder group, you are ICANN, we are working under the bylaws of ICANN and the bylaws of ICANN make it clear that the content is not included in their mission.

So when you speak about harmful content, even if it is more or less agreed on, it cannot be different from one country to another. So I think that you as an individual registry or registrar, you can perhaps act at the DNS level, because of the content, but you will do it according to your local law or your applicable law, you cannot do it, we cannot speak about it here in ICANN because we are not allowed to judge or to assess content. Thank you.

GRAEME BUNTON: This is Graeme for the transcript. Thank you, interesting point, I agree about the bylaws, that has never stopped anyone from talking about content issues in the history of ICANN. But to your point, one of the reasons that this was not a formal stakeholder group initiative and was a voluntary action from a few contracted parties is because it does go outside of strictly DNS abuse and addresses a couple other things, and that is at our discretion. We're private companies we're publicly traded companies, however you want to phrase that, and we can choose to adopt these things as we see fit, and that's what we've done. This document is not ICANN policy and did not go through the ICANN policy process and that's why it got done real quick. Thanks.

JOANNA KULESZA: Thank you, I'm going to finish my queue from around the table, I have John, I have one more participant, but first to Alan, then to Holly, then we move back to the audience. Thank you.

ALAN GREENBERG: Thank you very much, Alan Greenberg speaking. The project that Graeme reported on is really encouraging, and Drew made the comment that policy is needed to allow ICANN to enforce things. I disagree. There's two ways to give ICANN tools to enforce things. It could be through policy development or it could be through contract negotiation. So what I'm seeing missing, still, is real cooperation among all of the players. So Graeme's project is really encouraging because it's the registrars and registries talking to each other and coming up with something real viable and practical.

But I also hear around the table that, well, this is an OCTO project, not a compliance project. I will be really encouraged and rest a little bit easier, when I see and hear the registrars, the registries, Compliance, OCTO, and any other parties that are involved in this sitting around and saying, what can we do as a group to make this better and to address the problems and not just have these little quadrants that don't talk to each other, don't cooperate, and say we can't work, because I believe together we have the tools to put together the mechanisms for at least the good registrars and registries to take action, to give ICANN Compliance the tools that they can use to enforce, and I want to see the registrars and registries sitting around and plotting how can we build these tools so the people who aren't the honorable ones can have action taken against them by Compliance and if OCTO is an interested party that has developed some tools, they should be sitting there too, and figuring out how can we put all of this together to make it actually work and not have isolated little islands. Thank you.

UNKNOWN SPEAKER: Alan, just to clarify one thing, when I said DAAR was an OCTO project, I want to be clear that it didn't arise out of the contracts, but in the most recent DNS registry audit we did in fact, Compliance did in fact coordinate closely with OCTO in the development of the data that was used for the audit.

ALAN GREENBERG: That will add a bit more encouragement, but I still don't see the level of cooperation that I think we need to really address these problems. I think Drew was trying to talk.

DREW BAGLEY: This is Drew for the record, and I just want to clarify, too, the way that the CCT Review team reframed some of the recommendations I mentioned was actually through the contract amendment process and getting the parties to the table, building these things into the contracts which would then provide that means by which ICANN Compliance would have the tools.

ALAN GREENBERG: I knew you knew the answer, but here it was talked about is that policy was the only way to get those provisions in, and that's not the case.

JOANNA KULESZA: Thank you, Holly, your question or comment?

HOLLY RAICHE: Holly Raiche for the transcript. We recently had, it wasn't a webinar, it was a teleconference with Dave Piscitello who I'm sure a lot of you know or knew, who has done a lot of work in this area. And the comment that he made was you can make a huge difference if you simply outlawed really big bulk registrations. Why don't you do it? Because the only people who want to do the bulk registrations are the ones who actually want to abuse the system. Thank you.

GRAEME BUNTON: This is Graeme. I don't actually think we see all that much bulk registration at Tucows, but boy, that as an absolute statement is really not useful. There are, of course, lots of reasons for people to do some bulk registrations. The most recent one I can think of was a telco in South America that bought a domain for each one of their cell towers, for whatever infrastructure reason, and they were essentially algorithmically generated, which is also another problem or event that people think is universally problematic, and in this case it was a company managing their infrastructure.

DREW BAGLEY: This is Drew for the record. I'm familiar with Dave's work, something I thought was kind of interesting about his proposals in the report was that he actually suggested changes that could be made that would take care of those edge cases of legitimate use, while prohibiting what we all see, which, not to say it's universal, that every registrar sees it, but that what we see on the flip side for the victims is that oftentimes, yeah, there was a bulk registration associated with some sort of campaign going on that's leading the data breaches, or what not, and so I'll let Dave speak for his report himself or someone else read it, but in general, he was basically drawing the dichotomy that maybe there's certain categories of registration such as bulk registrations, where if you're a trusted entity and you go through a process to become approved to do bulk registrations, you can do them, and if not, it's not just enabled by default.

The same thing with domain generation algorithms and what not, and so I think that's consistent with the attributes that the CCT Review team saw that correlated with the systemic levels of abuse and so I know today we're speaking about all sorts of DNS security abuse items, but there's the systemic issues tied to operators with these really high percentages and then there's the types of abuse that are going to happen even at the actors that have robust means for enforcing their own internal compliance and what not, and so that's where I really think part of what needs to be encouraged are means to think creatively about how you can proactively mitigate abuse instead of just dealing with it on the tail end, you know, on a one off domain basis with abuse complaints.

JOANNA KULESZA: Thank you. Drew. We are pretty good on time, we still have half an hour. John, your questions?

JOHN LAPRISE: Thank you Joanna, this is John Laprise for the record, ALAC. I'm heartened by this discussion, but I would encourage everyone to get a move on because this is one of those opportunities to get out in front of legal regulation. ICANN has been steamrolled by both IANA and GDPR and this is just the kind of issue that in a few years, if it's not addressed, we'll see wholesale regulation on, and then we'll be catching up again and we will have another EPDP on DNS abuse of one kind or another that we will have to be doing something about because some country or group of countries has made law about it. So, I encourage everyone to move forward on this with all deliberate speed. Thank you.

JOANNA KULESZA: Thank you, John, I second that, I think that we need to be aware of legal facts that are unfolding around us. Does anyone have a comment of the panelists? Should we just move on back to the audience? Sir, the floor is yours.

SIVASUBRAMANIAN: I'm Sivasubramanian, I'm an ATLAS participant. All the DNS abuse measures seem to be domain name centric. Does it go beyond names and is the abuse measures look at abuse that happens outside the legitimate DNS from the dark web, which is a greater form of abuse, which is the greatest harm.

So maybe I could put it non-technically is to move from name-centric DNS abuse approach to a number-centric DNS abuse approach. So the abuse that happens even without a domain name, even without a legitimate domain name, could also be attended to, must also be attended to. Also the alternate DNS, what about abuse that happens through illegitimate alternate DNS? Or does ICANN think that it is beyond the purview of ICANN look at what is beyond the legitimate DNS? Thank you.

UNKNOWN SPEAKER: So, maybe I'll take a first crack. As a registrar who sells domain names on the DNS, there is literally zero I can do about stuff that does not use the DNS. And I would certainly argue that alternate DNS stuff is precisely outside of the purview of ICANN. It's unregulated and there's nothing that we could actually do there.

DREW BAGLEY: Yeah, that's correct, and the scope with which I've been speaking about has been the CCT Review team, and our mandate was to look at the expansion of the DNS with the introduction of the new gTLD program. So similarly, I'm not speaking about ccTLDs either, in the context of this discussion. Like Graeme said, we're trying to speak about things that are within the realm of ICANN, but even though, from a cybersecurity perspective, even though the so called dark web or just alternative DNSes being used to perpetrate all sorts of things, that's not something that can be solved here.

There's things that can be solved here, and so there's a distinction between I think where some of these things are going to be solved through hosting providers, through ISPs or at a national level versus what we can solve here with unique identifiers or have a healthy debate about it. So I'm not at all surmising we can solve everything here, but those are just two totally different scopes, even though you're absolutely correct, that both can have an effect from a cybersecurity perspective or other illegal things depending on the jurisdiction.

JOANNA KULESZA: Thank you, if I could just ask for clarification, if you could expand on alternative DNS for those people who might not be acquainted with the notion? Thank you

DREW BAGLEY: Oh, sure, this is Drew again, for the record. The dark web in essence is a fancy way of describing a network that is not relying upon the DNS we all know and love, or not relying exclusively even if it relies in part, to resolve identifier. And so oftentimes we think about TOR when we talk about the dark web, but basicallyyou could say alternative DNS for anything in which you're not utilizing the actual DNS and you're connecting computers in some other way.

So that's where you have dark web marketplaces and all sorts of other things, but from a cybersecurity perspective, what we see in terms of the way in which people are impacted by personal data breaches, or by intellectual property theft or anything else, is oftentimes utilizing the DNS, even if cybercrime tools or whatnot are procured on the dark web to begin with, whereas, and I would certainly defer to law enforcement and other sessions to speak to this, whereas what you'll often hear from law enforcement is all sorts of other crime going on through alternative DNS, but again that's outside of the scope certainly of what the CCT looked at, what ICANN is looking at, and what this discussion about DNS abuse is oriented on.

JOANNA KULESZA: Thank you, Drew, that was most helpful. I'm giving the floor back to our moderator, Jonathan.

JONATHAN ZUCK: Thanks, Joanna. I don't know if I need the floor back, I was just going to enter the queue here a little bit. I'd love to drill down a little bit in the conversation that went back and forth, but ended because of the structure of this and one is this that I forgot the name of the guy from GoDaddy, James, yes, sorry. I'm terrible.

UNKNOWN SPEAKER: James, welcome to your first ICANN.

JONATHAN ZUCK: That's the guy. James, when you gave your objections to the CCT recommendations, you said two things that I thought were interesting, one was that you were supportive potentially of Compliance having additional tools to enforce its existing remit, and the second is you were concerned about new sort of prescriptive policies that would take a long time, lots of people would be involved in, et cetera.

Drew had the opportunity to answer that none of the recommendations from the CCT we're in fact prescriptive. One was somewhere about creating incentives for self generated self regulatory moves, such as the ones that you're already currently doing but many aren't. And then the other recommendations were about providing additional tools to Compliance. Those two statements feel incompatible with each other, as I've summarized them.

I hope I haven't misrepresented what either of you said, but I do know the CCT study found domains that had nearly 50% abuse. So, that suggests that whatever is the status quo is not sufficient. So, a document that embodies the status quo and makes it voluntary for those people to comply, whatever tools Compliance have, either they weren't doing their job or didn't have the tools necessary to deal with that problem, because the fact that it exists means the status quo, as it stands today, isn't sufficient.

JAMES BLADEL: If I could respond.

JONATHAN ZUCK: Yes, sir, thank you, James Bladel former head of the GNSO.

JAMES BLADEL: Yes, and it might be my second or third ICANN.

JONATHAN ZUCK: Your hair is a lot shorter than I remember.

JAMES BLADEL: It is, I look very different than when I first got here, I will give you that. So, you went quite a ways down the road but I think you made a wrong turn at Albuquerque, if I could back up. I didn't say that we were in favor of providing compliance with new tools.

To clarify, I was encouraging Compliance and Jamie to enforce and to fully leverage the tools that they already have in the existing agreements and I pointed specifically to a little known bit in the RAA that allows them to take action against registrars for example for illegal activity, that exists today, that's part of the status quo, and I don't want to -- I think you mentioned whether they can't or they don't want to, or something, or maybe it's just a question of I'm just not clear how the community would support an aggressive interpretation of some of those provisions when they encounter such egregious and concentrated abuse in one contracted party.

And I think what we were saying was let's take a look at those provisions. We signed on to those knowing that we were putting our business and our contract at risk if we were bad guys, and we were doing the bad things that we see out there. So let's talk about what the community wants to see in terms of an interpretation by compliance of those. I just wanted to mention that because you said they're incompatible, what I said, and yes, they would be, but I don't believe that I was trying to convey that message that we don't agree that new policy tools are necessary until we've exhausted the tools that we already have.

JONATHAN ZUCK: Just to hold you up for a second, sorry, I wasn't trying to split hairs, I guess, but if you feel like they have the tools that they need now, because there's a provision that says they can go after them, but if they don't have the mechanisms to identify them I don't know what the answer is. It feels like a simpler question when you look at the fact that it exists, and it wasn't taken care of for a long period of time. So, again, I don't want to make this all about compliance, being out of compliance, but if that's the issue then we need to address that issue.

But I think the problem is where this meeting is sort of heading is hey, we're the good guys, we're already doing good stuff, this isn't where the problem is, we're showing you we're documenting what we do, because we'd rather continue a regime of self regulation, rather than having a laborious and process of policy development for external regulation, et cetera, which all makes sense, but somehow in the process of that conversation leaves out the fact that there's a bunch of registries and registrars that are far outside of what would be considered norms in this space, and what can we do about that proactively.

And so that's what I want to get to and have a hardcore conversation about that and I can only echo Alan's statement that it's great what you guys are doing and I appreciate the investments that you're making, and all your customers are benefiting from it and users are benefiting from it. What do we do about the rest that makes you less nervous about what the unintended consequences of that might be, et cetera. How do we get to dealing with the folks that aren't the good actors? That's the question I'm trying to ask.

JAMES BLADEL: And I just leave it with, you know, I think that we need to stand up and help Jamie and his organization. I don't think it's an awareness problem, necessarily. I think that maybe it was in the past, but I think that's changed quite a bit with tools like DAAR, you know, there's a detection grid now. He's operating under a different set of pressures I think that we don't always see. One truism of ICANN is every problem looks simple from the outside.

So, we need to encourage them to take a look at the contracts as they exist today and look at aggressive enforcement when those egregious cases are encountered like that. Because I think the tools exist, and I don't know, Jamie, if you want to respond, whether you think those tools are inefficient or inadequate, but we think that you have some hammers you could hit people if you felt that you had the backing of the community to do so.

JONATHAN ZUCK: Jamie, Drew, I'd love to hear from both you guys.

JAMIE HEDLUND: Yes, so just quickly, yes, there are great tools and there are tools that have raised awareness. I would say that DAAR is more efficient and effective for the registry space than the registrar space at this point. I know there's a lot of work going into fixing that.

One thing that became clear from the registry audit on DNS abuse is the vast, vast majority of registries not only comply with Spec 11-3B, but they do a whole lot more to mitigate DNS security threats and we will continue to work with registries and registrars on enforcement and look for their creative ideas on how we can better leverage the tools that we have, also look forward to seeing where the discussions go in the community and if there are changes either through policy or through contractual negotiations, ICANN compliance will enforce those.

DREW BAGLEY: This is Drew for the record. On the CCT Review team, what we saw was that the existing provisions were inadequate to deal with what the data showed, but we also recognized the innovation going on in the community by contracted parties to do good things, and so that's why we wanted to build in incentives and we suggested that they could be perhaps financial incentives so like a fee reduction or something for operators adopting certain proactive anti-abuse policies, but I think that the encouragement of proactive versus reactive was really important and we saw that absent from the current contracts, a structure to encourage that, and yet we saw that as being necessary for what we were seeing with the data, and then also a means to deal with the systemic abuse.

So one of the examples that we highlight is for example, where you had one of the operators I mentioned earlier, alt names associated and I don't recall off the top I had the exact number, but associated with half of their registrations or maybe more being abusive, nonetheless, because you had a reactive model, you are having to depend on complaints to be filed for each domain name when there was this clear systemic issue and it took nearly a year for ICANN Compliance to be able to do anything against alt names, and in the end it was because they didn't pay their bills that they got in trouble, it wasn't because they were facilitating this sort of DNS abuse.

And so I think that really illustrates that, and I know you were citing the provision about illegality, but I don't think that's sufficient for dealing with these types of things. But again, something that I do not think at all is incompatible with what you're speaking about is the fact that the CCT Review team recommendations were purposefully not overly prescriptive in the means by which certain things are done and similarly, we're not even overly prescriptive in what thresholds should be, and even with the suggested thresholds, there are thresholds that from what we saw with the data the entity showing up at ICANN meetings would not have to worry about.

So, I think if anything, the contracted parties here would actually probably find positive if all the recommendations were adopted because the asked for incentives for good behavior and then probably would not be affected by the provisions that would give ICANN Compliance more tools for that systemic abuse.

JONATHAN ZUCK: Greg Shatan.

GREG SHATAN: Thanks, Greg Shatan for the record. I agree with others who said that this is a good first step, and indeed I think the circle ID article identifies it as a first step although I think I can recall some previous steps, but maybe this is a good first step or the first good step, not sure exactly which. In any case, I am concerned, though, that it may be doesn't go far enough and that there is kind of a ring fence around certain very technical types of domain name abuse or really DNS abuse but not domain name abuse and that there are some things especially that may be more a concern to end users and that may even feed back into some of the types of things that you identify within the ring fence.

For instance, domain names that are somehow, you know, they may be trademark infringement, they may just be in some way, create an impression with consumers that are then intended to deliver malware, it's not necessarily spam, but it's something else that's kind of using the domain name in order to falsely gain trust and then create an issue similarly with phishing, spear phishing and the like, they're often now linked to other types of abuse that have been in the discussion about abuse within ICANN but they're not in this list and I know you identified four that were particularly egregious things, See Sam, opioid abuse and a couple credible threats to violence and there was one other really, really bad thing. But I'm concerned about kind of what has ended up outside the fence. I'm wondering what your what your thoughts on that are. Thanks.

GRAEME BUNTON: This is Graeme for the transcript. So, since we published that framework, I have had people tell me it went way too far and they're outraged and I've had people tell me that it didn't go nearly far enough, and they're outraged, which means to me I think in classic ICANN fashion, we got it pretty right. If no one is happy, we did a pretty good job. I think what I heard from you, Greg, and we've chatted about this before, was there's that very narrow remit set of issues that are content issues that are not DNS abuse, not more stuff particularly issues related to intellectual property, because we don't think it is appropriate to deal with those issues at the DNS level and that's not an accident that they were not in there.

However, if you are bringing to the table an abuse complaint to us that has some linkage between an intellectual property issue and one of the types of DNS abuse that we mentioned, then everybody gets a win. And so I would look at it that way. But it's very clear and deliberate that intellectual properties are outside of that framework.

JOANNA KULESZA: We have one more question from the lady who's been waiting on the mic, and then I have Tijani and Olivier. So that's our queue, we have 12 minutes. Thank you.

KATE PEARCE: Hi, Kate Pearce, Council of Internet New Zealand, head of security at one of New Zealand's large companies, but I'm speaking in my personal capacity. What I would encourage you to do, should you go down the regulation path, is to not just require that something be done, but to measure the time to response. I work in security, I do not care if you fix it two weeks from now, you may as well fix it five years from now, there are things that need to be done within minutes, and that is something that any process which is heavy on the jurisprudence will not be able to respond to.

That will leave hundreds of millions of people at risk of all sorts of things. So yes, we have to balance it, yes, we have to do a good process, but particularly with a new domain name If it's only been around a matter of minutes, that's a very different thing to something that's been around for decades. We'll always get concentrations of badness, but there are registries that people don't bother reporting. A lot of the stuff we're talking about, audit and enforcement, already happens outside of ICANN.

The entire security industry, there are shadow DNS filters, there are whole countries that have DNS firewalls to fix weaknesses in the space, but for whatever reason the regulation or the market is not solving. That might be where we want it, but I tell you, a lot of small end users do not have access to those tools that large enterprises do, we cannot forget that. For many small people, for many individual users of the internet, your regulation may be all that protects them.

JOANNA KULESZA: Thank you, do we have feedback from the panelists? Taken on board, that was an interesting comment, thank you. Tijani and then Olivier Crepin-Leblond. Tijani the floor is yours.

TIJANI BEN JEMAA: No, thank you, Mr. Moderator.

JOANNA KULESZA: Alright, so Olivier.

OLIVIER CREPIN-LEBLOND: Thank you Madam Chair, Olivier Crepin-Leblond speaking. I'm going to echo the words of what my friend and colleague, Alan Greenberg, said a bit earlier, regarding the fact that we do seem to have an alignment of the planets and an amount of collaboration that we've not seen so far when it comes down to having both registrar, registries, end users and others at ICANN. The concern I'd like to emit is regarding the ICANN Compliance department. What I've heard today mirrors very much what I heard a few years ago.

I've looked at the reports of the ICANN Compliance department and yes 99% of the action that is being taken is regarding nonpayment of fees, and a few years ago it was exactly the same thing. So it looks as though many have actually moved forward and I absolutely commend the registrars and registries, and the contracted parties that have signed this letter, the document that we were talking about earlier. But compliance doesn't seem to have moved much.

Now, either It doesn't have the tools to do other things than just enforce the fees, in which case we're in a situation where Al Capone can kill, do all sorts of business, but then can only be caught by not paying his taxes and of course we know that today such activity can actually be somehow prosecuted in different ways than just going after someone's taxes, because law has evolved and there are laws now regarding this type of thing.

I think ICANN Compliance needs to evolve and it needs to actually look at the tools that it actually has, rather than just use the easy tools, the easy way to go forward, which is to wait until someone doesn't pay their fees and then you just tick the box and say, ah, we've made enforcements this quarter, and all by just saying they haven't paid their fees, the easy ones. You have to go after the tougher ones, and I'm just concerned that we're not seeing any movement on this. So I hope that you'd be able to do that. And Jamie, I know you've inherited a situation in Compliance, but it's been going on for quite some time and at the moment I'm not seeing that determined will to change things.

JAMES BLADEL: This is James from GoDaddy again, and I just actually wanted to commend Jamie and his team for finding a way to get the bad guys, I don't care how or what provision, that's inside baseball stuff, and I was going to raise the Al Capone issue as well. They put them away for tax evasion, fine, he's still behind bars, not doing his criminal stuff. And so I think it's an example of, and eventually dead, thank you. Last I checked.

So, I don’t think that's a problem, I don't think that's a bug, I think it's a feature. I think it shows that compliance is aggressively pursuing every possible dimension of noncompliance or bad behavior. If someone's not answering your calls when you point out that 50% of their zone is junk and spam and phishing, they're also not answering your calls when it's time to pay the bill. So, I don't think it's a problem, think I commend him for it.,

JAMES BLADEL: Thanks, James, if I could just quickly answer, so Olivier, I take your point and we are always open to constructive suggestions on how we can do our job better. I think you have a skewed view of what we do based on what's published and what's published are the things that go to breach, and a lot of things that go to breach are payment and recently they've been a lot of registries from the new gTLD program and a handful of registrars. We handle between 40,000 and 50,000 complaints a year, a very small percentage of the total is payment issues. Could we do a better job? Absolutely. And we look forward to your

suggestions and the suggestions of ALAC on how we can do it. Thanks.

KJOANNA KULESZA: Thank you, we have Alan and then I'm going to give it back to Jonathan to summarize. Alan?

ALAN GREENBERG: I'm just going to follow up on those previous comments, I think it's great that if you can get a bad registrar or registry on payment, it's very hard for them to dispute that. But we need to be able to get the ones who actually are stupid enough or smart enough to pay their bills.

JONATHAN ZUCK: Joanna asked me to summarize, I don't know if I'm prepared to do that. This is obviously an issue, it's an emotional issue in many respects, and it's also people's businesses that are at stake here and everything and so we want to find the right balance. But I think this is something that there's a consensus in the At-Large that we want to take more seriously in get engaged in a more specific way, so expect to hear more from us, both aimed at compliance and at the Board with respect to the best ways to move forward and mitigate this.

None of this is a lack of appreciation for what any of you are doing It's really about the identification of problems and trying to figure out the most equitable way to deal with them, because as I said at the outset, we're tasked an enviable responsibility of trying to think about four-and-a-half billion users that are just using the internet and they're not interacting with ICANN, they're not interacting with registries or registrars in any way, they are just, getting on and trying to make dinner reservations, and so how do we address their needs and what is within ICANNs remit to do that, and that's our daily struggle.

So I want to ask you all to join me in thanking these folks for showing up for the firing squad for this conversation that we're just getting started, but there's a lot more to come. So, Drew Bagley, Jamie Hedlund, Graeme Bunton and James, and the audience, thank you so much for standing up, and Andrei, as well, who is part of At-Large and part of SSAC. Thanks so much, guys.

[END OF TRANSCRIPTION]