DEVAN REED: Good morning, good afternoon, good evening to everyone. Welcome to the At-Large policy session two, tackling DNS abuse, on Tuesday the 19th of October 2021 at 17:00 UTC. In order to save time, we will not be doing a roll call today. However, attendance will be noted from the Zoom room as well as the audio bridge.

We have Spanish and French interpretation on today's call. If you need a dial out to the Spanish or French lines, please send a direct message to staff with your preferred language and phone number. Before we begin, I would like to remind everyone to please state your name when taking the floor each and every time and to please speak at a reasonable pace for accurate interpretation and to please keep your microphones muted when not speaking to prevent any background noise. Thank you very much, and with this, I'll turn the call over to you, Joanna.

JOANNA KULESZA: Thank you very much, Devan. And again, thank you, everyone, for joining us. Particular thanks to our speakers who have agreed to meet around the topic of DNS abuse, which was we know has proven to be a very important and at the same time, at times contentious around the ICANN community. We view the session as a consensus building exercise, just a way for us to catch up on what particular constituencies have been doing with regards to the DNS abuse topic. Thus far, not a policy development process, but we have seen DNS abuse come up in various narratives around the community.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

The background for this session is us to conclude with a clear understanding of DNS abuse, one that is not contended, one that we can, so to speak, present to the world. The reason why the At-Large proposed this session as a possible plenary during ICANN 72 was because we seem to look at the same problems around security, cybercrime, abuse of the domain name system, from sometimes different perspectives. And I am thrilled to say that today, we have been successful in inviting members of different constituencies ready to give us some insights into what they have been doing with regards to what we within ICANN like to refer to as DNS abuse and hopefully allow room for discussion of those who have joined us here today to exchange ideas and views on whether the framing we have for DNS abuse right now is ready to be exported outside the ICANN community or whether there are issues we might want to address and discuss.

Now, with this in mind, let me introduce our speakers. We have agreed on a specific intended speaking order. That would be the next slide. I will start us off with an introduction of our speakers, and that will give me a chance to show you where this session started, why we have the speakers we have and what is the intended purpose of the 90 minutes we have reserved for this session today.

We will start off with Graeme Bunton, who is leading the dedicated institute for DNS abuse with a thorough background in managing the topic on the technical side. Graeme will start us off today with giving the broad perspective on DNS abuse.

Here within the community, we have at times looked with some concern at the definition of DNS abuse, and Graeme has kindly agreed to start us off with an introduction into the topic for those of you who might be new to the DNS abuse debate.

Then we will look at the issue of DNS abuse from the registry perspective with Brian Cimbolic kindly agreeing to speak on behalf of the PIR. Brian is the vice president and general counsel with the Public Internet Registry. So we will try to see how the—as already noted somewhat ambiguous—DNS abuse policy is enacted in practice, in real-life circumstances.

Then we are thrilled to be joined by James Bladel, who's the VP for global policy at GoDaddy. So we are looking into the registrar community trying to understand what are the challenges that that community might be facing currently with regards to DNS abuse.

Now, we this contracted parties perspective, we will try to move into the end user narrative. Again, we are lucky to be joined today by Lori Schulman who is the IPC president elect, also acting as the senior director for Internet policy within the International Trademark Association. So we will have an intellectual property perspective on DNS abuse. I'm very much looking forward to Lori discussing the scope or the practical application of the policies we have in place.

And last, but by no means least, we are thrilled to join our colleauges from the Governmental Advisory Committee, today represented by a good friend of the At-Large, Nigel Hickson, who will discuss or briefly introduce the discussion within the GAC on DNS abuse. The ALAC and the GAC do have a history of working together on various policy-related topics, and revealing a little bit of the agenda for ICANN 72, let me note that both the ALAC and the GAC have put DNS abuse high on their agenda.

We will be discussing this in a joint meeting, but we within At-Large thought it would be tremendously useful to share the GAC perspective with regards to potential regulation of whatever we within ICANN understand as DNS abuse.

The first interventions therefore will focus more on contracts and Contractual Compliance, the way it impacts individual end users, but hopefully, Nigel will shed some light on what the governments will have in store with regards to what we view as voluntary bottom-up DNS abuse-related policies.

We have reserved relatively little time for our introductory remarks from the speakers, and this is primarily because we want to keep this as close to a roundtable format as possible. We are not able to meet face-to-face, we're losing a lot of the added component of an ICANN meeting, so we have decided against introducing slides, presentations, anything that comes close to preaching about DNS policy. We want this to be a friendly exchange of ideas, hopefully giving us a thorough understanding of the peculiarities of DNS abuse-related policies, making us ready to present that discussion to the outside community.

Now, I have the opportunity to act within the ALAC, within the At-Large, as the vice chair for capacity building. I view these discussions primarily as a capacity building exercise. We want to make sure that end users know what is happening with regards to them being protected from malicious activity online. But I am thrilled to be joined today by both of our Consolidated Policy Working Group co-chairs, Jonathan Zuck and Olivier Crépin-Leblond. Thank you, gentlemen, for taking the time to join us and make sure that the discussion stays on track with regards to issues relevant for ICANN policy development.

With that, after these initial presentations from our speakers, I will hand the floor over to Jonathan to take us through the Q&A. You are more than welcome to pose your questions and comments in the chat, you are more than welcome to raise your hands, and Jonathan will skillfully navigate us through these discussions. And hopefully, almost when our 90 minutes are done, we will then be ready to hand the floor to Olivier who will summarize and produce a comprehensive on DNS abuse, making us ready to present it to the outside world.

That is the idea we've had for that session. You could call me idealistic, but I think that that is an achievable goal. And with this in mind, I'm happy to hand the floor over to Graeme Bunton. [inaudible] ready to take the floor. If you could start us off with DNS abuse, giving us a little bit of insight. You have been gracious with your time and very kind to make sure that you join our At-Large discussions around DNS abuse. Thank you for accepting the invitation once again. If you would be willing to take the floor and give us a brief recap of the most recent work that the DNS Abuse Institute has done, we would be most thrilled. Graeme, with that, the floor is yours. Thank you very much.

GRAEME BUNTON: Thank you, Joanna. Thank you to the ALAC for inviting me today. I appreciate that robust and thorough intro. I appreciate being able to go first here, I can give some broad context for DNS abuse and talk about what the institute is doing at the same time, and hopefully this'll be interesting for everybody.

Let's start with the definition of DNS abuse. This is a topic that comes up a lot, and I find a little bit almost boring at this point. But I think we really need to set some expectations for what we're talking about here.

DNS abuse as defined by the Contracted Parties House, drawing on a number of different sources from within and without the ICANN community, is malware, botnets, pharming, phishing and spam where it's a vehicle for those preceding four harms. It's a relatively simple list, it's pretty constrained, and that is useful when we're having discussions about DNS abuse. The institute that I run, the DNS Abuse Institute, recently set up as an initiative from PIR, has adopted that definition as well.

Without going into the details on this too much, I will say there are other opinions on this, there are some weaknesses in the existing definition, it's quite categorical, what do you do with new harms, pharming as a harm is really a DNS poisoning attack with a phish and there's absolutely nothing a registry or registrar could do about local DNS poisoning, and we already have captured phishing so I'm not sure it's even appropriate to be there.

A more sophisticated approach to this problem is maybe worthwhile, and I have a very long think piece on this on CircleID that I'll find the link and put in the chat, that proposes a new way of coming at this, but really and practically and for driving conversation forwards, this definition is going to capture really most of what we're talking about here, and really the places where we need coordinated, concerted action.

We can talk about lots of stuff on the margins at some point. But my general perspective is with this sort of categorical definition, we've got lots of work in front of us that we need to tackle, and it's important that we do so.

So that's what we're talking about. Where is it, how much of it and where is it happening? The unfortunate answer to this is that there really is no useful, transparent, robust set of data or analysis on DNS abuse. ICANN has produced the domain abuse activity reports, DAAR. You can go read them. They give you a pretty general sense of abuse, but they're really not helpful for understanding what registrars or TLDs abuse is happening.

The community has a tendency to talk in anecdotes. And this is kind of a real problem because we want to be able to identify where abuse is happening because that helps us inform what we need to do about it and what solutions are going to be appropriate. I will say that this is something that the DNS Abuse Institute is working on. We're looking at developing our intelligence platform so that we can really dig into the problem and find out at which registrars and registries DNS abuse is a problem, but also conversely, which registries and registrars are doing excellent jobs on this that we should be celebrating.

And part of that is really understanding that there is a difference between malicious registrations and compromised websites that are engaged in DNS abuse. It means understanding not just existence of abuse but persistence of abuse so that you can understand how quickly registries and registrars are acting on abuse. It’s ensuring that what you're calling abuse is actually actionable in the first place, that it’s evidenced.

And that points to another important thing to understand, is that most of the data around DNS abuse comes from what's called RBLs, reputation block lists. These are produced by security companies, primarily for the role of network protection. So people subscribe to these lists to prevent e-mails or network activity going to these abusive domains.

The problem with that is that that's not produced for mitigation. The risk profiles for protecting your network versus taking down a domain name are very different and the evidence requirements for those things are very different. So the primary tool we have to understand DNS abuse isn't really created for the purpose in which we’re using it. This is really creating a gap.

We’re going to have to spend, I think, as a community some time—or at least as an institute I need to spend some time on really understanding the RBLs, where the data on abuse comes from and how we can actually make that more useful for registries and registrars. And I'll come to that in a sec.

But broadly speaking, just so everybody has a sense of what we’re talking about, if you look at the latest DAAR report, they capture about 210 million generic TLD domain names in their report. They have inside of that about a million they flag as abusive, and 80 to 90% of that is spam. So that leaves you somewhere between 100,000 and 200,000 domain names out there in the world that are engaged in harm in some fashion. That does not distinguish between malicious and compromised.

So the good news is, as a relative measure, boy, that 100,000 on 210 million is very small. The bad news is that counting domain names is a really terrible way of understanding actual harms. You know, a single domain name engaged in a really aggressive phishing or malware distribution campaign can really damage a lot of people and businesses in ways that are very real. And so we need to make sure that as we're looking to understand that data, we pull ourselves back up a little bit and look at this problem a little bit more holistically sometimes.

So let's understand—And I recognize, I'll try and keep this relatively brief, we need to understand the context in which DNS abuse is happening across the registrar and registry ecosystem, the DNS ecosystem. The economic context here is that it's a globally competitive business, that registrars, no matter where they're located, are competing for customers around the world, in a very high volume, low margin business, often making somewhere between 25 cents and a dollar per name per year.

And most registrars really don't make the majority of their money selling domain names, it tends to be an add on to their existing hosting business, often other web services, for small businesses and such. And so when we think of registrars selling domain names and making lots of money, that's often not true. And it's often just not the core of what their business is, it's not something they're paying a lot of their attention to.

And that leads us to what I would call or an economist might call a collective action problem, where there is something that's impacting everybody, but there's a number of disincentives towards acting collectively. And this is to a certain extent where the DNS Abuse Institute is stepping in where we can see this collective action problem. And through the generosity of PIR, we're able to step forward and say, okay, we're gonna go and do the work that we think is going to help make this ecosystem better, and essentially absorb some of the costs that would help the entire ecosystem and put forth some education, some tools, some resources, and try and make a difference on DNS abuse.

And so lastly is, what can someone actually do about abuse at registrars and registries? Well, there's two sort of broad approaches. One is preventative, which is you're trying to prevent abusive domains from being registered in the first place. And so you are trying to identify the attributes of a malicious registration and either prevent that from completing or preventing that domain from resolving. And so that could be like, “Oh, this has PayPal in it. Let's put it into a queue for manual review,” some sort of process like that.

The other side is reactive, which is where the domain has been registered, it becomes engaged in abuse and you get it reported from somewhere else. And you then investigate and respond, and typically that would mean preventing the domain from resolving anymore. Longer term, of course, preventative is better than reactive, you want to prevent those harms from happening. But given the economic context we were just sort of talking about, that requires a registry or registrar to write code to build friction into the registration systems. And that's a big ask.

Lots of registers have these long, elaborate backlogs of work they need to do to keep up with the changing regulatory environments, commercial demands, things like that. And so I think there's a lot of room around improving reactive responses. This means improving the process to report abuse to registries and registrars, which is currently unstandardized and a mess. And it means things like better education so that people can understand how to keep their websites and domain safe, it means registrars and registries are going to have a better set of best practices on what to do. And so we're definitely working on that educational piece at the institute.

But the most important thing, I think, that we're working on right now that I'm pretty excited to talk about a lot is we're building—the website will be differently titled at some point, but what we call a centralized abuse reporting tool. And this is going to be a single website where anyone could go and report abuse to any registry or registrar. And so you won't even need to do that lookup, you'll be able to put in a domain name, it will know what the proper registrar is for that. If you think it's a phish or a malware, it's going to collect the required evidence, and then will send that along to the registry or registrar.

And so that cleans up for the end user, the person who's found abuse and is trying to report it, it makes that process a lot easier. For registries and registrars, they're currently getting garbage abuse reports that are really messy, unevidenced unactionable, often duplicative, and we're able to clean that up for them too. So registries and registrars will get a bunch of value from this, people reporting abuse will find that process much easier. And hopefully, that begins to reduce a lot of the pain around reactive abuse mitigation efforts. And so I'm pretty excited about the prospects of that and hope to have something launched on this, I'm going to be going out on a limb, it's probably going to be Q1-Q2 next year. And you will be certain to hear about it, I'll be talking about it everywhere I possibly can.

But hopefully that gives everyone a pretty good overview of what DNS abuse is, what we understand about it, which is unfortunately very little right now, what the economic context is for abuse inside of registries and registrars, and the methods of mitigation. And I'll stop there and pass it over, I think back to Joanna, thank you for the time. Sorry if I went long.

JOANNA KULESZA: Thank you very much, Graeme. That was very useful, insightful, and very precise. So thank you very much for that intro. I know that you have worked with Brian very closely previously, and I am certain that Brian Cimbolic will be able and willing to complement that comprehensive introduction with a more specific narrative around the activities that are taken by PIR to make sure that we remain DNS abuse safe. So with that swifter turnover, I give the floor to Brian, if you would be willing to take us further. Thank you.

BRIAN CIMBOLIC: Of course. Thanks, Joanna. Thanks so much to the ALAC for having me here. I'm Brian Cimbolic, General Counsel at Public Interest Registry. And I am going to actually wear two different hats here and I'll tell you when I'm switching. I am a co-chair of the Registries Stakeholder Group abuse working group. And there's a counterpart in the Registrar Stakeholder Group, they have their own abuse working group too. But together we also sort of form a collective Contracted Parties House abuse working group. And so my co-chairs that are Jim Galvin of Donuts, Reg Levy of Tucows and Luc Seufer. And I apologize. Sir Graeme can put in the chat which registrar Luc is.

But our abuse working groups over the last few, actually, more than a year now have really sort of put our nose to the grindstone and tried to develop a number of practices to help inform registries and registrars how to deal with abuse. But as well as sort of address the concerns of our friends across the various aisles.

And so we've conducted some outreach. We've met with every constituency there is out there now from our abuse groups, and have developed a number of practices specifically aimed to address those concerns that have been raised.

For example, after conversation with the GAC Public Safety Working Group, the registry abuse group co-drafted a document with the Public Safety Working Group aimed to address problems associated with domain generating algorithms that are associated with malware and botnets. So these are algorithms that would register 10s tens of thousands of domain names. Registries have to register thousands of domain names to really properly address the threat that's associated with that. So it's a relatively complicated area that we thought it was important that registries get educated on it and that law enforcement as well get educated on the constraints on the registry side. So we jointly drafted that document together.

The CPH, just in the last week or so has developed and published a trusted notifier framework. And so what that is is a document that educates registries and registrars but as well as those organizations that want to serve as a trusted notifier sort of walk through the tenets, what are the foundational elements of a trusted notify relationship? I'll put all of these links in the in the chat when I'm done, but just wanted to sort of speak to some of the work.

There's also some, the registrars have led and have already published a guide to abuse reporting. So what goes into a helpful abuse report, what makes something more actionable, that's actually—we're updating that, we're in the process of updating that now, it should be out soon and have a more contracted party house view. So it also includes registries.

Finally, there's some ongoing work focused on IDN homoglyph attacks, the registrars are putting out a paper on BEC scams. And they are also finalizing a document on registrant appeals when a domain is taken down for abuse.

So that's sort of just a high level some of the ongoing work from the CPH abuse working groups. And I would invite you next Monday, at ICANN 72, we have an outreach session. Please come let us know what your concerns are, what other areas you'd like to see us work in. So hope to see you there.

The second hat is I'm, as I said, General Counsel at Public Interest Registry, and part of what my responsibilities are is overseeing our anti abuse program. And so our anti abuse program is really focused or built upon what we call our anti abuse principles that I’ll also in the chat. Those are sort of our cornerstone thoughts around abuse, and it's built around principles like transparency, commitment to due process, and recognizing sort of the balance between the scale of harms involved with the harms of DNS abuse and the potential collateral damage of taking action at the registry level.

And so out of that, those principles, you see why PIR, we're sort of unique in the gTLD world, we regularly update, typically once a month, our abuse numbers so we publish all the abuse that we've seen, what actions were taken, the frequency of things, predominantly DNS abuse, but we also publish what court orders we've seen and the instances of child sexual abuse materials and how we ultimately mitigated those.

We also have published a registrant appeals process so that if we take action on a domain name that a registrant thinks it was done in error or in violation of our policy, they can challenge that decision to a neutral third party. But really the core of it is what Graeme was describing, is the proactive and reactive steps and dealing with DNS.

So reactive, we have all the, we'd like to think pretty industry leading reactive measures, and that all .org new creates are checked against a number of reputation block lists. And as Graeme mentioned, that's not definitive, necessarily, but it gives us a good reason to look into a domain, as well as regular sweeps of all .org registrations against those same lists. And so that sort of belt and suspenders approach typically is good at catching newly created malicious registrations, but then that sweep also helps identify potentially compromised domains or domains that aged a bit before engaging in DNS abuse. So that's sort of on the reactive side.

On the proactive side, PIR has developed what we are calling quality performance index, QPI. This might be something you've seen me or [inaudible], one of my colleagues, speak to. What QPI is is it's a registrar incentive program where we use six criteria, including abuse rating, so what we observe a registrar's abuse rate relative to its new creates, domain usage, renewal rates, a handful of other things to essentially give a scorecard to a registrar. And if the registrar falls below a certain score, then it doesn't qualify for any discounts.

However, if it has healthy registration patterns, it can qualify up to a modest discount. The idea behind this program is to create responsible growth and we know that deep discounting is sort of almost an invitation to DNS abuse in certain instances. So we try to be very thoughtful about the way that we incentivize our registrar channel.

And so of those six factors, only one of them is a gating mechanism. The registrar can have great domain usage, renewal rates, those kinds of things. But if it fails our test that we set forth for abuse rates, it is automatically disqualified from QPI.

And so QPI, it's been very successful for us, we've seen really a number of registrars fundamentally change the way their abuse registration patterns in .org where in order to qualify for this financial incentive, they dramatically decreased their abuse that that we see in .org for them. And so it's both that carrot and a stick. It's a carrot in that it rewards registrars for performing well and having low abuse and being responsive on abuse.

But it's a stick at the same time because those registrars that don't qualify know that they're at a competitive disadvantage and so are incentivized to then come to the table and get better abuse. And we've really seen that happen, where several registrars really changed the way that sell .org in order to qualify. And so we're very proud of this program.

Also, if you go to www.qpi.org, sort of an open invitation for other registries to participate. We're happy to sit down with any other registry and talk about developing their own QPI program. PIR, we're nonprofit, we're doing this because we think it's good for the entire DNS. And we've also seen that it's been good business practice, not just for us, but for the registrars. So we've seen participating registrars in this program have seen a 4% improvement in renewal rates, which is significant. It might not sound like much, but when you're talking about the way that Graeme described, the state of the industry, it's sort of thin margins and 4% increase in renewal rates is significant. So it's been good business, we've seen it, our abuse rates overall decrease, and we've seen real improvement in registrars. And I think that these sorts of proactive approaches, as Graeme mentioned, might be a way to obviate the need for heavy handed reactive approaches in the end. If you can create an environment, foster an environment that's going to have low abuse on the front end, then it's less work on the back end. Happy to take any questions once all the other panelists are done. Thanks.

JOANNA KULESZA: Thank you very much, Brian. That is a very insightful, very pragmatic—I always appreciate a pragmatic approach. I love the fact that you've emphasized how voluntary this entire program is. We did have a roundtable within EURALO emphasizing the impact that this voluntary approach might have, should the European Commission proceed with the legislation that is now being discussed. But we will get to that, hopefully, somewhere around Nigel's intervention with regard to the GAC position and the GAC concerns.

Speaking of voluntary measures from registries, let me also welcome again James Bladel who's the vice president at GoDaddy for global policy. He has kindly agreed to share the GoDaddy, the registrar, perspective on how DNS abuse is being handled. Without any further ado, James, the floor is yours. Thank you.

JAMES BLADEL: Thank you, and good morning, and good day. Very grateful for your invitation to come and speak today. And also grateful to my colleagues, Brian and Graeme for kind of setting the stage a little bit and taking a lot of the introductory work. It allows me to dive in a little bit more substantively.

First off, I wanted to circle back to something that was mentioned in the introductory remarks, that this is a contentious topic or the topic of DNS abuse is controversial. I have a different view. I think that this is a complex topic. And it's a recognition that the subject of DNS abuse does not have a single source, does not have a single party or segment of the industry that is able to control it or able to stop it. It requires a broad effort on the part of a lot of different industry players, and that's one of the reasons why I think organizations like the Domain Name Abuse Institute are important in helping to coordinate all those moving pieces so that we can bring a comprehensive effort against DNS abuse.

And as Graeme mentioned, no contracted party, registry or registrar, is welcoming of abuse. In my view, in my experience, the margins are so thin that a lot of industry players are either not aware of abuse, or simply lack the capabilities to effectively address it on their platforms. And it's only some of the larger companies that are able to make the necessary investments in people and the tools and technologies to address the problem. And even from our perspective, we sometimes feel like we're chasing the different evolutions of the problem. But I think that, just agreeing with my previous colleagues that this requires an industry wide approach.

I wanted to mention, it's kind of a common statement and something that we come back to a lot, but it's really important for us to spend the time and do the initial work to adequately define the terms of DNS abuse. I think the framework that was put together by various contracted parties, the framework on DNS abuse, starts this effort. I know the DNS Abuse Institute picks that up and runs with it a little bit.

But I think it's incredibly important for us as a community to have a shared understanding of what the problem is and which aspects of the problem can and cannot be addressed via potential policy changes or industry best practices or different coordinated tools like reputational lists.

And I say that because I have sometimes—and this is anecdotally, but I have sometimes heard a lot of different things thrown under the umbrella of DNS abuse, and some of which include, for example, disputes, economic disputes, or complaints about the veracity of information that's associated on a website or misinformation, lots and lots of different problems on the Internet are sometimes captured under that umbrella of DNS abuse. And I, like many of you, I think, having come through some of the traumatic experiences of the EPDP that is associated with WHOIS and privacy, know that it's really important to get consensus on the definition of the problem before we charge off in an attempt to solve it.

I also want to point out that although GoDaddy is an integrated company, we are a registry, we're also a domain name registrar, and we have strict institutional controls to separate those two businesses, we have determined that there is value to cooperation on DNS abuse. So that is one of the few areas where we do coordinate registry and registrar internally. And it has also I think, at least from our perspective, highlighted some of the distinctions between the two roles of what is the registry’s role in addressing domain name abuse versus what is a registrar’s role.

And a registrar’s role in particular, I think, this is the frontlines of DNS abuse. This is where the domain names are registered. This is usually the first place that abuse report is filed, and registrars have to make the necessary investments to both capture and investigate and mitigate those reports almost entirely as in a reactive fashion, as Graeme and Brian noted, because of the challenges of addressing these things proactively.

In terms of an abuse queue, I think that we have seen some statistics where 90% of the reports that are submitted to registrars are unactionable. Either they lack evidence or they're duplicative. We see things like social media campaigns to report a particular website where we can receive thousands of identical reports on a particular domain name or website. If it's actionable, or if it's not actionable, that's a lot of noise that's drowning out the signal in our abuse teams.

The registry has a role as well. And I think, as Brian noted, it has a little bit more of a perspective of abuse that's occurring across registrars but within the same TLD. But I do think that because the registry doesn't have a contractual relationship with the end user, its focus is correctly on the managing the abuse performances of the registrars. And that's why I'm very encouraged by the actions taken by PIR to help align those incentives by their QPIs and their different discount qualification programs for registrars that do take those extra steps and do incur those additional costs to address the problem of DNS abuse.

And then of course, the Domain Name Abuse Institute plays a vital role in standardizing the reports and then helping to filter out some of those superfluous reports and then ensuring that there is some evidentiary standard in what's submitted on to the registrars. And those things, of course, then start to look very similar to that of a trusted notifier in that we understand that reports coming out of an experienced and regimented organization like that will have a higher quality score when they're presented to our teams.

But aside from that, I think, I look forward to questions. I think that it's very clear that this is a very distributed problem, and it requires a coordinated solution. The economic incentives, as Brian mentioned, are often misaligned, and we can work together as a community to help those contracted parties that have the right intentions to address their share of the problem but perhaps either lack the awareness or the capabilities to do so. And certainly would welcome any questions in that regard. So thanks again for the invitation. And I look forward to the other speakers. Thanks.

JOANNA KULESZA: Thank you very much, James, this is much appreciated. As already said, we are trying to identify the core of DNS abuse for us to be able to advance the discussions as we have had them. Thank you to Lori—switching swiftly to our next speaker—for joining us here today. Lori has kindly agreed to speak on behalf of the IPC. But there is an end user angle that I know Lori will highlight in her intervention. And so all of these presentations focus on the contractual obligations that are resulting from the ICANN contract, but also voluntary measures, as our speakers have highlighted, that come in a relatively bottom-up process and impact the way that we keep the network safe.

For that unique end user perspective from the IPC, I hand the floor over to Lori, whereas I am keeping in mind, we will also discuss the possible regulatory approaches to DNS abuse, with Nigel being our next speaker. So in this middle ground, Lori, I hand the floor over to you. Very much looking forward to your intervention. Thank you again for accepting our invite.

LORI SCHULMAN: Thank you very much. And thank you to my colleagues on the panel and to all of those who dialed in from the ALAC and the IPC and the other constituencies that I see inside the roster. Having 111 participants in the middle of prep week in the AGM I think is remarkable, and it shows the importance of this issue to the community.

And where James and I completely agree that this is an extremely complex topic, there is no surefire, simple answer. Had there been, we would have figured it out 20 years ago. So here we are today, in a world that in some ways is exactly the same in terms of the DNS works as the DNS does, but in fact, is quite different.

We have more Internet users, we have more people concerned about online safety, the issues that we're seeing exploding in all areas of regulation when it comes to the Internet is the result of what we've known for a long time, that the Internet is a good thing. But it's important to have guardrails and it's important to have safety measures in place. And it's important for the community to be responsible at all ends for how the DNS infrastructure is used today and moving forward.

I do want to say that on behalf of the IPC, generally and in my capacity for the International Trademark Association, we view this as a three-pronged problem. And our first set of speakers really focused on the first prong that I'll call voluntary practices. And this is where ideally, we would like to see the industry be. We would like to see practices that are tight, practices that are predictable, practices that meet the needs of the end users. And to that extent, I would say that we are cautiously optimistic about the developments that we've heard today. We still have concerns that I will illustrate later on.

But I also want to mention too the work of the Internet Jurisdiction and Policy Network which has a lot of participation from governments, the private sector, contracted parties, and more and more so intellectual property owners, and developing these global norms and standards is very, very important to whether we move forward from a voluntary perspective, a contractual perspective, or regulatory perspective. And those are the other two prongs.

I think it's very important to understand that there's a contractual element to fighting domain name abuse. Some of the stickiness to the problem has been in the definition, which has been alluded to by the other speakers. There are many definitions of abuse. There is the voluntary definition. There's abuse as defined in Specification 11 of the registry agreement. And in the register accreditation agreement, article 3.18, there is a duty to investigate abuse and a duty to have an abuse contact.

So we know that abuse has been around long enough and is serious enough that addressing it has been embodied in ICANN contracts. Where some of the controversy has come in is what do these contracts actually mean? There has not been enough litigation around it yet to determine at least from a judicial perspective what they mean. We're relying on the community to develop definitions. And this is where a lot of the tension approaches because from an IP perspective, domain name abuse goes further than the constrained—and I'm using my colleagues' word, constrained definitions that we have.

Our community sees this more along a continuum of harms. And so it's important to recognize that continuum. And from an intellectual property perspective specifically, we certainly want to see piracy, content piracy and trademark infringement specifically recognized as they are carriers of so many of the harms we have heard spoken about today, phishing, botnets, malware, etc.

So this isn't just a simple fix. And we do appreciate the fact that the industry is understanding this and responding. But there's absolutely more to be done on the regulatory side, which I think would be important for Nigel to address for all legislative perspectives and outcomes and proposals. We are very mindful that the EU has played a very important role in setting parameters around the dialogue to information access in terms of WHOIS, but we're seeing a lot of other jurisdictions also impose regulations on information access.

And we do welcome though the fact that when regulations are not easily understood or overly broad, that governments can and will step into correct. And that's what I believe we're seeing now with parts of the NIS, the cybersecurity directive out of the EU.

I also want to note the EU has commissioned a domain name abuse study. It's rather comprehensive. They've had a lot of workshops and my colleagues have attended as well as I to give different perspectives about what DNS abuse means and how it should be managed.

Now, of course, from a government perspective, we would default to a regulatory solution. But again, I see the regulatory solution as part of this three-legged stool of voluntary, contractual, and then ultimately regulation stepping in when the industry itself cannot solve its own problems.

What is the IPC doing? That's the next question. So the IPC has formed a DNS abuse response team. This is the first time we've had a team. We've been very proactive and vocal in contributing to ICANN working groups, contributing comments and interventions. But we now have a group—and I am the leader of the group—to have a more definitive response particularly to these voluntary measures, the papers that were mentioned by our colleagues. We are formulating responses, we have also very appreciatively and kindly attended meetings where we've asked to weigh in on these positions.

And we appreciate this inclusiveness because I will say up until this year, one of the major concerns from intellectual property owners were that these voluntary discussions and practices were not as inclusive of the perspective of the IP owner as they well should have been. So the fact that the doors have opened, we welcome and we are ready to get to work and sit down and find very practical solutions when we can and to keep the community on track so that we have the multistakeholder model that we envisioned 20 years ago. That is extremely important.

My organization itself, I can speak for INTA, we've developed a WHOIS toolkit, and I will put the link in after I speak. But the WHOIS toolkit was formulated as a best practice document for intellectual property owners who do have complaints that they would like to submit to a registrar and registry, because we are mindful that there are issues of how much evidence should be submitted, when it should be submitted, what is appropriate.

And I think this is where the community as a whole can really step in here and contribute so that we understand what is the basis of a good complaint and when you get a good complaint, what should be acceptable service levels for turnaround.

Now, of course, the 800-pound elephant in the room, or whatever, the gorilla in the room is the access to WHOIS information. This is an issue where I think there's been some small amount of progress inside the EPDP. From an IP owners perspective, that progress is not sufficient. We have no guarantees of access. Even if we go through enumerated steps.

And none of us believe that the balancing tests that are envisioned by any of the privacy laws being enacted globally envision a completely darkened situation. This is a serious point of contention, it continues to be, and we will sally forth to argue that balance really means balance. It means making sure that you protect individual rights and freedoms but at the same time protecting individuals from consumer fraud, from outright financial—there's a lot of damage that's being done, names are being used, identities are being stolen, financial information, bank accounts drained, counterfeit harmful products being sold, poisonous drugs.

And I think probably the most unintended and consequential outcome of what we're seeing in the enactment and interpretation of particularly the GDPR but other privacy rules as well is that law enforcement itself cannot get access to information. That's very problematic. Because from where I stand, law enforcement is part, again, of another stool that's super important. And that's with the private sector and the public sector working together to help each other in their investigations to provide and share information when we can. Those routes have been completely cut off to us.

And this is where I feel the balance is absolutely out of balance in the ICANN discussions. And I believe I'd like to see that incorporated further. So as I said, we're hopeful, we're willing to talk, we're here to talk, we're participating in the accuracy scoping, we have an IPC position paper on accuracy. We hope that we will make some progress in this arena. But I will tell you, we have negotiators and people in the room today—I see them online—who are weary, they're exhausted, because we got a little bit down the road in terms of agreeing, perhaps, to an SSAD, but we don't know what that looks like, really, we don't know how much it costs, how long it will take. And again, there's absolutely no obligations of any contracted party to release information that should be released.

And I'm going to end there. Thank you.

JOANNA KULESZA: Thank you very much, Lori. One thing I deeply appreciate is a person who speaks with passion about DNS abuse. So thank you very much for doing that. I am in the session as a moderator, so it would be utterly inappropriate for me to make any suggestions or positions. I couldn't refrain from adding a comment in the chat. What you highlight, Lori, the concerns around the system working on the ground are shared by various actors, including some of the governments. That study on DNS abuse that you mentioned that was commissioned by the European Commission reflects these concerns which might be reflected in proposed legislative acts.

Now, it's not just the NIS directive, it is not just the GDPR, which has given the ICANN community quite a headache, if I say so very bluntly, but there is also that Digital Services Act, which we did focus on within the At-Large within the EURALO during the previous roundtable. There is also the Council of Europe, which seems somewhat impatient with the EPDP and has proposed a new additional protocol to the Budapest Convention which just might attend to these concerns, particularly with regard to access to information by law enforcement.

Now again, refraining myself from picking up a thorough narrative here, I hand the floor over to Nigel Hickson. Thank you very much for agreeing to join us. I am aware that Chris Lewis-Evans has also joined this call. I do welcome participation from both of you gentlemen. I know it is challenging to speak on behalf of the entire GAC. That is not what we're asking. If you could just shed some light on the discussions on DNS abuse that are going on within the group, that would be wonderful.

Chris is co-chairing the Public Safety Working Group where the At-Large have had very useful conversations around the work going on there. So with all of this potential, I hand the floor over to you, Nigel, and I'm more than excited about what you're going to add to this debate. Thank you very much. I have been advised to speak slowly. This is me trying to speak slowly. And I forward that request our speakers. Thank you very much, Nigel, the floor is yours. Thank you, sir.

NIGEL HICKSON: Yes, thank you very much, Joanna. It's an absolute pleasure. And Chris is going to start and he'll talk as slowly as I will. Thank you.

CHRIS LEWIS-EVANS: Yeah, thank you, Nigel. And hello, everyone. So As Nigel said, I think rather than Brian's two hats, we’re going to split ourselves here. I'll concentrate on the public safety side and then pass over to Nigel for more of a governmental view of DNS abuse.

So when we talk about DNS abuse, what does it mean from a public safety standpoint? And for us, it's actual harm to the users and the people using the Internet to perform their business. So when we talk about actual harm, we talk about monetary loss, we could talk about an end of a business. And also, we can see services impacted that might have threat to actual harm to people just because of the DNS abuse. So I think it's really key to have that spin on it.

So how does that relate to the defined term of DNS abuse? I think as Brian and Graeme both said, the term in the DNS abuse framework does cover a large percentage of that the harms covered by criminal entities exploiting the DNS to cause that abuse, cause that harm.

But does it cover everything? No. And I think they recognize that. And I think, as Graeme said, really tackling what is in that framework would really help us to get a long way into stopping some of that harm, which is, really, from a public safety point, what we're focusing on, is really preventing that harm.

And I also noted that Graeme mentioned compromised domains. We see those that have been impacted on as victims. And that does include people who have had their domain names exploited or taken over to commit harm. But what we really need to be able to do, and this is something that the PSWG is striving to sort of educate all the law enforcement agencies, is how do we create the best evidentiary standards to be able to inform registries and registrars to take action that can stop harm being committed on the Internet, can stop the DNS abuse from happening.

Whilst we understand that suspending, even temporarily, a compromised domain will have an impact, it might be the right option. If that domain is causing multiple victims by being up, then that might be a choice. But you can only make that choice with the correct amount of evidence and I think where the direction of some of the conversations that have been going in the last year or two years is a really good step forward of being able to have more consistent systems where we can provide the evidence to be able to take quicker sort of effective proactive action. It's not preventative, which would be ideal. But when we do act, we need that action to be very, very quick.

Education is really key to being able to protect some of those victims of the compromised domains. So I think there's a large part of work, and we don't want to miss out on any one part to be able to affect a whole system.

And so I think going back to the preventative side, I think that comes down to a more legislative function, and some of the things that maybe Nigel might touch upon. And certainly some of the things that Joanna has mentioned, looking at what can be done on a legislative function to enable more preventative action, but also, from our point—and this may be touched on the Budapest Convention—is to increase the speed of some of that action.

The way that the DNS is being exploited is very much an international mechanism. And that makes it very hard for public safety to act in a quick manner, utilizing some of our legislation legislative functions. So, having those right tools is very important for us to be able to take action against this and work with registries, registrars, hosting companies and service providers to not only take the right action, but to stop the harm, which is really important.

And I think engagements like this, and I think it's probably fair to say that the GAC and the PSWG would up their engagement to be able to make a direct impact on how we can tackle DNS abuse. And I think it's really key that we continue doing that. And I know that utilizing ICANN and the multistakeholder model is really important to us as law enforcement and GAC as well, very important to get that that right and to effect change.

And so I'll probably quickly hand over to Nigel before I use up all the time, and go from there. And it'd be really good to answer some questions later. So Nigel, over to you. Thank you.

NIGEL HICKSON: Thank you very much indeed, Chris. And it's probably a good idea for you to use my time. And then I have less to say. So thank you so much, Joanna. I regard this as very important. I think I'm the last person that I ever thought would be passionate about DNS abuse. But I am passionate about DNS abuse. And I'm not passionate because it's DNS abuse. I'm passionate because we need to solve the issues. I'm passionate about ICANN, I'm passionate about the multistakeholder model. I'm passionate about Internet governance. And we have a key role in that. Because, boy, the eyes are on us, the eyes of the world are on ICANN, the eyes of the world are on what we do. The legislators are looking at us, and we must move forward.

But we have come a long way. There seems to be an understanding of what we want to do. There is tremendous goodwill, there is tremendous activity in various places in the community. We heard today about the excellent work that the Contracted Parties House and others have put in place in regard to the trusted notifier scheme. We heard about the DNS Abuse Institute and the excellent work that is going on there. We heard about the work in the I & J network on this issue. And I've been contributing to that. And that really is superb contributions from many from the ICANN community and making that work so much viable.

So why are we still where we are? Why are we still discussing these issues and not discussing specific actions? We have the data, we have the DAAR reports, the excellent work that ICANN has put into providing data. And of course, there's data out there from other places. So how are we going to move forward on this? How are we as a community going to respond to this? Are we still going to be here in three or four years’ time having plenary sessions where we just exchange views, or are we going to move forward as Lori and others have said?

And I think we have to move forward. I'm not speaking for the whole GAC at all in this but I think many of us in the GAC have the same experiences. We have our governments, we have our ministers that get letters daily in their post bags. In the UK, we have some rag called the Daily Mail that writes letters that has letters in it from constituencies and readers that challenge the whole nature of the domain name system.

People ask, why is it that a website that is put up to sell cakes or sell bunting or to sell anything is taken over and the next day, it’s used for pornographic images or is used to defraud people or what else? Why can that happen? Why can't that site be shut down? Why cannot a site that's legitimately registered to do something quite legitimately, and then lent to be a site for a botnet or some other fraudulent activity, why can't something be done about this? These are the questions our ministers are asking us. And we have to have answers.

So what do we need to do? How do we need to take this forward? How are we going to work together to solve these problems? We've often talked about a PDP on DNS abuse. We've often discussed other ways forward. Of course, there are tremendous issues around policy development process and the length it takes, and the volunteers that it would use additional energy from. And I think many of us in the GAC are conscious of that.

But what alternative methods do we have? Should we form a cross-community working group to look at this? Should we solve these problems through some cross community working group? Or should ICANN form some sort of group to look at the contractual obligations that currently apply and work from that side?

I'm not suggesting there's a definitive way forward. But what I am suggesting is that time is running out. We need to do something, we need to be positive, we need to be articulate, and we need to be able to answer those voices. We are the ICANN community. We did the IANA transition. We have done many other things. Not me personally. I was just an ICANN staff member.

But we have done tremendous things. People remember ICANN for what it's done in this multistakeholder framework. And we must once more step up to the plate and do something to solve this problem. Thank you.

JOANNA KULESZA: Thank you very much, Nigel, that is a much-appreciated call to action. Although let me just note, we have heard from Graeme, Brian, James about all the activities that are already happening. We do appreciate these and I do read your comments as an encouragement to take these a step forward, to carry the message and to make sure that these policies are comprehensive and effective universally in a way that we would envisage them to be. Thank you, everyone, for these very insightful contributions.

I have made Jonathan's work very challenging now, because we are relatively short on time. But we have collected the questions and I have conveyed them to Jonathan. And I would love to see Jonathan try and summarize and go through our speakers with a recap of these questions,. I know you can navigate the audience. So with that, with full confidence, I hand the floor over to Jonathan to handle the Q&A session before we let Olivier summarize. Jonathan, I know you'll have tested your audio and video, this should be working well. If you can hear me, the floor is yours. So thank you.

JONATHAN ZUCK: Thanks, Joanna. Thanks, everyone, for your discussion. I'm going to try with a bunch of questions that have been put into the chat to bubble them up into meta questions, if you will. One question I have is that there appears to be a very strange dynamic between the ICANN community and the contracted parties on the one hand in that everything that we think of as policy changes, as reforms etc. end up putting a bill on the desk of the Contracted Parties House and as you say, it's a sort of low margin activity and there's resistance that leads to this collective action problem that that Graeme mentioned.

The other piece of it though is that ICANN itself invests a great deal of money into these things. And yet there's substantial evidence that those tools might not be as effective as they could be. DAAR is up for review.

There's a public comment period coming up on DAAR. And it makes me wonder if the generosity of PIR to create the DNS Abuse Institute, has Graeme in some respects replicating some of the functionality that's being discussed inside of ICANN. So this centralized complaint system sounds suspiciously like the SSAD system that was so famously fought over in the EPDP. The ability of creating a better tracking system seems strange in the context of DAAR.

Why is there this disconnect between the tools that ICANN is trying to create to help this and the sort of pragmatic or practical tools that it seems that the community really needs? And how can we address that? Because there are resources available there. It seems like they're just not hitting the mark. So that's a question for any of the panelists that want to take it, but maybe first of all, Graeme, because I feel like he's foremost been put in the role of sort of redoing things and that that feels unfortunate.

GRAEME BUNTON: So there's a lot to unpack there. Thank you, Jonathan. So DNS abuse, online harms are bigger than ICANN. They're bigger than registries and registrars. We’re only one piece of a much larger, much more complicated puzzle. And sort of James talked about this a little bit. And I didn't, I talked about registries and registrars in that economic context. The people perpetrating online harms are sometimes onesie twosie script kiddies in their basement trying to do bad things.

And also, a lot of it is organized, coordinated criminal gangs that are better resourced than ICANN or better resourced than like, essentially, the entire industry. Like they have lots of money and resources at their disposal. And trying to combat that individually is essentially impossible. And that's where we need to come up with these collective solutions.

Things like DAAR, for example. And I think, essentially, it's a proof of concept that you can collect date on abuse and report on it. But it really doesn't go far enough to provide any useful information for people to take action on. And I think that's a couple reasons. One, it was built a few years ago as sort of, again, that sort of proof of concept that it can be done. But ICANN is also encumbered by perception and its contracts and its relationship with registries and registrars and the rest of its community and so I think has to move very carefully.

And so I take a great lesson from DAAR. There is something there, it can be done, boy, let's see if we can do it better and faster and in a way that provides more valuable, more useful information. And so I think that's going to be true of initiatives between ICANN and the rest of the community that like ICANN’s job in a sense might be to say, hey, we think this is useful and good.

But ICANN remit is not the entire Internet. And these problems do cross boundaries in interesting ways. And so then it's for things like the DNS Abuse Institute or other organizations to learn those lessons and then go see what we can build and engage with registrars and registries and hosting companies and content delivery networks and Internet registry like RIRs, for example, all of these bits and pieces that have a role to play in sort of the abuse ecosystem.

I think I covered most of that in there maybe to that question. There are probably some other bits and pieces I should address at some point, too. But I'll throw it back to you, Jonathan.

JONATHAN ZUCK: I guess, Graeme, what I was trying to get at though is that it feels—the pilot versus implementation thing makes sense to me. Then should we be telling ICANN to stop investing in DAAR, or should you instead of investing in something similar, be providing guidance to ICANN? It feels like there's a replication of activity, which is only a dispersal of resources. And the money is coming from the Contracted Parties House in the first place to fund ICANN. There's just this strange thing.

And so I'm wondering, is there a way—and part and parcel to this question, you and I have talked about this before, you mentioned in your session about the high costs associated with predictive analytics. And there are so many contracted parties that don't have the resources to invest there. And is domain of these DNS Abuse Institute or ICANN or in conjunction somehow equipped to potentially provide predictive analytics as a web service or something like that as another possible investment? Is there a better use of the resources than having duplicative projects?

GRAEME BUNTON: So I think probably you're right. The centralized abuse reporting tool that we're looking at standing up, boy, if I'm aggressive in my approach with that and we're able to execute on this well, it would be a thing that I would love to see ICANN formally support, like, whether that becomes a policy or a contractual thing, like, “Hey, you just need to be able to accept reports from this tool that the industry has already used to a large extent and is endorsed by the community and does a net good.” That would be an amazing win for I think the community and the Institute and would go, hopefully, some distance in helping reduce DNS abuse.

But we just don't have any examples of that yet. And so I would love to get there, I think would be ... You're right re: DAAR that there is some duplication of effort. I just think that that is what that is as.

JONATHAN ZUCK: As a pilot project, should we be recommending the DAAR be discontinued at this point, now that there's an open comment on it?

GRAEME BUNTON: I'm not gonna touch that one. I'm gonna leave that for someone like Brian.

BRIAN CIMBOLIC: I think part of this is there sort of a—DAAR became a shiny tool that was used improperly in the sense that DAAR wasn't meant to ever be actionable, at least from the registry or registrar side. The license requirements on their side, they could never say here, we've spotted 10,000 domains in .org—This is an example. This is a hypothetical. 10,000 domains engaged in abuse in .org. The natural question is, great, can I see them? No, you can't. That's not what DAAR is. It's the equivalent—using DAAR as a panacea is like trying to use a screwdriver to hammer up things. It kind of sort of works, but it doesn't.

That's not what it's there for. DAAR is meant to be the highest high level, sort of overall health report card for the gTLD space. It doesn't even really—the reports don't get to the registry level. There's really nothing actionable from it other than okay, how are we doing as a whole overall?

And so if you just accept it as that and recognize it has very limited uses, if you accept that and look at that one limited use and don't try and extrapolate and solve broader and more complicated problems with a very simple limited tool, then I think it has value, but you have to recognize what its actual value is and not try and misuse it.

JONATHAN ZUCK: All right, thanks. Another question that came out of the chat has to do with the availability of the information collected by these systems. So part of this might be a question for Graeme as an intentions question. But a question for you and for James as a desired outcome question. If you begin to build a gateway for complaints, etc., will you do reporting from that? A lot of folks along the way have made the request of Compliance, made the request of DAAR—as you say, it might be a licensing problem—of being able to get information out from it that might affect consumer and law enforcement behavior based on propensities of high levels of complaints, slow response times, etc. Is it possible this information will be made available either publicly or under some sort of a trusted program?

GRAEME BUNTON: Thanks, Jonathan. It's a good question. And let me talk about it briefly from the institute's perspective, because we're looking at building a reporting solution, a centralized reporting solution for the industry that gets people useful, actionable stuff when they need it, where they want it, and also an intelligence platform to understand DNS abuse, where it's happening, at registrars and registries. Persistent, evidenced, good stuff. And I talk about these things on the institute's website in more detail. And please, people, go read our roadmap, there's lots of good stuff in there.

I think quite a lot about how those things are going to be coupled. And at the moment, they're not. Because I think we need to have an independent, robust, transparent reporting system on DNS abuse. And I think we need a system to capture abuse reports, make them useful and get them to where they need to be. But for me to get registrars to adopt a system that I think provides real value for them, and then use that same data to maybe throw them under some sort of bus of public opinion would be really disingenuous. And so I think you need to be extremely careful about how close you're tying those systems together. And at the moment, I'm not.

JONATHAN ZUCK: All right, thank you. Lori, go ahead.

LORI SCHULMAN: Yeah, I just I just wanted to chime in here, because I think this is one of the enduring sticky points, is about scope. And DAAR has limited scope. And we can't figure out how to figure out the scope. And then we get stuck in the mud in terms of trying to illustrate a problem. People keep screaming about “show me the data, show me the data.” We've got private sector reports, we've got public sector reports. There's a ton of information out there right now. And I think the problem is even more fundamental than agreeing on a definition, we don't even trust where we're getting our data from. We keep crushing each other's data.

So to the extent that the community itself—and I don't know if it is through the DNS Institute, it might be, or maybe it is through and ICANN process where we have collective agreement on what data means at a given point from a given source. We don't have that. It's a big problem. As you well know, Jonathan, working on a CCT RT review, getting the data was extremely difficult, expensive, people have different ways of recording information. Reports are inconsistent. I think Graeme pointed out that reporting generally is a mess. Or was it Brian?

The reporting is a mess because we haven't figured out some sort of global or universal agreement about what things should look like. So I don't even know how we get to a definition when we don't even know how to scope the problem that we can agree upon.

JONATHAN ZUCK: Thanks, Lori. Yeah, data is a very clear problem in this for sure. So I think every time anyone mentions the creation of data, everyone wants that data. So it's definitely an ongoing question, especially because data presented is usually in sort of modified form, and then is indicted by others that are looking at the data. So it's a tough thing to agree on the data as well. I've got a little bit of a cue here.

I wanted to ask a quick question of James, that I gave you a heads up about, which is that, again, part of what we hear is that there are those that are somewhat bigger contracted parties, bigger registrars versus smaller ones able to invest, more able to come up with these best practices. And the CPH has gone a long way to start to document, represent what are good practices, etc.

Do you have any evidence or indication whether or not those in the industry we don't hear from the most that are out there, that aren't regulars at ICANN meetings, are taking advantage of these documents, that they're taking these things on board and trying to implement some of the best practices that you've developed?

JAMES BLADEL: Thanks, Jonathan. I'll jump the queue. I guess, with apologies to Chris.

JONATHAN ZUCK: I'm not taking your question yet, so ...

JAMES BLADEL: Okay. I was actually gonna respond to a comment from Lori. But yeah, I think it's a challenge. It's kind of like, do we have any indication of the folks that we don't see are changing course? I think certainly, we've gotten some attention with things like the framework on DNS abuse, and we've got some folks that have come out of the shadows a little bit to say, “Hey, how can I get involved? How can I sign on?”

But I think it highlights this problem that we have with the long tail in the industry, which is, you're going to have the folks who are responsible actors come to ICANN meetings, come up with ideas and implement solutions and make the investments, and then you're going to have kind of this long tail of smaller providers that are either unwilling or unable to match those commitments.

And I think that what we're seeing from efforts described by Brian and CPH, from the DNS Abuse Institute and framework and even projects like the Internet Jurisdiction project is trying to kind of lift that baseline so that maybe not everybody's performing at the top of the scale of abuse mitigation, but at least maybe we can raise the floor a little bit for some of those smaller players.

I think it's always going to be a challenge. And I think it's indicative of a couple of realities that are really tough for this community to face, one of which is that there's not one single choke point that we can say, “Here's the problem, let's go and kind of squeeze that bottleneck and fix it.”

The other one is that there are a lot of aspects and dimensions to this problem that exists outside of ICANN’s remit, and so we can kind of make this particular area maybe unpalatable to those bad factors. But a lot of this, these are social problems. These are intergovernmental problems. These are criminal justice problems and jurisdiction problems.

And there's all kinds of sort of overlapping things that ICANN really, we can, we can talk about them, we can even maybe bemoan that they seem intractable from where we sit, but we have to kind of—and I think I keep coming back to definition, we have to understand which parts of those problems that we can take on and that we can solve, because the way you address botnets, for example, may be radically different than the way you address phishing as an issue. And so they may require separate processes and separate policies. And noting our experience with some of the other PDPs, a contracted party's internal policies and procedures could evolve three or four times over the lifespan of a single PDP, which is also conducted out in the open.

So it's kind of an element of, is ICANN are ICANN's policies the right place and the right tool to address some of these problems? And I think, what we keep coming back to is there are probably better, faster, more efficient and more effective ways to take this on.

So I don't know, that's a roundabout way of answering your question. But I think the goal is to make the bottom of the scale either raise their game so that they're more effective in kind of contributing, or convert them to resellers and get them out of direct contracts with ICANN.

JONATHAN ZUCK: Thanks, James. We are really running out of time, so I'm actually going to close the queue at Chris Lewis. Christopher, you're not going to make it this time. So we'll figure out the best way for you to get your question answered. Chris Lewis, do you want to make a comment? And then I will—Lewis-Evans, and then I'll hand it over to Olivier.

CHRIS LEWIS-EVANS: Yeah, I'll be very quick. So just [inaudible] what James and Lori said together there, I think there isn't one way to solve this. We don't have any trusted data. Graeme mentioned RBLs, James mentioned a couple of things with DAAR, sort of Brian did.

So having an agreed transparent mechanism where we can collect data and see what some of these voluntary frameworks and things are having an effect on the DNS abuse would be really key. So I think having a proper way to record and measure that would be really helpful for tackling the problem as well. I'll stop there. Thank you.

JONATHAN ZUCK: Thanks, Christopher. And then Joanna has asked me to hand the baton to Olivier. Unfortunately, you you've got zero minutes, but if you have some closing thoughts or summaries of what you learned on this, then give it a shot, Olivier.

OLIVIER CRÉPIN-LEBLOND: Yeah, thank you very much, Jonathan. Just a few points. I guess we've learned a lot of things today. I think it was a great discussion. The first point I think that we came up about was that DNS abuse is just one small part of the wider range of abuses that we see out there on the Internet and malware, botnet, pharming, phishing, spam are all types of activities that involve or do not involve DNS abuse.

Most of the data—and this is Graeme who first spoke to us about this, most of the data about abuse comes from reputation block lists which sometimes are not looking at the same angle. Rather than mitigation, it's more looking at cutting things off. Registries and registrars try their best to mitigate abuse, but they often receive rubbish abuse reports. So you end up with reports that they can't do anything about or where they don't have the right information to allow them to take action.

Brian Cimbolic from PIR spoke to us about the amount of work that was done in contracted parties to mitigate DNS abuse. And much of it also involves capacity building towards the contracted parties on how to handle this. Work has taken place to promote principles within the Contracted Parties House, transparency, active mitigation of the abuse.

And PIR is also rolling out various programs that incentivize registrar channels to have high quality domains with low levels of abuse. The equality performance index is one thing that they're rolling out and that has really been well received. It's a voluntary program to improve the way the registrars do business and has had some positive impact.

James Bladel from GoDaddy has spoken to us about how important it is to really define DNS abuse. It's important because sometimes we're just putting so many other things under the DNS abuse bucket, such as contract issues, commercial disputes, things that a registrar has absolutely no control over. So we need to make sure there's a common understanding on that. And when you look at the number of reports that come out there on the desk of a registrar, 90% of the reports are unactionable. You have social media campaigns that create so much noise and that the abuse teams are subjected to. And often because the registry has no contractual relationship with the end user, it's the registrars that bear the brunt of the costs in mitigating the abuse. So work that the DNS Abuse Institute does in filtering out these reports and ensuring there are quality standards and the pinpointing of DNS abuse is something that would be helpful.

We also heard from Lori Schulman at IPC, who mentioned that the Internet is a great thing, but it's important that we have guardrails and for the community to be responsible. It's not a simple fix. And of course, the EU has set parameters around the dialogue of WHOIS and information access. And for Lori and the IPC, one of the biggest problems is that that access to information. The emphasis should be voluntary, contractual, and only regulation when the industry itself cannot solve its own problems.

So the IPC is formulating responses to voluntary methods and appreciates the inclusiveness for the formulation of these voluntary and practical methods to mitigate DNS abuse. But access to information is important. And we've seen in the recent EPDP on the WHOIS issues regarding GDPR that there hasn't been the balance that the IPC has wanted to see in this.

Chris Lewis-Evans from the GAC Public Safety Working Group has mentioned that there's a lot of harm out of the abuse that is taking place. It's actual harm, it's its monetary, loss of business, it's bigger than just the sort of ruffling of some feathers. The GAC Public Safety Working Group is trying to find out with law enforcement how to create the best evidentiary standards, because the best way to be able to go after those perpetrators of the abuse is to have proper standards and proper evidence for this. And having the correct amount of evidence is so important, especially since we're dealing with a global network and therefore national law or national initiatives just don't go far enough.

So being able to work with registries, registrars, service providers and hosting providers to address the problem in a multistakeholder manner is an important thing.

And Nigel Hickson from the UK GAC representatives has emphasized the whole point of this multistakeholder work that's been going on at ICANN and has suggested perhaps there needs to be more than that, because ICANN is under scrutiny by governments at the end of the day. Newspapers, the popular press often points out the fact that a website has been taken over and has caused a lot of harm, and just wonder how can this happen, why doesn't the government do something about it.- And so that there's really the pressure on ICANN community to work on this.

Q&A, a couple of questions were aimed—so first, the whole thing about DNS abuse being bigger than ICANN itself. And Graeme mentioned that perpetrators of DNS abuse are not just like the script kiddies that we used to have in the past, but it's often organized crime with huge, huge resources. It's a real, real test, towards the community.

DAAR is a proof of concept. It's not a real solution, it's very limited as it goes only to such an extent but doesn't actually provide full details of what the perpetrators are. So as a proof of concept it is good, but there needs to be work done to perhaps to get DAAR used widely or publishing full data, then then it would be great. But at the moment, it's become some kind of a shiny tool that is not meant to be actionable and that makes it very limited.

So there's a question about building a gateway for complaints. And Graeme mentioned that the DNS abuse Institute is currently working on putting together an intelligent platform for registrars and registries, but also some way to have independent and robust reporting of DNS abuse. But it just will not work if this system is used to actually put registrars in the corner and point the finger at them and throw them under a bus as he has mentioned. So one has to be quite careful about this.

Lori did come back and say there is a problem in getting the data, because it seems that nobody really is trusting the data that we have out there. Everyone that brings data is seen in some suspicious way.

And then finally, the last questions are those in the industry that we don't hear about, the ones that don't come to ICANN meetings actually taking part, have they started to follow the best practices that were developed by contracting parties? And Jim has mentioned that the framework on DNS abuse triggered some folks to come out of the shadows. So yes, there is more going on. But we have to remember that a lot of the abuse that we're seeing is not stuff that is in the ICANN’s remit, it's social, jurisdiction, legal. So we have to be careful. And it's a difficult field to work on.

And finally, Chris Lewis closed up on the discussions, that there's not just one simple way to simple way to resolve this. The RBL, the DAAR, all of these are there. But there needs to be a transparent system to record the success of these systems so we get the feedback and then we can improve on them.

That's really the discussion, but it was a lot for this 90 minutes.

JOANNA KULESZA: Thank you very much, Olivier. Thank you to all of our speakers. I was hopeful of us achieving a comprehensive compromise. Whereas it seems as if once again, we've only touched upon the surface. But I do believe that the amicable atmosphere we have enjoyed is a step in the right direction.

As already noted in the chat, there will be a DNS abuse dedicated session in the joint ALAC-GAC meeting. We will also be discussing security, safety, DNS abuse throughout the ICANN 72 week. So we do hope to see you around the At-Large session and around ICANN 72. And we will pick these discussions up again online and hopefully also offline when we do manage to meet face to face during the next ICANN meeting hopefully coming up sooner rather than later.

Thank you everyone for joining us. Thank you to our excellent speakers. Thank you for the skillful moderation of the Q&A section and a brilliant summary from Olivier. Until I see you again. Stay safe everyone, talk to you soon. Thank you very much. This meeting is adjourned.

DEVAN REED: Thank you all for joining. This meeting is adjourned. Have a wonderful rest of your day.

[END OF TRANSCRIPTION]