MONTREAL – DNS Abuse
Wednesday, November 6, 2019 – 10:30 to 12:00 EDT
ICANN66 | Montréal, Canada

BRUCE TONKIN: Okay, everybody. If everybody could please take their seats, we'll get this session started. I know there's a lot of people interested in this topic, so we want to make the best use of time starting this morning.

So today there's been -- it's Wednesday. For most of us, it feels like we have been here for two weeks already.

The purpose of this session really is to bring together a lot of discussions that have been happening pretty much every day this week around the topic of DNS abuse. I guess the context for the topic is that there are a number of references to DNS abuse and collecting information about DNS abuse and the existing registry and registrar agreements. The topic was touched upon by the Competition, Consumer Trust and Consumer Choice Review Team. And they had three or four recommendations that related to elements of DNS abuse.

We have ICANN, the organization, that's been collecting and publishing data on statistics on the number of domain names that they've seen reported in various registry and top-level domains that relate to DNS abuse.

And we have a lot of industry practices out there that are probably not well-known. And I think from a community point of view, it's probably not clear on what the requirements are for registries and registrars to

investigate. It's certainly not clear what happens after a particular report is made of DNS abuse. And that's probably the area which is least understood.

So the purpose of this session is to give a bit of an introduction to the topic. We have a panel of experts from various parts of the ICANN community that will be able to comment on topics. And then I want to actually hear from the audience and allow the audience to ask questions or make suggestions for how we can move forward on this topic and basically protect the end user from DNS abuse.

So what I'll do just to start with is just do a very quick introduction to the panel members. So if each member of the panel could say their name, what part of the ICANN structure they're from, and why they think this is an important topic just in one sentence.

And then we'll give a short overview of the topic, which is basically a shortened version of a Webinar that was done in recent weeks on this topic.

So starting on the right, Gabriel.

GABRIEL ANDREWS: Hi, folks. So my name is Gabriel Andrews. I'm here on behalf of the Public Safety Working Group. You sometimes might hear that as PSWG. And in my day job, I investigate cybercrime in the United States.

FARZANEH BADII: Hi, I'm Farzaneh Badii. I'm here on behalf the Noncommercial Users Constituency and I work at Yale Law School.

BRIAN CIMBOLIC: Hi, I'm Brian Cimbolic here with the Registry Stakeholder Group. And I work at Public Interest Registry, the operator of .ORG.

GRAEME BUNTON: I'm Graeme Bunton. I work for Tucows, a Canadian registrar. I'm here on behalf of the Registrar Stakeholder Group.

MASON COLE: Good morning. I'm Mason Cole with the law firm of Perkins Coie, here on behalf of the Business Constituency.

JEFF BEDSER: I'm Jeff Bedser. I'm here with the Security and Stability Advisory Committee. And my day job is with iThreat Cyber Group.

BRUCE TONKIN: Thanks, Jeff. I would like to hand over to Gabriel to give a shortened version of some of the slides that were presented in the Webinar last couple of weeks.

GABRIEL ANDREWS: Well, let's test this out. Hey, it works.

At the outset, I know there's a lot of discussion that's been occurring about what is DNS abuse and the desire by some to seek a coherent definition. From the perspective of the Public Safety Working Group, there are already some very good attempts to try to define this space. And in particular, they would point to the advice that the Governmental Advisory Committee issued in 2013 called the GAC Beijing advice. You can see it highlighted there at the top. I don't want to read this whole slide to you, folks. But these are -- these are some initial recommendations surrounding what we consider DNS abuse to be. This got wrapped up into actual obligations within contracts that falls under what's called Specification 11(3)(b).

We view this as essentially a floor what registrars and contracted parties and others should view as their responsibility for addressing abuse that occurs online that damages us as part of this Internet ecosystem.

Since then, we note with pleasure that there has actually been a lot of very interesting discussion and the ball has been pushed forward by parties acting in good faith to adapt these understandings of the abuse that's occurring.

We note that the domain abuse activity report -- that shorthand is DAAR -- is trying to quantify some of the abuse that's seen. Data is good. Quantification is good. There might be individual complaints about methodologies, but let's work to improve that.

Further, we note with interest that the framework to address abuse, a product that I'll let others speak to because it's not ours, was a

collaborative effort by some contracted parties and some within the Business Constituency to go even further and describe some places where abuse can, should, must be addressed. We appreciate those efforts to collaborate and to actually try to come up with common-sense solutions to address it.

All that said, I'm a cop here, right? And I want to make sure that we don't lose sight of what's actually happening in the real world. And what we might term DNS abuse here is to me is cybercrime very often in the real world.

And I want to actually provide some pretty pictures for you all to take a look at that's just some real-life examples of abuse that's occurring now because while we might be very glad to somehow find a perfect definition of DNS abuse tomorrow, we should not allow that desire to inhibit the actions that we can take today that will be very good to address the crime that's occurring.

So three quick examples of what we see in the real world. The first we call business email compromise, sometimes shorthanded as BEC. It's as prolific and damaging as it is simple. It is bad guys lying by email to trick people to send money. The email you see here is a real email. This was used to solicit -- I believe the sum was $250,000 from an unsuspecting victim. The funds were protected and saved.

The domains that you see here are real used with permission -- at least the victim's permission. I didn't ask permission from the bad guy. We've redacted some of the names here, but I hope you can see that

this is a very simple scheme in which not much technical proficiency is really needed.

But you can see that there's just a single-character change between the "from" and the "to" addresses there: Flyjetedge, flyietedge.

I talked to some very smart people at an unnamed registrar that tell me that a single-character change between the "from" and "to" domains represents a greater than 80% chance of an email being a BEC email. This scheme has put universities' budgets at risk, has knocked out philanthropies from the face of the world. It has accosted to the world's global economy $26 billion since we have tracked this beginning in 2013. Each passing year we see as much of this scheme as all prior years combined.

It has impacted 177 nations in the world. Wikipedia tells me there's only 195. I don't know which 18 aren't there, but I doubt they're here either.

Second category I want to run through very quickly. This is a confusing slide. I'm not going to dwell on it, but we want to talk a little bit about botnets and a term you might have heard used before called domain-generation algorithms.

It's a little bit confusing. But in short botnets are when bad guys infect a host of computers out there. Maybe your mom and dad when they are complaining about their computer running slow and asking you to fix it, maybe their machine might have been incorporated in the bad guy's botnet.

Now, the bad guy has to control them somehow. And one of the ways that's done is by using domain-generation algorithms to randomly create strings of characters for domain registration.

You see that in the boxes there. Those red boxes that are highlighted, those are domains that are generated by an algorithm. The bad guy uses this to issue controls to all the infected machines of the world.

Interestingly enough, DGAs, domain-generation algorithms, are also used by bad guys to register a lot of domains for use in spam. There are far fewer legitimate uses, I suspect, for random-string domains generated by DGAs. Although I invite folks to catch me in the hallway and educate me as to what legitimate purposes are because I see sometimes in the real world certain registrars making DGAs part of their registration process alongside bulk registration.

Finally, the third category, ransomware in addition to the business email scheme I previously discussed is one of the top two most impactful, damaging schemes that we see today.

If you're like me and you're at an ICANN conference and you wake up first thing in the morning, you might turn on the news. If you did it on Monday morning, you might have seen this. This is the town of Nunavut, which my RCMP colleagues, the Royal Canadian Mounted Police, tell me is about a three-hour plane ride to the north of here. A small town.

As you can see in the white box there, they were hit by a string of ransomware. Now, ransomware is bad malware that will get on your

computer and it will encrypt all of your files such that you can't access them. You don't have the ability to see what's on your computer. And it will further go beyond that, it will move to all the computers on a network and infect them, too. And then they will charge you a ransom. If you pay the ransom, maybe you get the access back; maybe you don't. It's pretty hit or miss.

And I will leave you with this thought. This particular attack, they attribute -- as you can say, officials say random hack likely came from a spam email. Do we think that the folks in Nunavut, as they prepare for winter and get their government back online and snowplows back on the roads, do we think they really care about the perfect definition of DNS abuse? So I will leave you with that. Thank you.

BRUCE TONKIN: Thanks, Gabriel.

Brian, if you could give an update on the registry-registrar -- again, a shortened version of what was in the Webinar last week.

BRIAN CIMBOLIC: Sounds good. Graeme Bunton and I are actually going to tag team this to talk about both the registrar and registry obligations.

GRAEME BUNTON: Right. This is Graeme from Tucows. So we'll start with the registrar contractual requirements, which are relatively straightforward. There are three provisions in our contracts dealing with abuse. Briefly, they

are registrational, maintaining abuse contact and take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse. We have to maintain a dedicated law enforcement abuse contact 24/7 and review complaints within 24 hours. And we must publish our abuse handling procedures on our websites.

BRIAN CIMBOLIC: From the registry side, the biggest abuse obligations are contained in Specification 11(3)(b). And that requires registries to conduct technical analysis periodically to look for security threats, which as Gabe touched on phishing, malware, botnets, and to maintain statistical reports on what threats were identified and what actions were taken as a result.

So it's important to recognize in having these conversations what a registry and registrar can and cannot do. So we really only have one option -- one practical option in addressing abuse, and that's suspension of the domain name. And that is done on the registry side through server hold, on the registrar side client hold. Technically we could lock the domain, redirect, transfer, or delete the domain. Redirection and transfer is kind of an extreme remedy and typically would require a court order. Deletion is not an effective remedy because if the domain was being used for a bad purpose, once it deletes and gets cleared again, it can be reregistered and used for that same bad purpose. Suspension of the domain name not allowing any of the content to resolve or any associated mail with it is the most effective and really the only true tool that a registry has and a registrar has to address DNS abuse.

And so it's important to think about and keep in mind that we act at the domain name level. So if there's a piece of website content that someone has complained about, we don't have the ability to act at the website level. Hosting providers might be able to remove a piece of content. Registries and registrars cannot. We can only act at the domain name level.

GRAEME BUNTON: I think just another piece there, so acting at the domain name level, if it's an email issue is also problematic because we have no ability to impact any of the particular email addresses at the domain level.

And there's another piece here on unregistered domains, specifically around DGAs. I don't think a lot of registrars necessarily have tools to prevent registrations that don't exist yet. So it's an interesting problem for us.

BRIAN CIMBOLIC: And DGAs, domain-generating algorithms, is an area which registries work very closely with our colleagues in the Public Safety Working Group and various law enforcement agencies. So a law enforcement agency will discover what the algorithm is and work hand in hand with the registries so that we can register or block the particular domain names before they can be put to bad purposes.

So those two sides are important to recognize. One, are we contractually bound to do? And once we've identified abuse, what can we do from a technical perspective? So that's just kind of the baseline.

But it's really important to recognize that registries and registrars routinely go above and beyond what's just contractually mandated. So each of us would have our respective acceptable use policies which might cover website content issues.

There is -- as Gabe mentioned, a number of registries and registrars got together and published a framework to address abuse. Now, it's important to note that's not a Registry Stakeholder Group document or a Registrar Stakeholder Group document. It's a collection of recommended practices that we think are responsible for registries -- that responsible registries and registrars should think about adopting.

Contracted parties often also work with trusted notifiers in certain scenarios. We work with, for instance, the Internet Watch Foundation to help find and root out CSAM, child sexual abuse materials, in the .ORG zone. And many other registries and registrars have similar programs.

Lastly, there's also some incentive programs that reward good behavior among registrations. So PIR, we have something called the quality performance index which looks at a registrar's abuse metrics and domain usage renewal rates, things that really are earmarked of quality domain name usage. And so a registrar can get incentives -- price incentives for having quality registrations. And the first and foremost thing we look at with that is domain name usage. There's a similar program in the CC world. SIDN, the .NL operator, has something similar in place as well.

GRAEME BUNTON: So I think just a couple more points on this is probably registrars -- I'm not going to speak for registries on this -- tend to be just absolutely terrible at self-promotion on the work we're doing in this space. And the reality ends up being that registrars are taking action on DNS abuse all day, every day.

I know from Tucows, for instance, we're taking down something like 100 domains a day for DNS abuse. We don't advertise this. We don't tell people about it. And I guarantee this is reflected really broadly across the industry, but there is a lot of activity that's very important and we're really just bad at telling people about how important that is.

And then lastly to Gabe's point on a perfect definition of DNS abuse, that's one of the reasons that the framework was put out, was we wanted to default to action because it felt like we could discuss the definition for forever but we really wanted to capture what registrars and registries are doing and then move forward from there and actually start tackling some of these things rather than discussing some of these things forever.

BRIAN CIMBOLIC: I just wanted to piggyback on something Graeme said about this isn't just an academic discussion that registries and registrars do action these consistently.

We have started at PIR putting up our abuse statistics. We're going to update it once a quarter. And through the third quarter of 2019, we have suspended over 28,000 domain names as a result of identified

domain name abuse. So it's happening every day, and we're really only collectively starting to talk about what we're doing and what the results are.

BRUCE TONKIN: Okay. Thanks, guys. I think it's important we've heard from a gTLD registrar and a gTLD registry. But it's also important on particularly this last slide and certainly participating in discussions from country code operators during the week, many of them are doing much the same thing. So we heard from Europe, for example, .EU. There's a number of CCs that have different financial programs to incentivize good behavior, a number of them work with trusted notifiers, et cetera.

It's much broader than just a generic top-level domain issue. This is also tackled within the country code world as well.

A few of the speakers have talked about the definition of "DNS abuse." The definition, I know Gabriel had it on his first slide, talks about phishing, pharming, malware, and botnets which are different technical methods of abuse.

The ICANN reports report on spam. Spam has different forms. Sometimes spam is just marketing. So, you know, you send to as many people as you can to try to get them to buy your product. Usually countries have laws that you can do that once and people have to be able to unsubscribe. So there's a whole bunch of regulation around spam.

But spam is also used as a mechanism to initiate things like phishing attacks. It usually starts with email and that email is sent to a large number of people. And so one of the clarifications in the registrar -- registry document is they take action on spam that is used to enable phishing, pharming, malware, or botnets.

I would like to hear from other panel members at this point on whether you feel that sort of general definition that's been talked about so far is too narrow or too broad and what you think the definition of "DNS abuse" should be.

Perhaps, start with Farzeneh. What's your view on this working definition of "DNS abuse"?

FARZANEH BADII: Thank you. At NCSG, we believe that the DNS abuse at ICANN should be defined in a limited technical manner and ICANN should not get engaged with nontechnical programs that fight with DNS abuse.

And what I am puzzled about is that we actually have the definition. The definition should not be perfect, but it should be limited and technical. So -- because we cannot fight with all sorts of DNS abuse that happens in the world just because the DNS has been used in some kind of crime. We need to look at it and see whether it is in the mandate of ICANN to actually fight with that abuse.

And so far I have not seen anywhere in any document that anyone can point me to a novel DNS abuse crime other than the ones that the

registries and registrars have enumerated and also we have them in the agreement.

I have not seen any kind of other technical DNS abuse that is out there that we have not considered. And I think that the problem that we have is not really in the definition. The problem that we have is that we have patchwork of solutions here and there but we don't have a cohesive governance mechanism to know.

We came up with a policy. We implement it. We enforce it. And then there is a dispute resolution as well for the ones that want to use. So that's all.

BRUCE TONKIN: Thanks, Farzeneh. Mason.

MASON COLE: Thanks, Bruce. First, I want to applaud the registries and the registrars for what Graeme talked about in terms of leaning toward action. I think we can -- we can spend a lot of time discussing what a definition might look like for DNS abuse. But in the meantime, DNS abuse is happening and it needs to be addressed today and not tomorrow while we sit and sort of quibble about a definition.

But to your question, Bruce, the BC published a statement last week about DNS abuse and we called out in that statement exactly what we think our belief about what a definition of abuse is, which is it's an action that causes actual and substantial harm or is a predicate of such

harm and is illegal or illegitimate or is otherwise considered contrary to the intention and design of a stated legitimate purpose.

Further than that, the most recent Registry Agreement did a good job of capturing at least close to what a technical definition of abuse might look like when they called out distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, and counterfeiting.

These are all good categories, and it's a good place to start our discussion on what an abuse is.

During -- the definition of abuse was further called out in public interest commitments in the Registry Agreement. And during the transition, the BC did as much as they could with the Board to work to protect those PICs.

We learned earlier this week there's some difficulty in ICANN in terms of enforcing -- in terms of what compliance can do to enforce those PICs. So we're distressed about that, and we're looking forward to having a conversation with the community about how that can be improved.

BRUCE TONKIN: Thanks, Mason.

Jeff?

JEFF BEDSER: Sure. Thank you, Bruce.

So just a disclosure, while I run a company, I'm also on the PIR Board. So I'm very knowledgeable of what one of the registries is doing and very proud of what PIR is doing.

And I'm also -- my company is the company that runs the domain abuse activity report system, or DAAR. So I do have some knowledge about abuse.

One of the things that I would like to -- to open up in the discussion about defining abuse is that we have an issue where at the end of everything we're calling abuse is a victim, right?

And there's a victim who is being financially injured, is being reputationally injured, or all types of other problems and trying to define abuse in a limited fashion that says, Well, these are the only types of abuse we think we're going to take responsibility for is a very ethical slippery slope -- to actually use that term, I apologize -- when we're talking about an ecosystem that has roughly 200, 250 registry operators. It has about 2,000-plus registrars. But when you are talking about content and hosting, there's hundreds of thousands of hosting companies.

And I've asked a lot of experts this week how many do you think there are, and no one can actually come up with a number more than a couple hundred thousand.

So when you are looking at a scale of trying to stop victimization and simply put continued victimization -- right? We're talking about a

situation where if you don't take action and it stays live, people continue being victimized.

I coined a term the other night speaking about this topic with Brian Cimbolic where I do believe that when you go to the registry level to take an action, you are literally looking at a nuke-able offense. This needs to be taken off the planet now to stop continued victimization. But not all types of content abuse or abuse need to be taken that type of action. It can be a registrar level, and a lot of times it should be the hosting company level.

So putting those skills together really helps you understand the issues and the losses and the victimization.

But all types content abuse or abuse need to be taken that type of action. It can be a register level and a lot of times should be the hosting company level. So putting those scales together really helps you understand the issues and the losses and the victimization.

Graeme?

GRAEME BUNTON: Just a brief response, you know, on that framework definition. And, boy, do I not want to continue arguing about definitional stuff.

You know, I've heard from a bunch of people this week that we went considerably too far and that was a mistake. I've heard from people that clearly stated we did not go nearly far enough, which, to me, in classic ICANN land, means we really nailed it.

And just, you know, really briefly, to the BC statement, what does legitimacy mean? I don't understand how I could ever police whether something is legitimate or not. To me, that's not a definition that allows us to continue taking action.

BRUCE TONKIN: So sort of touch on another point that's come out a little bit.

There was mention earlier, and the general topic is around proportionality. So what do you do when it's not everything to do with that domain name that's causing a problem? So if you have the spam email and it's an email address of a person's name at Gmail.com, most people wouldn't consider removing Gmail.com as being the solution to that. Or if there was bad content on YouTube, most people would say that it's not reasonable to remove YouTube.com because there's some bad content that someone's posted to it.

So this proportionality, the solution that's being proposed, we as registry/registrars can't do something about that. But, hey, you should talk to the hosting providers or you should talk to the registrant.

And in the earlier part of the presentations, there's quite specific requirements for registrars to provide an abuse contact, the registrar has to provide a law enforcement contact.

But that information is becoming less and less available for either the hosting provider or the registrant. And, in fact, traditionally, people have used the WHOIS service, and they used the WHOIS service to find out that perhaps the technical contact details of a particular registrant,

and that might be the hosting company. Or they've got the administrative contact details of the registrant. But that information is gradually disappearing, partly in reaction to privacy laws.

I'm interested in what the panel's view is, when you say, hey, I'm the registrar, but I can't do something, go and talk to the hosting company, how do you suggest that people are able to find the right contacts to actually get action taken against a domain name that's got some problem with it?

BRIAN CIMBOLIC: Thanks, Bruce.

So I just want to -- On the framing of the question, there is always a question of proportionality when you are talking about using the domain name system to address Web site content abuse. It's almost de facto disproportionate.

Now, that being said, I think that's not the end of the discussion. That's not the end of the equation. The opposite side of the same coin, to me, is the scale of harms.

So if -- it is typically disproportionate to act via the domain name system for something on a Web site. But if you're talking about something egregious, like child sexual abuse material, distribution of opioids online, things like that where there is palpable, physical human harm, then I think that this scale -- that analysis of balancing the proportionality of response versus the scale of harms, that's analysis that we take very seriously.

So once you're dealing with something as egregious as that, you know, yes, you should try and work through the hosting provider. Yes, you should work your way up and not start at the very top to address this. But ultimately, in those instances, we would take action.

BRUCE TONKIN: But to the specific question, though, I'm asking, when you've gotten to the point where you don't think you can take action and you think that the hosting provider or the registrant should do something about it, how does the community actually do that?

What are the tools available for you? 'Cause all I've got is the registrar contact and the WHOIS. So I can ring the registrar. What happens next?

GRAEME BUNTON: So Jeff is probably in a much better position to answer this than I am.

I think there's an interesting gap there where there is some opacity between the domain and the hosting provider -- and I'm certainly not a cybersecurity expert -- that there's probably some really value in having a conversation about how to make that more transparent and what are the tools that would be helpful for people in doing that.

Jeff might know them.

JEFFREY BEDSER: Yeah, it takes quite a bit of research and investigation. And there's actually been a lot of changes in the last several years. For example, if

you use a particular DNS provider such as CloudFlare, the way their system actually works is that it actually hides the hosting. So you've got to contact them to get them to prove to them they should disclose who the hosting company is to you so you can contact the hosting company.

And if they're not familiar with the term "bulletproof hosting," bulletproof hosting sounds like it's great for protecting you from denial of service attacks and such. But bulletproof hosting is also used quite a bit for "we don't respond to anything. If you contact us to take it down, we ignore your emails. Until someone shows up at the front door with a badge and some court orders, we won't take any action."

So in that process is -- how many days are passing between the first contact and the second contact, the third contact before you actually can get some type of action if you can get some type of action, if you can get some type of action.

So I think Graeme's actually made a great point, is, while they may be responsible for that content and that problem, there has to be a methodology we can come up with that makes it easier to find them so they can be contacted.

BRUCE TONKIN: Gabriel?

GABRIEL ANDREWS: When we're speaking of gaps and dealing with abuse reporting, I think it's important to also -- let's have an honest conversation about what happens when good reporting comes to compliance at ICANN, and ICANN takes the actions to notify a registrar, hey, we've got reports that this domain is being used for bad activity, and the registrar, let's just go hypothetical, says, yes, great, we're acting on those domains while taking additional registrations from perhaps the same registrant on a host of new domains that are also then reported for abuse to ICANN. ICANN pushes that back around, allowing the cycle to be perpetuated. And regardless of whether or not there is potential within contractual agreements to do more, without having some sort of mandatory tracking of how many abuse complaints are being tracked back to a single registrar, registrant -- there has to be some sort of three strikes methodology here, if you want me to give it just a name, to actually track repeat abuse behavior such that we don't get caught in this perpetual feedback loop of report, great, done it, taken care of, report, great, done it. Ad infinitum.

BRUCE TONKIN: Thanks. So what I'm hearing there from a couple of the speakers, that we don't really have a good solution for being able to contact either of hosting company or the end user as it stands today. And, in fact, it's getting more complicated. As Jeff pointed out, there are a lot of services that are designed to protect against things like denial of service attacks, et cetera. So it's just layers of Internet infrastructure typically between the registry and the actual end user. So it might start with the registry. Then there's a registrar that submits things to the registry.

Registrars have resellers that submit names to the registrar. Then the reseller might use a DNS provider, they might use a Web application firewall, that might use a separate Web hosting company. So in a lot of these cases, you're actually talking about perhaps up to sort of five, sometimes up to ten organizations involved in providing the service that you see when you're typing in a URL in your Web browser.

And then actually trying to get someone who will actually take action gets increasingly difficult, because a lot of the contact details are just not available. And all you're left with is the contact detail for the registrar. And so that might be something the registrars can contribute a bit more in at least providing better methods of contacting their resellers or contacting the hosting companies that are associated with registrations.

Another topic that -- sorry, Farzaneh.

FARZANEH BADII: I just wanted to make it clear that when we talk about content, we are not talking about anything that is related to ICANN or ICANN should be doing anything about it, because it's an ICANN plenary, and I think for those who don't know, in our bylaws, there are provisions that prevent ICANN from content regulation. And mixing the content layer with the technical layer is a very risky path.

So I think we need to be clear when we are talking about content regulation.

And about the registries and registrars and whatever action they take outside of ICANN, I think -- I think they should be able to take action. And there's no doubt about that. However, if they want to make it more legitimate, then they might want to be more transparent about the policies that they have and about the implementation of those policies and also have a due process mechanism that if, by mistake, they have taken something down, the user actually can dispute that.

So thank you.

BRUCE TONKIN: Yeah, that's a good question, Farzaneh, which is, really, what are sort of the rights of appeal or rights of come-back. Perhaps the registry or registrars can comment on that. Like, what -- How does a person that's had their name taken down do something about it on their side?

BRIAN CIMBOLIC: Sure. Thanks. It's a good question and one that we grapple with.

We're actually in the process of formalizing an appeal mechanism for PIR so that there will be an actual formal process by which a registrant that had his or her domain name or its domain name suspended as a result of our anti abuse policy will be able to have that revisited by a third party.

In the meantime, though, we do -- while we're building that, we get -- it goes through our abuse email, where a registrant will say, hey, this --

my domain name was acted upon. And typically, the -- we will reverse if there's a credible claim that it was a compromise case.

So we try and identify compromise cases before we take action. But every now and then, one slips through the cracks.

So if a registrant comes to us and it's -- there is -- again, it has to be a credible claim that their domain name was compromised, then we will reverse the suspension, which is another benefit of suspension versus deletion, because we can remove that lock at any time.

BRUCE TONKIN: Thank you.

One of the things that came up in the Competition Review Report -- there were a couple of suggestions there. One suggestion was that ICANN prioritize compliance if there's a large amount of abuse that seems to be happening at a registry level or a registrar level. And that's something this abuse reporting system can highlight, that they perhaps sort of do a deep dive on that particular registrar.

Another suggestion for improvement from the review team was that registries/registrars look at different financial incentives to incentivize good behavior.

Do any panelists have any comments on either of those two?

Gabriel.

GABRIEL ANDREWS: So as to not request Brian to toot his own horn, I do want to say that the action that is being taken by PIR is worthy of analysis and perhaps even emulation.

When you're talking about having a registry incentivize for all of their registrars, hey, if you take all of these steps to combat abuse on your platform, you might get a discount on your registrations, that's worth exploring.

Because, ultimately, we have to remember that the bad guys out there are incentivizing bat behavior with their patronage. They're buying domains. We have to put in place some forms of carrots and sticks if we hope to make a rational actor who might be more or less immoral actually consider doing the right thing.

I'll go one step further and ask if we want to also consider, well, what can we do to encourage the registries to encourage the registrars?

Final thought: For every carrot, there could also be a stick. And I don't think that any of us up here on the far right end of the bell curve in terms of abusive behavior -- but there are some who exist. What are the sticks also, the disincentives that might be employed for the truly egregious behavior? What can we shine a light on to help quantify, who are the good actors? Who are the bad? How can we shine the light such that some can actually take nourishment from it. And let's observe who flees to the shadows.

BRUCE TONKIN: Graeme.

GRAEME BUNTON: Thanks. This is Graeme.

So I don't think we've talked a lot about incentive programs. This is, I think, a reasonably new idea, or at least it is to me.

I think we would need to be exceptionally careful about how we define those, what those metrics are that we're basing those incentive programs on.

But registrars, in general, are in a very small margin business. And that's probably pretty interesting to registrars in general. So I think that might have legs to explore further.

BRUCE TONKIN: Mason?

MASON COLE: Thanks, Bruce.

I used to sit on the contracted party side of the table, so I'm aware that, you know, there's cost incentives and financial incentives that could be an attractive solution to this. I would applaud the idea of looking into that. I think that would be a wise thing to do.

I also think now may be a good time for us to take a look at the contracts again to see if there are ways to open up the contracts and have a look at whether or not improved contract language can have an impact on DNS abuse. Because, again, what we learned earlier this

week is, the contracts aren't really as strong as we thought they were. And now might be a good time to examine where there's an opportunity to strengthen those and give ICANN better tools to combat abuse.

BRUCE TONKIN: My observation of the contracts is they're pretty heavy on what I'd say the reporting. So the registry contract requires them to sort of collect statistics and report it and send to registrars. The registrars report their abuse contact. They need to do investigation.

But it's absolutely not clear what actually happens with the abuse report. You know, that language is much more loosely in both the registry and the registrar agreement. So it does feel like there's room for improving the contractual language, based on experience.

Is there any other suggestions the panel would like before I go to the audience? Any other suggestions the panel might have for practical things that the community or ICANN, the organization, can do?

Brian?

BRIAN CIMBOLIC: I just wanted to jump back to the incentive question. This is anecdotal, admittedly. But with our QPI program, we've seen registrars that aren't receiving an incentive that might not typically have been aggressive on abuse come to us and say, "How can" -- "Okay. We didn't qualify for this. How can we get better?"

Now, and it is -- and it's driven by the finance of it, which is fine. But I think that that same behavior could scale pretty well at the ICANN level. If a registry or registrar is incentivized to have a cleaner space financially, I think you're going to see a lot cleaner space.

BRUCE TONKIN: Just to be clear, on the financial side, it's kind of a bit of a chain. So there are fees that the registry charges. There's also fees that ICANN charges. There's fees that registrars charge to resellers. So there's a bit of a chain. So the financial incentives are a broad thing that can actually be attacked at various parts of that chain.

Farzaneh.

FARZANEH BADII: I think that the incentives discussion is good. However, we need to be careful when there are, like, incentives -- where you are incentivizing a registrar to take more content down, then they might be very overzealous and they might be unfair on some of their registrants.

And this is -- we are being very outcome-oriented. Oh, we took down 2,000 domain names, and, yay. While I think that we should be a little bit more process-oriented.

We have the mechanisms and the redress and everything in place, and we can do something about abuse, DNS abuse, when it happens. I think that should be more of a goal than this.

And just to make the environmental a little bit more flowery and nicer, DNS and -- as a part of the Internet, we used it to be globally connected. It brings prosperity to our life every day. It's not only to commit crime. And it brings prosperity to a greater extent than it brings misery. So let's remember that.

BRUCE TONKIN: It's always good to be reminded that the Internet is -- overall, is still a force for good.

Brian.

BRIAN CIMBOLIC: Thanks. Farzi makes a great point. And I think, to clarify, I was speaking specifically about DNS abuse, not Web site content abuse.

In the programs that we work with trusted note fires with, we're still talking about a small number compared to the -- the overall number of domains acted upon. So we -- year to date, through Q3, I'm sorry, we've suspended 28,675 domain names. The total of those that were related to content were eight. So it's a small number. And it's a good story in that -- So the majority of that, six of those eight, were related to CSAM. But we've had over 1100 referrals to us from the Internet Watch Foundation. So that means we're actually getting remediation, which is exactly what we want. We don't want to have to act at the domain name level. So we're getting the problem taken care of. And so that the content is -- it's a small number in the much, much larger subset for DNS abuse.

BRUCE TONKIN: Acronyms, CSAM is relating to child abuse material, for those not familiar with the code that's used around here.

Gabriel.

GABRIEL ANDREWS: Farzi, I think your comment regarding processes is a good one. Yes, there's a lot that can be done there. And while I'm onstage, I would like to call out several good practices we've observed within the ccTLD space.

Some of you might have seen this in previous conversations. But we saw that EURid, in particular, they have a process by which they look at the registrations of domains and they try to block those look-alike domains. Remember on the business email compromise I showed you that there was, like, a bad actor-controlled domain that looked a lot like the victim domain. That's something that can be done as a process at the registrar level that is being done by some.

There's an additional process by which they're using past reports of abuse as a correlation mechanism to identify abuse in realtime.

The best predictor of future behavior is past behavior; right?

Those are something that should be applauded. To the extent we can incentivize them, I think it makes a lot of sense to incentivize. I think --

BRUCE TONKIN: Graeme?

GRAEME BUNTON: Very briefly, this is Graeme. I wanted to thank Farzi for that piece there, because I think it's really important, especially if you're investigating incentive, that you can't do that in a vacuum. That you would have to have appeals mechanisms and transparency as a part of that so that it's a robust process so that we don't end up with outcomes that are problematic.

Thanks.

BRUCE TONKIN: Jeff?

JEFF BEDSER: Yeah. And I think one of the incentives doesn't need to come from ICANN policy. One of the primary incentives here is, it's a market differentiator to have a business that has a very clean ecosystem, has good neighborhoods where you're not associated with abuse.

That's one of the things that as Graeme and Brian both pointed out, they don't do enough to trumpet the work they're doing, because in many of the organizations that participate here, the differentiator of what they're doing should drive customers to them, versus the bad actors who don't participate in the ICANN community, who aren't here, but are in the business. So some of the incentives can simply be doing the right thing can be its own reward and can be a financial incentive.

BRUCE TONKIN: Okay. We're about halfway through, and I said we'd make sure we provided a lot of opportunity for audience participation. So I'll start at the queue here, Mark.

MARK SEIDEN: Mark Seiden, for the record.

So we have a very blunt hammer here, and we're at the wrong place in the food chain to actually do enforcement.

Really, as a practical matter, only the people who have visibility on content can do any kind of content-based enforcement. And that mostly means hosting providers and antivirus companies.

So I urge you -- In fact, it's practically impossible for us as registrars/registries to do investigations of some of these reports. We don't have access to the content, when you get right down to it, and sometimes we can't even reproduce the reported problems.

So I urge you, before turning off a domain, to go to the way-back machine, look at the history of the domain, and try to understand what -- what's going on with it before we invent these systems which are so flawed, and perpetual an extremely blunt hammer.

Also, whatever we do should not train the adversary. An example of domain generation algorithm actions is just prevent them from blocking -- prevent them from registering any domain in the DGA.

It would be much better if we took their money and then we denied them service, thereby causing them financial harm and getting a little revenue from them.

So, you know, I urge you not to train the adversary, because they'll just go somewhere else or change their DGA, which they can easily do.

BRUCE TONKIN: Good suggestions, Mark.

Elliot.

ELLIOT NOSS: Thank you, Bruce. Elliot Noss from Tucows.

We've been talking now for, you know, 45, 50 minutes this morning, and for 20 years, on this topic.

There is great progress in seeing that, you know, here are six panelists from six different points on the star, and you are all in violent agreement from -- to my ears.

There was one line buried in this whole 45 or 50 minutes that I believe is the most important line in terms of actually making progress in 2019 and 2020. That was when Mason said, "Well, compliance is having problems enforcing the PIC spec."

I was struck from the very beginning of this panel as Gabriel laid out three examples, three egregious examples, of DNS abuse.

Every one of them is acted on by responsible registrars. I believed that. I believe that to be the case for well over a decade. I checked with compliance in our shop before I got here.

So now we're down to the age-old good registrars/bad registrars, people who are here/people who are not problem. I am tired of this. I've been tired of this for years. I've been saying that in public forum for years.

Let's act.

The most important member of this panel that could contribute to moving the ball forward is not on it. And that is either Jamie or John Jeffrey, or both, to explain why compliance is unable to enforce what I think is inside the four corners of the existing contract.

I want to be sympathetic to them and to that position, and I think we need to bring all of our community efforts together because you all have just agreed, you know, for better or worse. That is where we all need to take all of our efforts and energy in the immediate term. We have a framework from the community. And I want to note as I did yesterday briefly in the Board and contracted parties meeting, it is not necessarily about people who are here and not here. We talked about incentives. Today, there are clear financial incentives put forward by registries, well intended, that incent bad behavior. That's inside of our community by people that are here at numerous ICANN meetings.

This is not unknown.

We need to deal with the issues that are in front of us. If compliance is able to effectively identify that there are specific elements of the contract that will help them enforce very clear bad acts that we all know are in existence, then let's talk about those. I don't believe they need those. I don't believe they need anything additional to what's in the current contracts, but let's talk about those. And let's get on with that specifically. Compliance dealing with known bad actions that we all agree should be dealt with.

Thank you.

[Applause]

BRUCE TONKIN: Thank you, Elliot.

If I can take an online comment or suggestion.

REMOTE PARTICIPATION: We have -- we have four comments and two questions.

The first two comments are from Maxim Alzoba: DAAR contains false positives, no evidence, and does not give any actionable info to registries. No domain names, just numbers.

And the second comment is: Please be aware that the requested fast takedown and lack of due process for registries and registrars, termination of the contracts, will be used by criminals for blackmailing

of the contracted parties and will undermine stability and security of the Internet.

The second comment is from Andrew Campling: Please do not let definitions and remit squabbles get in the way of action to reduce crimes and other harms committed through DNS abuse.

And a comment from Michele Neylon: Abuse is an issue that impacts the Internet ecosystem. There's no doubt about that, but it's an issue that industry is in a much better position to resolve than adding more insane obligations into our contracts.

And we have a question from Sivasubramanian Muthusamy from India. Question: What is all this artificial boundary on ICANN's mandate or only the technical aspects? If ICANN restricts it's attention only to abuse in registered name space, the abuse occurs in the numbers space, without a registered domain name, is left unattended, which leaves a proportionately large portion of abuse turned a blind eye. If IANA is part of ICANN, how does this form if DNS abuse outside ICANN's mandate? In fact, ICANN is the only organization that has the required technical understanding and capabilities to competently address abuse that occurs outside namespace, and even abuse originating from the Dark Web. What is it that makes ICANN resident?

And the last question is from Andrew Campling: The DNS ecosystem has been highly decentralized and collaborative. With the advent of encrypted DNS through protocols such as DoH, will the centralized resolver operators like Cloudflare be required to scan for abuse and

share the resulting intelligence or will they instead look to exploit that intelligence for commercial gain?

BRUCE TONKIN: So the first question, where does the mandate come from, it flows, starts with the bylaws. Then ICANN, which is a private sector organization has contracts with registries and registrars. They, in turn, have contracts with end users. So that's the flow. And so what Farzaneh is talking about is essentially the limitations in the bylaws that flow through.

FARZANEH BADII: Also -- Farzaneh speaking. Also, when we talk about cybercrime in general, and one part of the crime is facilitated through using the DNS, this doesn't mean that everything related to that crime has to be solved through an organization like ICANN. And it is a very risky suggestion to say that we use this forum which is a centralized organization, we use this forum for all of the DNS-related problems, for all the crimes that happen, and that one part of it is usage of the DNS, then we are going to put in danger the open, global, interconnected Internet.

BRUCE TONKIN: And then the second question, then, there was mention of a particular service provider, and do they have to contribute to abuse filings. It kind of relates to the point we were making earlier that there's quite a long supply chain. And what people are saying, you need to get to the part

of the supply chain that's closest to the problem. And a lot of that is about sort of getting the contactability of the right party right, I think.

I don't want to have a long discussion on each point, because then we won't get a chance for everybody to comment.

So, Alan.

ALAN GREENBERG: Thank you very much. Is this on? Yep.

My comment is going to follow on an alias pretty closely with one somewhat different perspective. The kind of work we're hearing about here from Graeme and Brian is really encouraging. Not that there wasn't action being taken before, but doing it in public and encouraging other registries and registrars to do is really positive.

I was interested to hear Brian's -- Mason's comments on PICs. We've been hearing for decades that, yes, we know there's a problem, but we don't have the tools, compliance doesn't have the tools to do it. In some cases, I suspect Elliot is right, that there are clauses in the contract which could be construed as enforceable, but compliance has said, you know, in practice, they can't really use them in an enforceable way. You know, it's not as easy to remove someone for those clauses as for nonpayment.

I've heard comments that the DAAR report is important and useful, but it's OCTO. It's not compliance.

What I want to see now is all of the parties getting together at the same table. And if, indeed, compliance needs contractual changes, let's get everyone to agree on them and put them there. Let's make sure that the artificial separation between OCTO and compliance does not stop us from using information that is useful and valuable.

We can -- we can do something about this. And as Elliot pointed out, it's really easy to say the bad actors aren't at ICANN. Some of them are.

So let's stop pretending and act on things that we can act on.

Thank you.

BRUCE TONKIN: Thank you, Alan. Another one from the audience. Stephanie.

BRIAN CIMBOLIC: I wanted to touch briefly on something Alan mentioned about outreach to other registries and registrars to work on something like the framework to address abuse.

We are just to open call to registries and registrars in the room, if you've read the framework to address abuse and think it's something you would implement, we are adding signatures for people that are going to be committed to living by what's in that document.

So the more the merrier. We've got a number of country code operators that are involved at this point, too. So hoping that people can sign on.

Thanks.

BRUCE TONKIN: Stephanie.

STEPHANIE PERRIN: Thanks. Stephanie Perrin from Noncommercial Stakeholders Group. And I came to the mic to endorse what Farzi was saying. There's a word she didn't use, and it's one that we care about in the Noncommercial Stakeholders Group, and that is "shadow regulation." Any move that ICANN makes to financially incentivize what is considered good action amounts to shadow regulation. And we're deeply concerned if it strays over that bright line that ought to exist between technical abuse and content abuse.

And we know that there is a global pressure right now to address content abuse across a range of particular kinds of abusive content. But, please, I beg you, stick to the technical abuse, because you've got plenty of work to do there. And I think I endorse what Elliot was just saying. As long as that bright line is protected and ICANN does not get into the business of financial incentivization through contracts which is outside the multistakeholder policy development process.

Thanks.

BRUCE TONKIN: Thanks, Stephanie.

So what I'll do -- I know panelists are probably keen to comment on each person, so I want to make sure I get through the queues, and then

I'll go round the whole panel and you can comment on anything you've heard, basically, in reflections.

So next.

DIRK KRISCHENOWSKI: Yeah, Dirk Krischenowski, vice chair of the GeoTLD Group. I'd like to make a comment on behalf of the GeoTLD Group.

All of our members have contracts with their governments which include various public interest obligations, including abuse as defined by the national law. Last year, we have done a GDPR survey that showed that geo TLDs manage the very few requests very good.

I'd like to -- today, I'd like to give notice that we were conducting a DNS abuse survey with 22 geo TLDs over the last 12 months. Yes, there is abuse in geo TLDs, but very little. Only three members have more than ten cases within the last year. We will publish the results of that study very shortly, but I'd like to notice that regarding the current discussion, we think there is no need for further contractual obligations. And I can quote Tucows on that. And even there's no need for unified access model which I heard is also named the system that rules them all.

Thank you.

BRUCE TONKIN: Thank you, Dirk.

If we can come back to an online.

REMOTE PARTICIPATION: This question -- excuse me -- this question is from Andrew Campling: My question about the impact of encrypted DNS was misunderstood by the chair and not answered. The DNS ecosystem has been highly decentralized and collaborative. With the advent of encrypted DNS through protocols such as DoH, will the centralized resolver operators be required to scan for abuse and share the resulting intelligence or will they instead look to exploit that intelligence for commercial gain? If not, how will the registrars and registries know where the abuse is occurring?

BRUCE TONKIN: Jeff, do you want to comment on that briefly? There was a question.

JEFF BEDSER: I have to give a think on that one. I don't have a direct response to that.

BRUCE TONKIN: ICANN doesn't have a contract with the DNS resolver to start with, so it can't compel them to do anything, but clearly there is -- they are part of the ecosystem. I did understand the question. That's a question of how you resolve it.

BYRON HOLLAND: Byron Holland from CIRA, the ccTLD operator for .CA. And thank you for getting this conversation really going. I appreciate the conversation.

But I have heard a lot of violent agreement up there with perhaps the exception of Farzaneh, who I think has made a great few points.

I want to make a couple of comments, though. I know there's at least one lawyer up there and at least one deep policy thinker. I'm sure there's more. Let us think about the notion that let's just get on with it and the dismissal of definitions.

Words matter. And as lawyers and policy thinkers, we know words matter. Otherwise, we're going to end up running wildly off in multiple directions. So let's make sure we nail the definitions.

From my perspective as an operator, the notion of that -- what Stephanie just said, the bright line between technical abuse and content abuse, that matters, and how we define it I think will be of critical importance for the success of creating clean spaces, which we all want, though we may differ on implementation.

I think we also need to pay close attention to the ICANN bylaws, which I think speak pretty clear on where their remit starts and ends. And content abuse, I'm going to argue, is probably over that line.

The other thing I would say is let's look at where in the stack the issues are and where the regulation rules or actions are going to be taken. If we in the DNS operate in the second, third layer and content is riding at the absolute top of the stack, I think we need to be careful about where we regulate and where we act to affect what layer of activity is actually the problem.

And for those of us, and there are many in this room, who fought a lot of Internet governance battles, a lot of them have been about regulation and legislation at the right layer. For all of those in the Internet governance space, let's make sure we don't suddenly, ourselves, go and breach all the things we have been talking about over many years in many forums and many global forums.

And then my final point is a lot of the comments made around individual actors acting, I think there is clearly some space for that, but let us remember that judicial oversight is not a bad thing. In rule-of-law countries, having third-party, independent, judicial oversight that gives us permission to do these things, those aren't bad words. Judicial oversight, they are not bad words, and we shouldn't just dismiss them out of hand because we want to act immediately.

Thanks.

[Applause]

BRUCE TONKIN: Thank you, Byron.

Bill.

BILL JOURIS: Yes, this is Bill Jouris, I'm a member of the At-Large stakeholder group.

The gentlemen from the registries and registrars were talking about what they do to fix problems when they're identified. And I'm

wondering if you'd considered what can you do to keep them from -- problems arising in the first place. To take the easy example that got tossed out, if you knew that EZIAET was going to be registered and said that's going to cause confusion and didn't register it, the problem never arises. Now your obvious question is so how do we tell what will be confusing?

Well, good news and bad news. The good news is ICANN through the internationalization of domain names' effort is compiling long lists of characters that are confusable. So you can simply feed that in. The work to identify them is being done for you. It's not a complete list probably, but it will get you a long step down the road.

The bad news is ICANN publishing those lists. And anybody doing a domain name generation algorithm no longer has to guess what will confuse people. We're telling them.

Personally, I think mandating using those lists ought to be in the contracts, but however it gets done, I think it's something that the registries and registrars need to do by way of prevention.

Thank you.

BRUCE TONKIN: Other comments?

GRAEME BUNTON: Can I jump in on one? Sorry, Bruce. I think the devil is in the details and just feeding a list into a system to prevent registration I think is a

substantially more complicated problem than we might think. And I think the idea of doing sort of pre-crime on domain names runs into the same concerns that Farzaneh expressed with incentive programs where we may be doing more damage that we just don't know about.

So I think there's real risk to that and we would really need to think about it more.

Thanks.

BRUCE TONKIN: Yeah, one thing that some of the CCs are doing is they are using predictive software to identify issues. That doesn't necessarily stop the registration but it can identify something that's worth further investigation, perhaps asking for information as to why that name is registered and things.

So I think there's more than just stopping a registration but there's also using as indicators as to whether something needs investigation.

Next speaker.

NEIL SCHWARTZMAN: Hi, I'm Neil Schwartzman. I'm the executive director of the Coalition Against Unsolicited Commercial Email. Interesting discussion. Welcome to Montreal, everybody. This is my home town, and (non-English word or phrase). We're hearing the same discussions over and over: Oh, let's worry about the Chinese blogger. I'm here to provide a little bit of context from my personal perspective.

Up until the end of August, I had my hands deep into the abuse that was happening on the DNS, with the DNS, of the DNS, for a little hardware manufacturer that makes these (indicating).

We saw no fewer than -- and 28,000 is a nice number. We saw 30,000 phishing attacks per month involving 90,000 assets. I personally took down 50,000 in a month.

So when we talk about the efforts, and maybe we need better definitions, it's 50 years on since the Internet started. What's keeping the definitions from being defined?

It's time to move. I'm not saying move erratically or irresponsibly. I understand the process, but it's time to put some effort into it, some concerted effort, because it is a crisis when there is going to be anonymization of IP to IP. When there is effectively anonymization of who owns an asset such as a domain, you're talking about free rein to criminals, and they are making huge use of it. APWG, the Anti-Phishing Working Group, does not even begin to approximate the number of phishing attacks, with all due respect to the folks that actually try to do it. So much is not actually reported, because we don't have the time.

Abuse is a cost center to every one of the registrars and registries here, so they are incented not to put money into it. That's the incentive right now, is it's the opposite.

I agree, we should not incent people to set up fake systems, put a bunch of domains into play, and then abuse them so they get money. That's not the way to do it. The way to do it is to deal with the actual

problem that's happening now with proper reporting and accurate reporting.

I will say this as another point of context. One of the biggest registrars that has a massive hand in the phishing problem -- not by virtue of any malfeasance -- they have three people working on the phishing team. One of them just had a kid, so that's two people, full time. That's not nearly enough.

We need -- And that's just phishing. We're not talking denial of service, spam. One spam -- as you said accurately, one person's spam and another person's marketing. We won't even go there. We're talking about stuff that will deride and erode consumer confidence in the Internet and that's why we're all here, is to protect the end user.

Thank you.

BRUCE TONKIN: Okay. Next.

PIERRE BONIS: Thank you. Pierre Bonis, AFNIC ccTLD .FR for the record.

I would just like to, echoing what Byron said, ask ourselves why we are talking about that today, because abuse is not new. Technical abuse is not new. And by the way, this is in the contract.

I think that we are talking about that today because there is more and more pressure, legitimate one, from a lot of stakeholders outside

ICANN, say governments but also some civil society organizations, that are fed up with, I would say, digital players telling them, oh, we cannot do anything.

So huge platforms, huge search engines have said that to the governments and to a lot of players for years and years and years. And when we try to say that there is a technical layer that we are in charge of and there is a content layer that we are not in charge of, no one listen anymore because they have heard that kind of sentence for decades by people who were in charge of content.

So I think it's very important not to import the responsibilities of hosters, platforms into the DNS industry just because people are fed up of technical explanations.

If we go down the path of trying to do something about the content to make sure that people see us as responsible players, at the end of the day we will not be responsible because we will do the job of the judges or the police, which is not our job, not because we don't want to do it but because this is not democratic.

So, really, this call to action is very nice, but I think for the better good and the general interest, we really have to be very cautious and to say that we can do something on the technical layer, but there is a huge risk of bringing us looking at what is a good or bad content.

And just to finish, this is true at the national level for a CC like .FR, but this is even more true at the global level for an organization like ICANN, because of course no one -- no one thinks that an organization being

global and multistakeholder can have a definition of bad content that can comply with all the international jurisdiction and that would comply with all the cultures, by the way.

Thank you.

[Applause]

BRUCE TONKIN: Just in the interest of time, if we can try and keep -- they are very good pieces of feedback. But I want to get through the whole queue.

So if we can just keep the presentation shorter.

Next speaker.

TOM LAM: I'm Tom Lam from CloudFlare. A question and a couple of comments, since we came up twice already.

On the incentive programs, would the registries provide registrars with a list of domains that have been registered and deleted within -- within the one- to five-day time frame? Using that list, if registrars choose to sign up to black list those registrations, you know, registries could incentivize the registrars somehow for the other good domain names that they do allow through. And, of course, registrars would need to develop some sort of method for legitimate customers who get caught up in that sweep, that they can contact the registrar and, you know, go through the registration process that way.

My comments regarding CloudFlare being a bulletproof host, we are not a bulletproof host. We do provide hosting contact information. And we do provide origin IPs to trusted reporters. We do have a program for that. So, you know, if anybody is interested in that, please feel free to reach me or contact us. We're happy to discuss that.

We don't share your information. We drop it immediately. So, you know, there should be no concerns of us sharing or selling your data. We are working on addressing the issue of malware with (indiscernible).

BRUCE TONKIN: Thank you.

Next speaker.

DEAN MARKS: Dean Marks. I'm with the Coalition for Online Accountability and vice president of the IPC.

I wanted to -- I'm also a lawyer, so I want to just respond to some of the comments about shadow regulation, the very important role of a justice system, an independent judicial review, to remind folks also that for every registration, there is a contract between the registrant and the registrar. And that contract has obligations that flow both to the registrant and the registrar. And, in legal terms, if there's a breach of that contract, the registrar is legally entitled to take action, including, in many of those contracts, the suspension of the domain name.

If the registrant believes that that contract has been violated, of course judicial review is appropriate.

So I really don't see where there is shadow regulation.

I want to say to Farzaneh that I agree with you, that I think if there are these frameworks in place with registrars and registries to suspend domain names, there should be an easy way for a registrant to go to that registrar and registry to say, "I think you've made a mistake in suspending my domain name." Without having to go to court.

So I do embrace that concept. But I wanted to thank the folks who have put forward this framework for addressing abuse. I think it's important. I don't think all responsibility lies on the domain name system. I think it needs to be spread across all sorts of platform operators. But I think it's a great step forward, and I want to express my gratitude and the gratitude of the IPC.

And also, just finally, one point.

The framework talks about trusted notifiers. I think that's a great concept. When I worked for the motion picture association, we put them some trusted notifier arrangements with (indiscernible). I think they work well. And I wanted to invite anybody who's interested in those arrangements, please come talk to me.

And thank you.

BRUCE TONKIN: Milton.

MILTON MUELLER: Yes. Milton Mueller, Georgia Tech.

I felt compelled to make a comment at the mic, because I had this real nagging feeling that the fundamental issue that we're debating was not being identified properly. And we need to frame this issue quite differently than is being framed.

So the question that you're starting out with here is, what should we do about DNS abuse. And that, of course, leads naturally to, what do we mean by DNS abuse. And then we have a debate about how much of the content-related stuff is included under the rubric of DNS abuse.

And I think that's kind of the wrong perspective, because the people who are advocating for a more expansive definition of DNS abuse are sort of pretending as if we don't define it as DNS abuse, then nothing will be done about it. Okay?

And so when we're talking about content-related things, let's take child pornography as an example, that is unbelievably illegal in every jurisdiction in the world. And there are incredible mechanisms for reporting and taking down child abuse that are in place that have nothing to do with ICANN or the domain name system. Right?

Same thing with copyright infringement. We have global treaties. We have -- anybody take a look at what our ICE has been doing, immigrations and custom enforcement. Don't ask me why they're dealing with copyright enforcement. But they are incredibly active in taking down things all over the world. And, of course, there are other

jurisdictions that are doing the same thing. So it's not like if we don't define this as DNS abuse, it's not going to be stopped or attacked legally and politically.

So the question I think you should be asking is this: Is, when is a problem with the DNS so immediate, such an emergency, that we have to bypass due process and have the registries and registrars deal with it directly. That's the question that you're really debating here, is when do we want to make registrars and registries the judge, juries, and executioners of policy matters related to content?

I can see some justification for that in certain kinds of cybersecurity, spam-related, phishing-related things. I see no justification for that in content layer things.

Thank you.

[Applause]

BRUCE TONKIN: Thank you, Milton.

James.

JAMES BLADEL: Thanks. James Bladel from Go Daddy, one of the 11 companies that helped to develop the framework on abuse.

And I just want to respond to a couple of comments. One is that the framework is really not all that new. For the most part, those practices

that are described in there have been going on for years or decades. They represent maybe perhaps a lifting of the veil of what's already occurring at registries and registrars, and an attempt to, you know, help raise awareness and educate the rest of the community on what's already taking place.

But I wanted to zoom in on something specific that you said, Bruce, 'cause there's a lot going on here. But I think you had something earlier on about if the hosting provider is the most appropriate entity to deal with content abuse -- which I think we agreed that that's where content abuse normally needs to be addressed -- then how do the -- what are the registrars doing to make sure that those contacts are being made available to complaints?

Sometimes that's very easy, because we are also the registrar and the hosting provider, and we can take action under our hosting agreements and terms of service, and it provides much more flexibility and room to act than any of our contracts with ICANN, and it's a lot faster.

In some cases, we know who the hosting provider is or we can have a clue, and so we can send the person in that direction.

But beyond that, I think it's wrong to assume that the registrars have any idea who the hosting provider is or how to contact them. There's a number of cases where these things are just going off of our network, on to someone else's network, and we are just as -- I don't want to say "clueless," that's not the right word -- but we're just as much at square one in terms of researching how to reach out to those folks as anyone else. And I think perhaps we can look at other resources that are

already under this roof -- I'm thinking of the ASO -- at providing some different tools and directories that fill in those gaps. But assuming that the registry and the registrar have some privileged information that they're not sharing about how to contact those off-network hosts, I don't think that's a correct assumption. So I just wanted to challenge you on that point.

BRUCE TONKIN: Just to be clear, James, I wasn't necessarily implying that you have that information. I was just saying that the information is not available.

Next speaker.

LUTZ DONNERHACKE: Lutz Donnerhacke, EURALO, At Large.

What we're discussing here is what's in the remit of ICANN. And if I understand correctly, most of the issues discussed here are contracts. So if there is a possibility to see on which contracts registration was made, it would be easy for the law enforcement agency to find out who is responsible.

Without putting too much energy to the registrars gathering the data and putting in a large database, you can go down the contract chain, follow the chain. Because the contract needs to be maintained correctly. Not the registration. Registration's (indiscernible). Most of them, it's automatic. Nobody cares about contracts in real detail. But

the contracts between the registrars, registries, these contracts are always in place, and they have correct data.

So my question is, why dot not publish the contract chain for each registration?

For instance, using a WHOIS as much as, a thin WHOIS service and forgetting about GDPR.

BRUCE TONKIN: Okay. Thank you.

On this microphone. Yep.

KATE PEARCE: Good morning. Kate Pearce. I'm on the board of dot NZ, speaking individually. I'm also a chief information security officer myself, so I'm on the other side of a lot of this. And I'm also on the board of a big security trust group in New Zealand.

A couple of points.

I'll slow down my speaking. Sorry. The New Zealand accent can get a bit intense.

Okay. So a couple of quick points. The first one is that domain age matters. The majority of issues we see are in very recently registered domains. And the majority of the harms we are most concerned about occur in aged domains. The harms are less likely to occur to the same

impact in the first few days of registration. We need to remember that, whatever we do, at whatever level.

But another thing is, we talk about shadow regulation. It is already happening in resolvers. It is happening a lot, particularly in the enterprise and government space. There are DNS filters. And whether you see that as protection or censorship, it is happening.

And maybe that's right. But what the result of that is, is that a lot of these smaller list resourced organizations and individuals in this world do not get whatever protection or censorship that offers.

So for many of them, this may be the only point of contact, particularly with fast-moving hosting.

BRUCE TONKIN: Thank you. David.

DAVID CANE: Hi, David Cane, Noncommercial Stakeholder Group and also a security professional.

My issue with the term "DNS abuse" is it always sits there and goes, what is DNS abuse. And its -- its definition is more or less when you -- something involving the DNS happens that is bad. And that is not a -- I mean, I -- I know arguing about the definition is there. But it still always relatively comes down to that. And that sort of bundles a whole bundle of things in together that are quite disparate. And some of them are very clearly within ICANN's remit as security and stability issues. But

even then, bundling a few together doesn't necessarily get you the best result.

I mean, for example, for botnets, you don't want to just remove all the possible domains that a botnet might reach out to. You might want to, you know, take -- might want to actually take over a botnet, command-and-control, and shut it down is a very common technique. That that can't be done just by a normal mechanism. You've got to grab a domain that hasn't been registered yet.

So with -- even though those things are all clearly within ICANN's remit, bundling them together doesn't get you the best result.

But there are also things in here that are clearly content issues. The fact that the content is un- -- you know, unarguably awful and illegal and no one is going to defend the specifics of it doesn't change the fact that it's outside ICANN's remit.

Now, we -- but it also -- the fact that it's outside ICANN's remit doesn't mean we shouldn't do something about it. Clearly, these are significant, real vital issues that we need to do something about. The question is, how do we sort of -- and both of those sort of positions are sort of well established. And it's great that there is a -- you know, a concerted effort to have a concerted response to some of these issues. But we don't need to sort of forget what we have learned from ICANN, which is that some of these issues, there are a lot of policy subtleties to it. Even on content that seems awful, there are -- you know, there's -- there are a lot of details in there. And sometimes -- I think even when we do go, okay, this is a content issue which needs to have a response.

And because it's an issue that needs a response, we have to do it outside ICANN, and this is what we're doing. We should still strive not to forget what we've learned from ICANN, that, you know, often the policy issues get complicated. We -- that people from completely different perspectives will notice issues that you don't realize.

Maybe we need to sort of think about how to take the lessons outside ICANN when we're building processes that will deal -- in a good -- in a concerted response to some of these issues. Maybe we need to think about, you know, how -- how we do multistakeholder policy development as a model outside ICANN and outside ICANN's complicated ecosystem.

Thanks.

BRUCE TONKIN: Thanks, David.

So the last two speakers. So Werner. Short so we can get to lunch.

WERNER STAUB: Werner Staub from CORE Association. I speak in a personal capacity.

We were talking about how to chase down bad domain names or abuse domain names.

Imagine just for a second we were not talking about domain names. Suppose we were talking about forgeries of bank notes and we were talking about accrediting operators of printing presses so that they

would not be producing or allowed the production of forged bank notes.

I think that in that kind of reflection, you would think of a second way, not to say that you shouldn't do the first. But what about improving the bank notes? Instead of saying we chase down the forgeries, we could improve the features that enable us to recognize what is a good one, not what is a bad one, the good ones paragraphs and this is actually our industry. That is where we're supposed to work. This is actually value added. So it just strikes me we've been engaged in a race to the bottom in terms of quality of registrations. Everybody wants to make it cheaper, make it less checked, and so nobody wants to have anything checked.

We get complaints from customers who positively want to be checked. They just ask for a way to be able to show to people and machines -- and machines -- that this is a verified registration. This is a business opportunity for registrars. It is a business opportunity for registries. It is a way for new TLDs to distinguish themselves. It is actually a positive way and a virtuous circle of incentives that will help us sideline the bad ones if you make it easier to see the good ones.

BRUCE TONKIN: Right. Thanks, Werner.

Last topic. Last speaker. Sorry.

ROB HALL: Sir. Rob Hall of Momentus. And I know I've been away for a while, but I thought you'd still recognize me.

I'm a little frustrated, because I think what we talk about is DNS, and we use that acronym to cover all things. But it actually is the word "system." And I think most of what we're talking about is the abuse of the use of a domain name, not our systems, and not the entire ecosystem. And let's not forget there's many other systems in this that when we talk about DNS abuse that we don't seem to be talking about.

And one I'd like to ask the panel or have the panel start thinking about is one of the abuses we've seen from registries and registrars over the years is the constant pounding and mining of our WHOIS systems, which are also part of the DNS systems. And we're about to put in a new system, RDAP, and I'm wondering why we haven't been discussing how the stop the abuse of that and historical record keeping and the data mining and the privacy abuse, if you will, of our customers.

I want to make sure we're not just focusing on what people think is one customer registering a domain name and abusing the use of that in their minds. Let's start talking about our entire ecosystem again and the services that we often forget about because they're not a hot button of the day.

Thank you.

BRUCE TONKIN: Thanks, Rob.

So just to close out, I'd like each panelist, if they've got any sort of general comments or messages that you want to leave the audience.

So starting with Gabriel.

GABRIEL ANDREWS: Well, I'd like to thank all the commentary. It's very interesting to see the bright swap of views. And I think it's educational for someone who's only at their third ICANN. So thank you.

For final thoughts, I think there's a general recognition that there is -- there is the potential here to find common ground on addressing some of the -- the most harmful behavior that exists in our ecosystem.

And we can -- we can speak to definitions. We can speak to trying to find these exact terms. But I will caution that the criminals are clever. The abusive actors are creative. And if we get to be too prescriptive with trying to identify every possible means of abuse that exist, we could potentially get caught down with our pants down with those that we fail to predict.

Nonetheless, there is genuine benefit to recognizing that there are good drivers on the road with us and responsibility still enforcing the rules of the road.

BRUCE TONKIN: Farzaneh.

FARZANEH BADII: So, two points. One, I don't think that -- and this came up about Cloudflare hiding the host, and I don't think that anonymity and a little bit of kind of like people being able to conduct actions and have like websites and express their opinion on the Internet is necessarily a criminal -- they can be like framed as a criminal in the end. So not everyone who wants to hide things or be anonymous is necessarily a criminal. And we need to think about them. And we shouldn't -- I don't think that we can just outright say, oh, but we should just put the whole contract and chain of the registrants on the Internet and identify the registrants. Our civil liberties are at stake as well.

The other thing that I want to clarify, and I think I was not clear in the beginning, we agreed with some of the ICANN-related DNS abuse that you mentioned in the framework, but we do not agree with the rest of the matters that you want to do as registries and registrars such as taking down content because of opioid and stuff like that. So that's something I needed to clarify.

Thank you.

BRUCE TONKIN: Brian.

BRIAN CIMBOLIC: Thanks. Yes, I think my take-away here is that there's a lot of registries and registrars out there that are doing their best. They're taking steps, even ones that they're not contractually required to do to try and address DNS abuse issues. But to the point that Farzi has made, and I

think is right, just taking down abuse to say that you've done it isn't necessarily the right approach. You have to do it in a thoughtful way, and hopefully a thoughtful and transparent way.

GRAEME BUNTON: Thanks. This is Graeme. Four quick points. We end up in a discussion quite a bit about registrars enabling abuse, and I think it is probably worth recognizing that it also impacts us as well. I think we are always, near constantly under a DDOS attack as a registrar. And so these things are important for our own interest as well.

I think, unsurprisingly, I agree with Elliot that there are plenty of tools in our contracts, but there are tools in our contracts; that we need to be a little bit creative -- more creative in how we use them.

To Milton and Farzi's point around the framework where it goes beyond DNS abuse, I think the argument could be made there that we're taking those actions in those very specific, very specific instances because of failures in governments and global regulation, and that's places where we see material harm where we don't feel like there are tools external to us that are acting there.

And sort of the last thought I'll leave you with from me is, and I'm playing with this metaphor that DNS abuse as we've defined it in that document is something akin to pollution, as a byproduct of the industry. And pretending that we can leave that as an externality is probably immoral, and we need to think more carefully about how making sure we're responsible for cleaning up that space.

Thanks.

MASON COLE: Thanks, Bruce. I'll just leave with a couple of thoughts. One is there's distrust on the Internet due to abuse. If ICANN doesn't do enough to address that distrust, then it undermines ICANN's legitimacy, and we don't want to see that happen.

So the BC applauds tools that fight abuse, we applaud what the registries and registrars are doing, and that includes trusted notifier and incentives.

I also want to agree very much with what Elliot said about compliance's role. We need to work together with compliance to give them the tools to bring down the bad guys.

So I hope all of us here in this room have learned something from today's session and we can get together and help ICANN do a better job.

JEFF BEDSER: So I've heard a lot about -- we talked about this for a long time. We continue to talk about it, but I'm actually really excited that this topic has been very forward on people's agenda this week and in the last couple of months.

I think that one thing we all have to keep in mind is that the perpetrators of abuse don't see these lines we're talking about between content and the DNS infrastructure. They don't care about lines that we say, well, it's your problem, it's your problem, it's your problem.

They're using this system and this ecosystem to victimize people and have continued victimization. We need to have a place to have the conversation. I'm not the policy person so I'm not going to say it should be ICANN's remit to do it, but I do think this is the community where we can have those conversations and get the ball moving and see who can do something to make the ecosystem better and have less abuse, improving reputation of the model as well as improve, bluntly, the capitalistic growth of commerce by people trusting the model they're using.

So, yeah, if not us, who?

Thank you.

BRUCE TONKIN: Thanks, Jeff.

So just to summarize, then, we heard some discussion around definitions and Byron mentioned it's really -- words do matter, and a few people spoke about being clear about the line between technical DNS abuse versus content abuse and making sure that there's a clear line between those two types of abuse. That some of the positive suggestions for further improvement, I guess, is how do we help people actually identify and contact the people that are physically responsible for hosting and continue to find appropriate ways of contacting the registrant.

That am I method of takedown needs to be matched with a method of appeal. So I think that's something that's a pretty common theme, that

there always needs to be a way of appealing a decision if something is taken down.

There's quite a few discussions about different incentives, and I think there was support for further investigation. Those incentives can be pricing, but there are other incentives, reputation. And a few people talked about if you make sort of higher reputation and people know what's good or bad, ways to improve that can help as well.

There was a few comments about solving the problem at the right layer. There's a bit of a mixture in this environment, and I think ICANN is still a really good environment to share best practices but at the contractual level, clearly the contracts need to be in scope of ICANN's mandate around the technical scope as well. And in particular, how can we help the Compliance Team be effective so that we can actually take action thence parties that are clearly not abiding by what the community believes is acceptable.

So, look, I'd like to thank all the speakers. I think each of the speakers in the audience and on the panel made a number of good points. And there's a lot for us to think about and move forward with. So thank you all.

[Applause]

[END OF TRANSCRIPTION]