ICANN72 | Virtual Annual General Meeting – GNSO: CPH DNS Abuse Work Group Community Update
Monday, October 25, 2021 – 10:30 to 12:00 PDT

REG LEVY: Good [inaudible], everyone, and Happy ICANN. I'd like to respectfully acknowledge that I'm speaking to you from the unceded territory of the Chumash Keys and Tongva peoples, which is also where ICANN is located.

Welcome to the CPH DNS Abuse Working Group community update. We've got an agenda on the next slide, which is probably less interesting than the third slide, which is our definition of what DNS abuse is. DNS abuse is composed of broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS abuse. Each of the Registry and Registrar Stakeholder Groups have additional information. And when you download the PDFs of these slides, you can click on those slides.

I'm going to turn it over to Brian now to present the Registry Stakeholder Group's [inaudible] on DNS abuse.

BRIAN CIMBOLIC: Thanks, Reg. Hi, everyone. I am Brian Cimbolic, general counsel over at PIR (Public Interest Registry). And I am Co-Chair of the Registries Stakeholder Group Abuse Working Group, along with Jim Galvin of Donuts, who's also on the call. Thanks so much, everyone, for joining. We want to save most of our time for Q&A after some brief presentations but just sort of a high-level summary of what the Registry Abuse Working Group has done and what we're currently working on.

The original genesis of our abuse working group was ably chaired by my Co-Chair, Jim Galvin, who worked on a DAAR working group that worked to provide recommendations to ICANN staff and particularly the Office of the CTO on how, from a registry side, we had improvements that we were suggesting to DAAR. That formed our abuse working group, and we've had several subsequent outputs as a result.

First of those was an education material demonstrating what a registry operator can do once it has identified abuse, recognizing that, with where we are in DNS infrastructure, we have very limited technical abilities to remediate harms. Ultimately, especially from a registry perspective, suspension is the typical remedy, and the collateral damage and impacts that can have, but noting, of course, that there are times where that is an appropriate remedy for DNS abuse.

We have also done a lot of collaboration as part of our outreach efforts with our friends across the various aisles. One of those was in conjunction with the GAC Public Safety Working Group. The registries and the PSWG co-authored a guidebook on dealing with DGAs (Domain-Generating Algorithms) that are associated with malware and botnets.

So there are some unique hiccups and challenges on both the registry side as far as creating the domain, getting permission from ICANN in certain situations for contractual wavers, as well as on the law enforcement side. So putting into one document what those pain points and best practices are should be very helpful the next time a, in particular, registry that hasn't dealt with these comes across it. That's built upon our prior work with the PSWG in the framework for registry operators to respond to security threats, which was another jointly authored document.

Recently, in just the last two weeks or so, the registries and registrars had put out the CPH framework on trusted notifiers. I won't steal Keith's thunder (because Keith is going to present on that), but that really was part of … In our outreach sessions with a number of constituencies, there was a lot of interest in (in particular, in the IPC, the PSWG, and the SSAC) these sorts of these relationships—so putting down, pen to paper, what those sort of core tenets of a trusted notifier relationship are.

So those are our existing and published works. We continue to solicit ideas on additional outputs that the community is interested in, so please don't hesitate to contact either Jim or myself if you have other ideas for us to look at. But we are currently working through the CCT-RT recommendations as they relate to DNS abuse and seeing how we can be helpful there. As well, Dennis Tan and Brian King are working through guidance on dealing with IDN homoglyphic text.

So that's, in a snapshot, what we've been doing, what we've been working on. It has kept us plenty busy since the last ICANN meeting.

And I do have one other item to hand over to Sam Demetriou to touch on. Sam?

SAM DEMETRIOU: Hi, everyone. This is Sam Demetriou. I'm the Chair of the Registries Stakeholder Group.

The one other item I wanted to mention that the stakeholder group has been working on, as has the Registrar Stakeholder Group, is a question about expanding the Domain Abuse Activity Reporting (DAAR) data to include registrar-level data as well as the current status of providing registry-level data. So this is something that we have been in discussion with ICANN Org about for a few months now, going back to, I think, just right around the ICANN71 meeting.

There is this desire on ICANN's part to extend the data that's available in DAAR. And as the Registry Stakeholder Group, we support this effort and we support this idea of having more information available for the community to understand the topic of DNS abuse better. We think that having more detailed data available for everyone will help facilitate better conversations about the topic of DNS abuse, which is really what this whole working group has been trying to get, in addition to tackling the problem of DNS abuse itself.

So the update here is that we reached agreement that this is an effort that we support. However, it does require an amendment to the base registry agreement in order to let ICANN use data that it receives from registry operators to do the mapping required to produce the registrar-level information in the DAAR report.

So the quick update here is that that's something that the Registries Stakeholder Group is working with ICANN on, and we're looking forward to engaging in the process that we need to go through to get that amendment done so that we can expand the DAAR data in that way.

I'll hand it back to Brian now.

BRIAN CIMBOLIC: Thanks very much, Sam. And, actually, I think that's it on the registry side for now, so we can hand things back over to Reg.

REG LEVY: Thanks, Brian. Thanks, Sam. The Registrar Stakeholder Group and the DNS abuse subgroup for the registrars [inaudible] a better job at tooting our own horn and promulgating the work that we do and have done for decades every day to clean up the [inaudible].

To that end, here is a list of some past, recent, and upcoming white papers on DNS abuse that have been published by the Registrar Stakeholder Group. The Guide to Registrar Abuse Reporting was republished in 2020 and gets revamped with some regularity as we try to provide best practices to all types of reporters regarding [what information a] registrar needs in order to adequately respond to a report of DNS abuse.

Registrar Approaches to the COVID-19 Crisis was also published last year, outlining common complaints about DNS abuse surrounding the early COVID-19 [inaudible] and providing data about how registrars responded.

We have newly published papers. When this PDF gets published, you can click on those links as well. We teased these in June at ICANN71 and have since published three new papers, which we'll present in a moment, and are working with the Registries Stakeholder Group to revamp the Guide to DNS Abuse Reporting to include recommendations on how and when to escalate a DNS [abuse report to a registry.]

I will now hand it off to Owen to discuss appeals mechanisms—no. Sorry. It's me still. We've changed the order, I think. I'm going to keep the floor as I discuss approaches to Business E-Mail Compromise scams. I encourage everyone to go and read and distribute this paper widely, as I consider that it includes a lot of good and actionable recommendations for people to protect themselves and their companies against BEC scams.

Business e-mail compromise is a social engineering hack that convinces the recipient of an e-mail that the sender is a party authorized to instruct payment. This could be a CEO, a government entity, or a bank. Compromise could include a lookalike e-mail or a domain name, or it might not. The U.S. FBI has estimated that the [inaudible] cost U.S-based companies more than $26 billion U.S. over a three-year period starting in 2016.

Because this scam may or may not rely on a compromised domain, registrars may help combat the issue, although an e-mail platform may. And many registrars also provide e-mail. Reporting to the e-mail platform provider is always the fastest way to have the issue resolved, but the paper also includes best practices for registrars that want to take an incident-response-type approach, including tips on debriefing your team to refine protocols for future issues.

For reporters, the document includes information about how to determine e-mail platform provider via a [dig] tool.

I will now hand it off to Owen to discuss approaches/appeals mechanisms following DNS abuse mitigation.

OWEN SMIGELSKI: Thanks, Reg. We put together here some appeals mechanisms for registrants that are subject to abuse complaints. I just want to bring up that last bullet point first. This is not intended to facilitate or protect abuse. This is just to ensure that registrants are protected and do have some sort of due process claim or approach that they can follow to ensure that their rights are protected. So this is just a way to "appeal." It doesn't necessarily mean that these are something that a registrar would have to actually appeal in that process. It's just to have that avenue for the registrant to be able to speak and have their voice heard and be able to potentially rebut any type of issue that may arise due to abuse.

So the first part is to ensure that all DNS abuse complaints are based upon material actionable reports that have verifiable evidence. Quite often, a large number of abuse complaints just say, "Take down this domain name. It's abusive," and there's not really that much that a registrar can do without being able to verify abuse. We can certainly try and look it up sometimes, but those may not necessarily be reliable.

I've also seen where there are also very IP- and geo-specific abuse. There was one complaint that we had from an APAC police department. It said, "This is abusive," and we couldn't see it on our end. And then when we sent us back a view of the website from an IP address in that region, we could see that the abuse was present. So we do need to have that because, if we're going to take a domain name away from our customer and break a contract, we need to make sure that we're doing it with evidence. And that also ensures then that the registrants are protected in that aspect.

The next appeal process, once there has been a decision, is that the registrant should be able to appeal internally through whatever type of customer service process that there is. So it's possible that one person's abuse could be somebody else's other thing, and the registrant should have the opportunity to present that. Like I said before, that's not meaning that they have a guarantee that it would get reversed but it's just to have that opportunity to be able to present that information/evidence and try and either refute or dispute some of the claims that were in there. Again, this will be something that is not necessarily revealing confidential information. I know some types of abuse complaints are sensitive and confidential, but you need to keep those in mind but still give that registrant that mechanism to appeal.

A third type of appeal mechanism that's there is some sort of internal ombuds process, where there is an independent third party (internal to the company in this case) that is outside of that customer service process—somebody to come in and take a fresh view, perhaps more of an independent view, not being influenced by what has already happened within that process there.

And then, always, there's a whole bunch of other appeals processes which we're collectively calling courts of competent jurisdiction, but that doesn't necessarily need to be an actual court process. Some countries to have a public ombuds framework, where a registrant can complain to. There's also consumer protection agencies that might step up to assist somebody in that case. There can also be law enforcement complaints if this is a very egregious type of action in belief of the registrant. And also there is opportunity to use other legal processes as well, too, such as actual litigation, too, if it's that type of concern.

So, again, these are things that are there to protect registrants in that and make sure that they don't have domains taken away without any reason. But also, again, I want to highlight that it's not to shelter or keep abuse in place. We want to make sure those are being actioned upon.

And with that, I think I pass it off to … I'm not sure. Thanks.

REG LEVY: Thanks, Owen. It now goes to Keith for the trusted notifier framework discussion.

KEITH DRAZEK: Thanks very much, Reg. Hi, everybody. It's Keith Drazek. On behalf of the Contracted Party House, I'll give a brief update here on developments related to our trusted notifier framework. I've got about eight slides here. I won't go through each bullet because I want to leave time for Q&A, but I think it's important to introduce this. The document itself is available on the websites—the Registry's and the Registrar's. We can provide that link as well in chat, I'm sure.

The Contracted Party House has been working over the course of the last several months—really over the course of this year—on the development of a trusted notifier framework. And it's important to note that several registries and registrars already rely on or have relationships with trusted notifiers to help address DNS abuse and website content abuse issues. The framework that we have relies, in terms of scoping out some key aspects … And that is expertise and accuracy of a trusted notifier, documented relationships with the registry or registrar, as the case may be, and a defined process for notification and recourse.

Next slide, please. The purpose of the framework is intended to serve as a guide for the parties who are considering entering into a trusted notifier arrangement. That's both from a registry and a registrar perspective, as well as for potential trusted notifiers. So this document is really intended to serve, establish, or set out a common understanding common considerations as folks consider whether to engage in a trusted notifier type of relationship or not.

It explains the role, the responsibilities, and the expectations of trusted notifiers in the mitigation of abuse. It's important to note here that we're talking about DNS abuse in the context of the Contracted Party House definition, the security threats that we've outlined, as well as the possibility for registries and registrars to engage with trusted notifiers as it related to content-related issues. And, again, I think it's important just to underscore here that, in the ICANN context, ICANN's bylaws are quite clear and quite explicit in terms of the limitation that ICANN has relating to content matters. So it's important to note here, as a distinction that, when registries and registrars engage with trusted notifiers related to content, it is quite clearly outside of ICANN's remit. So I just wanted to flag that as an important distinction for other parts and other groups in the community to understand.

Next slide, please. The expectations of a trusted notifier in the document is that the trusted notifier has strong and demonstrated expertise in the subject matter. This is important because, as registries and registrars, depending on the type of DNS abuse, particularly if it's content-related, simply may not have the expertise that a third party might. And so I think, as we as contracted parties, consider engaging with trusted notifiers, [inaudible] there's a matter at hand. But there's [inaudible] behind its reporting and is committed and [inaudible] to a low false-positive rate and the accuracy of its notices. And as a [inaudible] challenge the trusted notifier recommendations. I think this is also [inaudible] that relates to the actual trusted notifier. The process for registrants [inaudible] …

TERRI AGNEW: Pardon, Keith. This is Terri. Pardon the interruption. I do apologize, but your audio is cutting in and out, and at this time, it's very difficult to hear anything you're saying.

KEITH DRAZEK: So I'm going to hand it over to Dennis. Dennis, if you could take over at this point. Thank you.

ZOE BONYTHON: So we might need to make Denis a panelist. I'm not sure he … Because—

KEITH DRAZEK: I'm having some network activity issues. I apologize.

TERRI AGNEW: Dennis, you are now a panelist.

DENNIS TAN: I'm a panelist now. Can you hear me now?

TERRI AGNEW: Yes, we can.

DENNIS TAN: All right. So let me pick up where Keith left off. So roles and expectations. As Keith said, we have flavors of trusted notifiers. As it relates to either security threats or content issues, we expect that the trusted notifier has a strong demonstrated expertise of the subject matter at hand and operates with a consistent adherence to substantive and procedural due diligence, which basically refers to the collection of evidence that supports the alleged abuse, and also follows what the Internet & Jurisdiction Policy Network refers to procedural due diligence to report the abuse to the closest party that can mitigate, starting from the bottom, all the way to the registry, from the web hosting providers going through all the stages up to the registry. That helps to mitigate the abuse in a fairly quick and effective way.

Another aspect of a trusted notifier is that it stands behind its reporting and is committed to a low false-positive rate because that could cost him the designation of a trusted notifier.

And last but not least, it's to also have a process in order to appeal the recommendation of trusted notifier in case a registrant or the affected party feels that the action taken against the domain name was not fair or was misplaced.

Next slide. Here's a good notation as we get into roles and expectations. A notifier that is trusted is not the same as a trusted notifier. The key designation here or the key aspect of a trusted notifier is that that designation is based on the registry operator or the registrar. So it is not an organization or individual that comes along and names itself as a trusted notifier but rather it's a designation that is gained by the experience, performance, and all the processes that they have in place in order to, again, follow, fill the roles and expectations of the trusted notifier, of subject matter expertise, procedural due diligence and standard due diligence, and commitment to their reporting and so on.

Next slide, please. The trusted notifier obviously has the subject matter expertise in a subject. They file a report following the process agreed upon with the registry or registrar. But ultimately, the choice of action—what to do with a domain name—falls in the hands of the registry or the registrar.

Next slide. Another aspect of trusted notifier frameworks … These are different flavors, but in general, we see that trusted notifier [arrangements] are done in writing, where these rights, responsibilities, and expectations, including mitigation to the registry or registrar in case of commercial interests, are established so that the, again, rights and obligations and representations or warranties are clearly stipulated.

Next slide, please. So I'll deep dive a little bit more on due diligence by the trusted notifier. I mentioned that there are two levels of due diligence. One is the substantive one, which basically means that the alleged abuse is properly investigated, substantiated, and documented in order to file that report to the registry or registrar. But at the same time, we expect that the trusted notifier follows a procedure in order to report the abuse or follow a process to start at the bottom of the chain. For example, if it is a content issue, we would expect that they would start with the hosting provider, or even the registrant and operator, and move up on the chain as the case is warranted.

Next slide. We recognize that the trusted notifier may shortcut, for lack of a better term, the due process in terms of from a legal standpoint. So we recognize that there are concerns within the community in terms of following due process and what's the role of trusted notifiers. So we encourage in this framework that there needs to be a level of transparency in this relationship. And we draw from the work of the Internet & Jurisdiction Policy Network this two-dimensional approach into offering or providing some transparency into this arrangement. And one is to share statistics about the abuse reports process and the actions taken and also make the decision-making criteria as to what types of reports are processed and the decision-making criteria to take certain actions in what cases or not, so the community or registrants or the affected parties know what to do in cases of a decision affecting a domain name or not.

Next slide. This is our last slide. Also, we recognize that we see the value of trusted notifiers in both cases of content and security threats and that there is potential in future work in terms of how we scale the number of trusted notifiers and how we scale the number of registry operators/registrars offering these types of [arrangements] and how can we manage the number of trusted notifiers and the platform that can handle all these reports. So this framework is just a starting point. We will continue to see opportunities to improve upon it. And, again, one of the areas where we have identified the scaling problem here.

So I think that was our slides. And I think that's it. So back to you, Brian.

BRIAN CIMBOLIC: I think this goes back to Reg. Thank you, though, Dennis. Especially thank you for pinch hitting there. Reg, back to you.

REG LEVY: Thanks, Brian. Thank you, Dennis, as well. We're going to move the Q&A portion. I know there have been some Qs in the chat. If anyone has a question they'd like answered, if you could please put it into the Q&A pod, which is at the bottom of your screen.

We do already have a few questions queued in the Q&A pod. From NetChoice: "Does the trusted notifier framework require each CPH participant to show the same or similar terms of service definitions and standards for what constitutes DNS abuse and content restriction violations?" And I believe Brian wanted to take a first stab at answering this one.

BRIAN CIMBOLIC: Thanks, Reg. And thank you for the question. My answer also sort of touches on Griffin's question in the pod. So the core of this document—I encourage everyone to read it—is that it respects the variety and differences in between each and registrar's terms of service and what their abuse or acceptable use policies cover. So we wanted to specifically avoid standardization because we wanted to allow for each registry and registrar to make the decision as to whether or not to enter into a trusted notifier relationship because what PIR has under our policies may be different than what another registry or registrar has. So the cornerstone here is that each registry and registrar has to be in a position to make that determination to work with a trusted notifier.

And so there was a question of, are there existing relationships under this framework? Yes. If you look to any of the trusted notifier relationships out there, PIR has several, including with the Internet Watch Foundation, to deal with child sexual abuse material, and with the U.S. Food and Drug Administration to deal with the distribution of illegal opioids online. Each of those trusted notifier relationships really fall directly under the tenets of this trusted notifier framework.

So please do take a look at it, but central to the core of that is that a registry or registrar has to be ultimately making the determination for itself of whether or not the expert organization coming to it is an appropriate fit for a trusted notifier relationship. So this is not some sort of clearinghouse for vetting trusted notifiers. That due diligence still has to occur at the contracted party level.

REG LEVY: Thanks, Brian. And Maxim brought up a good point in the chat as well: each of our anti-abuse policies are going to be different, by TLD and by registrar. So each of us will have a different relationship even with the same or a similar trusted notifier.

We have another question from Mason Cole. “Trusted notifier is a good development. Can contracted parties provide any transparency about how many or how often requests for trusted notifier relationships are requested and granted?” I’m going to take a first stab at this.

There are some trusted notifiers that we work with that we explicitly keep secret. My terrorism reporter doesn't want me telling everybody who they are so that terrorist can go find them. So, for example, there are very good reasons why one would like certain types of transparency.

That said, I don't know if other registries or registrars are interested in saying how many people do reach out on a regular basis to offer to be a trusted notifier. I know that a number have reached out to me, but the successful relationships that we've formed have been where two Tucows has gone out to find a particular type of trusted notifier that we're on the market for and then found [it].

I don't see any hands from my side, so I will move on to [inaudible]. I apologize if I'm mispronouncing that question. "While ultimately it's the responsibility of the registries and registrars to take action on forms of abuse," dot, dot, dot, unquote. "What is the definition of "verified" in this context?" Also, the same question from Peter Van Roste concerning legal/financial consequences. I'm not sure what that question, is Kristof, so if you could put that into the Q&A pod, that would be great.

So, on the question of verified forms of abuse in the context of a trusted notifier framework, Keith or Dennis, would you like to take a first stab at that?

If not—

DENNIS TAN: Uh …

REG LEVY: Go ahead, Brian.

DENNIS TAN: I'm here. Or Brian.

REG LEVY: Go ahead, Dennis. Thank you.

DENNIS TAN: Okay. So "verified action" means that the alleged abuse is actually an abuse and largely will depend on which type of abuse we are talking about. Is it a phishing attack or is it a malware/botnet distribution network? So it depends. But we are not defining, prescribing what are these levels of evidence that we are asking for a trusted notifier for. That is going to be a one-on-one relationship with each trusted notifier and registry or registrar. So each one will define what's the level of control, of the rigor of the evidence that needs to be providing for the registry or registrar to act on such reports.

REG LEVY: Thank you very much, Dennis.

Brian, I saw your hand briefly. I wasn't sure if you also had an answer.

BRIAN CIMBOLIC: Thanks, Reg. I just put it in chat. So basically that's one of the reasons why substantive due diligence is such an important concept in this framework—and not just the substantive due diligence on the trusted notifier side but that the contracted party understands the level of due diligence that goes on on the trusted notifier side prior to entering into that agreement.

REG LEVY: Thank you, Brian. From Paul McGrady: "What is the timeframe for implementing the T/N?"

So my response to that is that this already has a number of trusted notifiers, so I was just in the process of typing a few of them into chat in the interest of transparency. And the timeframe is both immediate and past and future. Many of us have had trusted notifier relationships for some time for certain types of abuse. For example, NCMEC has always been a trusted notifier for Tucows with regard to child sexual abuse material. That doesn't need to be a formalized relationship. It's just that, when they say something, we [inaudible] because they [inaudible] notifier by law in one of the countries that we operate.

So many registries and registrars have had trusted notifier relationships for some time. We are looking to form some now and in the future. And the trusted notifier framework really is just guidelines for both contracted parties as well as potential trusted notifiers for level-setting of expectations.

Ashley, I see your hand.

ASHLEY HEINEMAN: This is Ashley here, Chair of the Registrar Stakeholder Group and GoDaddy. You hit just almost exactly what I was going to say. Just to clarify even further, this isn't a program, per se. As Reg just characterized, this is just to kind of level-set what the expectations are and to be a resource. So it's not a program that's being launched or anything like that. So just to make that clear. Thank you.

REG LEVY: Thank you, Ashley. A question from Griffin Barnett from Perkins Coie, LLP: "I appreciate the work being done to expand trusted notifier programs. Can any of the speakers identify existing operational trusted notifier programs and how people might seek to participate as a trusted notifier? If there are existing resources available on this, please feel free to direct me to these. Thanks in advance."

So, again, I am well-aware [inaudible] any parties out there who are interested in being a trusted notifier. And I invite you to reach out to the registries and registrars that you are interested in being a trusted notifier for to offer that service, along with an explanation of what area you think that you would be a valid trusted notifier in.

Please do read the white paper first because it includes a lot things that we're looking for, including things like—my brain just left the building—statistics about how often you are correct and how often you are incorrect with regard to identification. So please do reach out.

Nigel Hickson, U.K. GAC: "Good evening. Will the [inaudible] framework evolve as the work is developed further in the I&J Network Working Group?"

Brian, I see your hand.

BRIAN CIMBOLIC: Thanks, Reg. And thanks, Nigel. I raised my hand because I participate in the Internet & Jurisdiction Policy Network. And I see we've got Liz Behsudi, who's Director of the Domains & Jurisdiction Track. So thank you for joining us, Liz.

So the last portion of this document of the CPH trusted notifier framework explicitly states that this is a living document; that this isn't something that we put out there and we set it and forget it. So to the extent that there is other helpful guidance—and the guidance of Internet & Jurisdiction is usually very helpful—it helps to evolve this paper. I think that that's something that we're certainly open to.

Now, I don't know that we have it on our calendar that we're going to revisit this in X number of months, but I think it's incumbent upon us that we lay that gauntlet that this is something that we're going to try and help improve over time. So guidance like that is something that we would definitely look towards.

REG LEVY: Thank you, Brian. Mark Wilsons asks, "Speaking in a personal capacity, I see some good practices from registrars who are taking the initiative to launch their own "trusted notifier or VIP program," [inaudible] to make reports in good faith. That said, how will TNF apply to registrars and registries, as some engage with DNS, and others are poor to respond? Will TNF have an impact across these contracted parties who are poor to respond?"

Thank you, Mark. As we've said a couple times already in this—I realize that the question was asked before we started answering questions—this is just a framework. This is a set of guidelines for registries, registrars, and trusted notifiers to use [inaudible] valid relationships with each other. This does not sanction anyone who does not use trusted notifiers. And to the extent that it benefits corporate people who use trusted notifiers, it's only in the sense that they can laud themselves for doing so.

Russ Weinstein says, "Thanks for the good work on developing the framework for trusted notifiers. To your knowledge, do any registries or registrars pursue trusted notifiers on their own, or does the demand/initiative need to come from the trusted notifier side?'

So I can answer this briefly. I tossed into the chat a couple of Tucows trusted notifiers with respect to pharmaceutical complaints, and those are absolutely something that we reached out to various people about. Thanks to ICANN, when we used to meet in person, I met some of these people and I thought, "Hey, you do a thing that seems like it would be useful to me," which is the most important thing in the world (being useful to me).

So, yes, absolutely, registries and registrars are looking to reduce work for themselves and pass off that work to other parties, for sure.

That said, anyone who is interested in being a trusted notifier should reach out directly after reading the framework paper to registries and/or registrars who they think might be interested in their work.

Marc Trachtenberg says, "I also appreciate the work being done here on trusted notifiers and would like to participate. I was hoping for clarity on what is meant when it is said that the trusted notifier must legally stand behind the abuse complaints. Does this mean indemnification, support of the registrar/registry if a complaint is submitted by a registrant whose domain gets suspended, or something else?"

Thanks, Marc. Yes, in the paper it does include a discussion of indemnification specifically. Some registries and registrars may well require that indemnification. Most registries and registrars are going to look at a trusted notifier's or a potential trusted notifier's failure rate because it is the case that trust is earned. And so sometimes a trusted notifier may have to ramp up that reports are submitted, they are vetted by the contracted party, and then actioned in advance of going to a full-on "just anything you say goes."

I think that answers the question, but please feel free to drop another question into the question pod if it did not.

Mark Datysgeld says, "Thank you for advancing these discussions. Question: Are DGAs (Domain-Generating Algorithms) and name spinners being examined as a source of abuse?"

I believe this goes to one of the non-trusted notifier presentations that was made. Ah, yes, Brian. Thank you. I see your hand.

BRIAN CIMBOLIC: Thanks, Reg. And thanks, Mark, for the question. I'll put in the link in the chat, but, yes, the registries—this is one of the papers I touched on before—jointly drafted a paper with the GAC Public Safety Working Gorup on domain-generating algorithms—in particular those that are associated with malware and botnets. I'll put a link in the chat there.

I'd also note that, to bring up the earlier theme, Internet & Jurisdiction is taking a look at this as well. So the issue of DGAs does continue to get more and more intention. As I think either Jim or Gabe has coined, they are a low-volume, high-impact event. They don't happen often, but when they do, they cause significant headaches, obviously on the side of both law enforcement but also on the side of registries.

REG LEVY: Thank you, Brian. Griffin Barnett from Perkins Coie, LLP, says, "Do any of the participants have any insights they can share regarding how many trademark owners/their representative have been granted trusted notifier status?"

I know that some registries and registrars have received requests from trademark owners or their representatives to be trusted notifiers, and the contracted party house asked for indemnification, at which point negotiations broke down. I don't know if any other trademark representatives are trusted notifiers, but the industry is vast. There are many contracted parties. And, again, there's no requirement that these be made public because that sometimes can lead toward taking advantage of the situation. So I hope that answers your question.

That is the end of the questions that we have in the chat. There was a comment. If anyone has any other questions, please drop them into the Q&A pod. I do see that there is a vibrant debate in the chat, but I'm only paying attention to the Q&A pod for now.

So the questions that we have on the screen right now are the ones that we typically use to drive conversation with the outreach sessions that the contracted party DNS abuse subgroups have made with various ICANN groups. We have met with the Public Safety Working Group, SSAC, the IPC, and we look forward to meeting with them again and to expanding the list of groups within the ICANN community that we meet with to discuss DNS abuse and how they believe it impacts them and their constituency.

So, if anyone wishes to answer to ask questions that are on the screen now for their own purpose or representing whomever they are here to represent, they are also welcome to do that.

Sam, I see your hand.

SAM DEMETRIOU: Thanks, Reg. I just thought this would be a good time to remind folks that we've gone through most of the questions, I think, or all of the questions in the Q&A pod. And we appreciate those, but this is also meant to be an interactive session. So if anyone has a question or a point that they raised in the chat pod that we maybe didn't get to, or if you would like to follow up and react to any of the discussion that has taken place today, please feel free to put your hand up and get in the queue. I think we have the ability to open people's mics. So we want to hear back from you guys.

REG LEVY: Thanks, Sam. We have another question in the Q&A pod. Ken-Ying Tseng says, "Would the ICANN registry agreement be amended for the implementing of the trusted notifier framework or any other DNS [inaudible] measures?"

I see that Brian has a brief answer to that.

BRIAN CIMBOLIC: Thanks, Reg. And thank you, Ken-Ying. I appreciate the question. So my instinct on this is no. And, again, part of the pillar of the document is that the trust is established between the parties. So it's not for a third party to hand down to a contracted party, saying, "You now trust this organization." That has to be something that happens organically between the registry or registrar and the trusted notifier that comes with its expertise to the table.

And the other thing I'll point out is that the trusted notifier framework, while it does contemplate DNS abuse as one of the core areas that you can work with a trusted notifier in, it also goes beyond that to include the possibility that a registry or a registrar could deal with website content questions. And, again, PIR participates in such a program with

IWF and with the U.S. Food and Drug Administration, but neither or those would be appropriate to include in the contact with ICANN, just given its technical remit.

REG LEVY: Thank you, Brian. And, yes, from a registrar perspective, I would also like to underscore the fact that these are voluntary white papers, voluntary documents, that we are promulgating in the hopes that we can establish industry best practices. And that does not necessarily extend to the contracts themselves, which are more of a baseline.

I see a lot of thank yous, Brian, in the chat.

Also, to Brian's point about trust, there was a question—not a comment—on the question pod from Dean Marks. This isn't a question but rather a contribution. "Personally, I think the word 'trust' is a key component of trusted notifier arrangements, and it can take time to build that trust and mutual confidence/understanding. So I encourage people [inaudible] about this and to take the time to enter into discussions. [inaudible] speaking, I do not think this should be a scorecard type of effort or activity."

Thank you for that, Dean. And, yes, I think that the operative word of a trusted notifier is that trust. And establishing that trust is going to be different for each party. That's why this is a framework. It's a relationship, and it's a relationship that necessarily is based on trust.

Another question from Mason Cole. "What information can contracted parties share about recruiting other registrars and registries to participate in trusted notifier programs? Trusted notifiers are great, but of course they are not universal. Also, are further developments contemplated—for example, when an account is the subject of multiple complaints [it wants] but perhaps not yet from the trusted notifier[/]provider?"

Thank you for that, Mason. I would say that being public about the success of trusted notifier relationships is going to be the best form of recruiting other registrars. I'm always happy to make introductions for the trusted notifiers that I have to other contracted parties.

And to the question of transparency, I would say that I would be more likely to share some of that information within the registrar group itself than necessarily more broadly because that would be an industry group who would be interested in using those trusted notifiers specifically.

I also see that Brian has a response to this question.

BRIAN CIMBOLIC: Thanks, Reg. Kind of +1 to what you were saying.

And the other thing I would say is that this is an area in particular where not having face-to-face meetings has kind of slowed progress down, where the registries and registrars have a child sexual abuse material referral discussion group that was meant to be sort of a closed-door, Chatham-House-rules safe space where registries and registrars could raise their hand and say, "Listen, this is a tricky issue. I need help. I need guidance from either other registries or registries, as well as expert organizations." And we've brought, within those meetings, those face-to-face meetings, the INHOPE network itself, the National Center for Missing and Exploited Children, and Internet Watch Foundation each to those meetings. And those sort of personal relationships can form such that the bridge, the foundation, is really laid to create those trusted notifier relationships. Without those meetings happening, there's been a lot less of that exposure to organizations that might help become trusted notifiers in such important issues like CSAM. So hopefully that can pick up again once in-person meetings start again, whenever that might be.

The other thing I would say is on the question of, well, if you get multiple referrals on the same domain, even if someone is not a trusted notifier, would you still take action? I do want to just point out it doesn't mean that you get something from a trusted notifier and you act on it or nothing. With a trusted notifier, there's sort of a presumption that the registry or registrar has done its due diligence, understands the process of the entity making the referral, and is comfortable with that process such that it gives deference. The registry and registrar still ultimately has to be the done that makes the determination to take action on a domain.

And I think this is true of most registries and registrars. It's certainly true of PIR. It's not as though, if someone is not a trusted a notifier, we won't take action on an abuse report, especially with regard to something like DNS abuse. It just means that we have to do additional due diligence on our side.

So, yes, if we are getting reports of something like DNS abuse from multiple from multiple referrers on the same domain, it's something we're going to factor in in taking action even if we may not have a trusted notifier relationship in place with those organizations making the referral.

REG LEVY: Thank you, Brian. I'd also like to call out Jothan's comment in the chat, that it's important to underscore that there's not a trusted notifier program being discussed. That doesn't exit. This is just about the framework, which is intended to be a level-setting of expectations for contracted parties and trusted notifiers alike, should they be interested in it turning into a trusted notifier relationship.

Phil Marano asks, "Indemnification ordinarily involves a degree of fault on the indemnifying party. What specifically is the scope of the indemnity expected from trusted notifiers? All third-parties claims arising out of or related to a trusted notifier's complaint [inaudible] reasonable, like negligence or willful misconduct of the trusted notifier?"

I would say that that is a question to put to the contracted party by the trusted notifier themselves. It's very likely to be different in each situation with regard to what types of abuse the trusted notifier is supposed to be notifying about. So that would be a question for the contracted party that you are having that conversation with.

Thank you, Brian. Yes. It depends.

Jonathan Zuck says, “Has any thought been given to forming some sort of contracted trade association outside the ICANN context that might more formally adopt trusted notifier practices, come up with a seal, etc.?”

Thank you, Jonathan. I would say that i2C and I&J already exist. I don’t know if they have corporate seals, but I presume that they do. I myself enjoy a good wax seal, but I don’t think anyone is going to be vetting trusted notifiers because, again, this is a relationship of trust between two parties: the contracted party in question and the trusted notifier in question. We can share within our industry groups—and we do—when we have successful trusted notifier relationships with certain parties.

As Brian explained, PIR and Donuts have been instrumental in getting information from the Internet Watch Foundation, which is a trusted notifier for CSAM, out to the broader community. Back when we could meet in person, we would have regular meetings with members of law enforcement, members of other CSAM national reporters, and [contracted parties] where we could have the conversations about pain points, [inaudible], and meet each other, shake hands, and say, “Hey, I’m Reg,” so that we could start those relationships and start to form that level of trust.

Dean says, “Do contracted parties who enter or think [about entering] a trusted notifier arrangements consider limiting the number of [inaudible] that they will consider? This can sometimes be a useful way to begin a trusted notifier arrangement and ensure that contracted parties don’t feel overwhelmed by a particular trusted notifier.”

Thank you, Dean. That's actually an excellent question. That is a great thing that I'm going to add into my new trusted notifier rulebook for personal use, for corporate Tucows use: that asking them to just send a handful of reports at the first rung would be a great way to start that trusted relationship.

Brian also has a response.

BRIAN CIMBOLIC: Thanks, Dean. And I appreciate especially, Dean, the spirit of how you make it easier to implement—[that's] where that question was coming from—which I really appreciate. But at the same time, you want to, if you're dealing with something as serious as child sexual abuse materials, not say, "Well, just give me 20," or whatever it is. If it exists, you want to know about it. So it's an imperfect balance.

So, again, coming back to the squishy lawyer answer in the chat, it depends. But if you're dealing with something that has real potential for serious harms, it's not something that you would want to put any sort of firm cap on, in my opinion.

REG LEVY: Thanks, Brian. The Slack backchannel of panelists has told me that Jonathan Zuck's hand is up, but I cannot see it. So, Jonathan, if you want to jump in, please feel free.

JONATHAN ZUCK: I'm sorry. I was going to ask the question. I ended up typing. So I forgot to put my hand down. But thanks for noticing.

REG LEVY: Got it. Thank you. Sorry for not noticing.

Just did that one.

Griffin Barnett of Perkins Couie, LLP, has another question: "Further to Mason's question, do registries or registrars do any kind of analysis internally to see if multiple domains are with the same registrant/customer [inaudible] the consideration as part of the response?"

Thank you, Griffin. I can only speak to what Tucows does. And we absolutely correlate between a registrant who is the customer of a particular reseller as well as resellers directly. Since we operate primarily on a wholesale basis, it's more the reseller that we are concerned about. And if we see a lot of abuse within a particular reseller, we [inaudible] with that reseller to help them combat that abuse. We get reports monthly of how much abuse happens in each reseller.

And I have used this example before, but I kind of love it. A very small reseller that was never on our radar before that we've never heard of in the Compliance department was, all of a sudden, our highest scoring abused reseller. So we reached out to them and said, "Hey, can we help you with anything?" And there's a [inaudible]. We had a brief moment where we decided to accept cryptocurrencies. We're not doing that anymore.

So, yes, absolutely, we do our own level of correlation. I don't think that that's something that is necessary to write into a trusted notifier framework. That goes down into how each registrar treats abuse in its own network.

The next question from Griffin Barnett from Perkins Coie, LLP: "(even if not reported by the same reporter)."

Correct. The abuse [inaudible] who reports it.

Phil Marano asks, "Quick follow-up question. Are contracted parties entertaining reasonable limitations of liability to cap such indemnities from trusted notifiers? If so, in what ballpark?"

Thank you, Phil. With regard to indemnification again, that's going to go back to the relationship between the contracted party and the trusted notifier directly. Limitations of liability and indemnification are questions that are going to be unique to each party. Some registrars are going to require much higher—and some registrars are going to require much lower—levels of that. So that's not really a question that can be answered by the panel here today.

NetChoice asks, "Trusted notifiers will work well for large and legitimate contracted party players. The oft-cited bad actors will not participate. What can a trusted notifier framework do to help address that?"

Thank you, NetChoice. The issue of [not]-bad actors is something we deal with all the time. Here we are: a number of contracted parties doing our best to set best practices for the industry and presenting to you papers on how exactly we are doing that. I'm not entirely certain how you would like us to speak for people who don't participate in that.

If anyone else wants to try to answer—Sam, go ahead.

SAM DEMETRIOU: Thanks, Reg. This is a question that comes up a lot, as you noted. And the question of bad actors is one that comes up a lot. I think we're still at a phase in this work where we're trying to get as much information and resources out there across a number of topics. So a trusted notifier framework is one example, but so is the framework we did on the domain-generating algorithms and things like that. And I think, at least as an initial step—I'm not going to pretend that this is going to solve every problem—our efforts should be to try to put information out there. We're hoping that that helps address some of the problems, at least in the cases of smaller actors who just aren't really aware of some of these problems, and how they can go about addressing it.

So we understand that this is a starting point, but I think where we're at right now is, well, we're at least going to start somewhere. So I think that's how we've been approaching these as voluntary best-practice-type documents.

And the question of how to clean up bad actors further from there is one that we're continuing to grapple with as well.

BRIAN CIMBOLIC: Reg, I think you're on mute, maybe.

REG LEVY: Thank you. Jonathan Zuck asks, "Can someone comment on the recent ICANN Compliance audit that revealed a number of contracted parties were out of compliance with respect to DNS abuse? Should this effort be broadened? It was just a sample, yes?"

With respect to the lack of compliance that was potentially shown in the Compliance audit that recently finished, there are multiple responses on Domain Incite's blog comments, as well as the official comment from ICANN Compliance in its pre-ICANN compliance presentation.

Owen also has a response.

OWEN SMIGELSKI: Thanks, Reg. I'd like to just say bluntly that that headline in Domain Incite was incredibly misleading. It's not an actual representation of what the results were. For example, just to give a little color of some of the things, the failures that were identified could be ICANN saying, "Hey, we can't find this telephone number," and a registrar saying, "Here's where the telephone number is located." So that would be marked as something that would be not passing the first round, but that's not a failure by any stretch of the imagination.

There's also interpretation things, where ICANN says, "Well, you're not doing this because we think you should be doing this," and we respond back with, "Hey, this is what we're doing. [inaudible]," and ICANN would say, "Oh, okay."

Or I know a particular registrar—I won't call them out—had to specify exactly which customer service platform they were using. That was a deficiency.

So, again, I know it's a headline that gets a lot of attention, but it's really not representative. And the results show, from the number of registrars that did not have to go through any type of remediation or do any type work or action—and it was all basically closed before reaching any escalated or enforcement action or anything like that—that it actually was really good. And I don't know that it's necessarily representative of needing to find more registrars to deal with this because it takes a lot of effort and money for ICANN to do this. But the registrars that were sampled represent some 90-ish% of the gTLD registrations out there. So quite a bit of them were covered. Thanks.

REG LEVY: Thank you, Owen. And to the second part of your question, Jonathan, with regard to "Should this effort be broadened?" I'm not entirely certain which effort is specifically referenced in that question. But, yes, contracted parties are working with ICANN Compliance to make sure that they are actually [focusing on] what we think is important, not posting the customer service platform you're using on your website but rather actually dealing with DNS abuse reports. So, yes, absolutely.

Registries and registrars are every day—perhaps not every day, but every week—in conversations with ICANN Compliance with regard to what it is that they're focused on and how they can better serve the community by enforcing the contracts against us.

Nick Wood says, "The framework argues effectively that the relationship between registry, registrar, and trusted notifiers should be shaped by each registry/registrar and not standard. But could registries/registrars clearly publish the path a potential trusted notifier takes to get accredited just as they publish the [inaudible]?"

So I think this is a question about [which] particular contracted party could publish something on their website. And I suppose that they could. But as the paper points out, there is a vast [diversity] [inaudible] in what a registry or a registrar will accept from a trusted notifier, as well as what is required [for] types of abuse.

So previously I said [inaudible] is a trusted notifier for Tucows with respect to CSAM. That's not because of any official relationship that they have with us at all. They probably don't even know that they're a trusted notifier with respect to us because they just don't ever think about us, which is totally fine. But that doesn't change the fact that we will act on reports from them in a different manner than we will act on reports from just a random reporter on the Internet.

So I would say no, generally speaking, is the answer to your question, except that each registrar and each registry may take it upon themselves to begin to publish not just an abuse reporting page but also a trusted notifier sign-up page, if they would like to.

Dean says, “Brian C. mentioned that normally, in trusted notifier arrangements, the ultimate decision as to whether or not to take action on a notification remains with the registry/registrar. So that can be a path towards addressing the thorny issue of potential indemnification. I can share that, with some of the trusted notifier arrangements I have been involved with, on a rare occasion or two did the contracted party did not agree with the referral that was made. And that was clearly their prerogative. We agreed to disagree and continued with a productive trusted notifier relationship.”

Thank you for that comment, Steve. Yes, and, again, this is a relationship between two parties. The framework is just that: a framework, a way to level-set among registries, registrars, and trusted notifiers. What [inaudible] they might want to consider. If this is a party that has never been a trusted notifier, this is something that they should read. If this is a contracted party that has never had a trusted notifier, this is something that they should read. So that’s all that this is. This is just a framework.

Once again, we have reached the end of the Q&A pod. There has been vibrant discussion. I know that there’s a lot going on in the chat, and I’m sorry for not following it necessarily. We have 20 minutes left. If anyone wants to jump in the queue, again, you can raise your hand and I will try to look out for them, if you would like to make a comment on camera or on mic, rather. Otherwise …

Brian, go ahead.

BRIAN CIMBOLIC: Thanks, Reg. And not even really in particular for today, but the registries and registrars continue to do our outreach with the various stakeholder groups, SOs/ACs. So be on the lookout for future outreach sessions, and please do come to the table with ideas that you would like discuss. Obviously, the different stakeholder groups might have different ideas about how to approach DNS abuse, but we sort of approach this from the angle that, on any Venn diagram, there's going to be those areas of overlaps. And our time is best spend identifying the areas of agreement and focusing on the low-hanging fruit. And we think there's a lot more good that can be done in the coming months.

So, as those outreach sessions continue, please don't hesitate to share your ideas with us [on] where we can identify those areas of shared interests and we can do some good stuff together.

REG LEVY: Thank you for that, Brian. And thank you, everybody, for a really interesting debate. I enjoyed this and learned a lot. I hope that it was useful to other parties as well, not just the ones who asked questions directly.

I'm going to give it a few more moments before I give you 18 minutes of your day back.

All right. Thank you so much for your attendance. We will see you around ICANN72 but not, perhaps, in hallways. Have a great rest of your day, everyone. And we can stop the recording.

[END OF TRANSCRIPTION]