ICANN83 | PF – GNSO-CPH Membership with the SSAC
Thursday, June 12, 2025 – 09:00 to 10:15 CEST

SUE SCHULER: Hello, and welcome to the Meeting of the CPH Membership with the SSAC. My name is Sue, and I'm the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace. I will now hand the floor over to Beth, Owen, and Ram.

OWEN SMIGELSKI: Hello, everyone. My name is Owen Smigelski, and I am the chair of the Registrar Stakeholder Group from the domain name registrar, Namecheap. I think we're going to first start off here just introducing the chairs, and then since this has been the first time that the CPH and the SSAC has gotten together in a little while, we'll just go around, hear people at the table, introduce each other, and give their affiliation. So, I will pass it off to Beth. We'll introduce ourselves, and then.

BETH BACON	Hi friends. My name's Beth Bacon. I'm the Registry Stakeholder Group chair, and I'm with PIR.org, generally. Really happy to have some time, and thank you guys for fitting us in. I know it's a tight week. So, looking forward to chatting.
JAMES GALVIN	I'm James Galvin, SSAC's liaison to the ICANN Board, and with Identity Digital.
BARRY LEIBA	I'm Barry Leiba, SSAC.
MAARTEN AERTSEN	Maarten Aertsen, NLnet Labs and member of SSAC.
JOE ABLEY	Joe Ably, SSAC.
WARREN KUMARI	Warren Kumari, also SSAC.
ASHLEY HEINEMAN	God, I'm just irrelevant. Hello, everybody. I'm Ashley Heineman, GoDaddy, with the Registrar Stakeholder Group.

GREG AARON	Greg Aaron, SSAC.
STEVE CROCKER	Steve Crocker, SSAC.
KALINA OSTALSKA	Kalina Ostalska, Registry Stakeholder Group.
ROBERT GUERRA	Robert Guerra, SSAC.
VASYL BRATCHENKO	Vasyl Bratchenko, SSAC and Namecheap.
GABRIEL ANDREWS	Gabriel Andrews, SSAC and also PSWG.
ERIC ROKOBAUER	Eric Rokobauer, Squarespace Domains registrar and the RrSG secretary.
HONG-FU MENG	Hong-Fu Meng, Net-Chinese, Registrar Stakeholder Group and GNSO Council rep. Thank you.
UNKNOWN SPEAKER	Alex Sins [ph] with Fairwinds and the registries.

SUNCICA ROSIC	Suncica Rosic, NextGen.
RUSS HOUSLEY	Russ Housley, SSAC.
REG LEVY	Reg Levy, Tucows and the Registrar Stakeholder Group.
RICK WILHELM	Rick Wilhelm, PIR and SSAC.
GREG DIBIASE	Greg DiBiase, Registrar Stakeholder Group.
BRIAN CIMBOLIC	Brian Cimbolic, PIR registries.
SAMANTHA DEMETRIOU	Sam Demetriou, I'm with Verisign and I'm a GNSO councilor for the Registry Stakeholder Group.
DIRK KRISCHENOWSKI	Dick Krischenowski, .Berlin and .Hamburg registry.

EDMON CHUNG	Edmon Chung from .Asia registry.
CATHERINE PALETTA	I'm Catherine Paletta from Identity Digital and I'm the Vice Chair for Policy of the Registry Stakeholder Group.
JOHN MCCABE	John McCabe, registries.
MICHAEL BAULAND	Michael Bauland with Knipp and also Registrar Stakeholder Group treasurer.
PRUDENCE MALINKI	Prudence Malinki, MarkMonitor, RrSG or registrars and also GNSO councilor.
KAREN DAY	Karen Day with the Registries treasurer.
LUC SEUFER	Luke Seufer, EuroDNS registrar.
JEFF NEUMAN	Jeff Neuman, vice chair of admin for the registries and with Dot Hip Hop.

SARAH WYLD	I'm Sarah Wyld, I'm with Tucows and I'm the vice chair for Policy of the Registrar Stakeholder Group.
GEORGIA OSBORNE	Georgia Osborne, SSAC.
SUE SCHULER	Sue Schuler, secretariat for the registries.
ZOE BONYTHON	I'm Zoe and I'm the Registrar secretariat.
ROGER CARNEY	Roger with Registrar Stakeholder Group.
RAM MOHAN	Ram Mohan, Identity Digital, I guess registries, but also SSAC chair.
MEGHAN BOYCE	Meghan Boyce, RrSG and Newfold Digital.
OWEN SMIGELSKI	Okay, this is back to me. So now we'll go ahead and I guess jump into the topics. So, the first two are ones that the SSAC brought

forward and the next two are ones from the CPH. So, Ram, do you want to kick that off?

RAM MOHAN

Let me do that. And before we get to that, just a couple of things. First, I'm really pleased that we got the time on your calendar that you made the time to meet with us. For me personally, it's nice to be back among friends. And from the SSAC's point of view, we've got a clear plan to engage with each of the various groups inside of the ICANN community. One of the things that we recognize is we do the work, but it's perhaps as important after the work is done to be able to share that and to be open for questions and answers and respond, right? So, that's one thing, this is part of that.

The other part is for the last year and a half, the SSAC has moved to an open by default mode. So, for the most part, our meetings when we are at ICANN are all open. And so, if not here today, but for meetings in the future, I welcome you to come and participate and listen. We have lightning talks and there's some interesting topics that touch on abuse, touch on others. Some of it is pretty technical and engineering oriented, but some of it is not that way. So, I welcome you to come and be a part of it. It's also, after quite a while, we have a couple of folks who are registrars who are now SSAC members and that provides a really useful perspective. Jatin there, Vasyl there. So, it provides a really useful perspective for the work that we do. So, I appreciate the participation and the engagement.

So, with that, we just published SAC127 on DNS blocking. And we have the co-chairs of that work party, Greg Aaron and Warren Kumari here. So, I'll hand it off to them. We have a few slides on that. The goal here is to not talk at you, but to share what our findings are and then stop us along the way, if you have questions and if you have clarifications or comments and let's go forward from there. Over to you, Greg and Warren.

GREG AARON

Hi, everyone. This paper is a revision and update of two papers we did about 12, 13 years ago. DNS blocking is not something new, but it's something that continues to be done. There've been new cases and there are also some new technologies that allow people to do it or get around it. So, we've updated the paper.

Next slide, please. And next slide. So, what is it? DNS blocking is basically-- We're going to be a little technical because we know you guys know this stuff. Basically, it's when a recursive resolver gives a different result than would normally be given. So, there's an official response in the zone, but DNS blocking is going to tell someone who's querying for a domain name that either the domain doesn't exist when it does, or it's going to send the user to a different location. So, in some ways, you can say it's either changing the result or some people even say the server is lying because it's different from what's actually in the zone.

So, the goal is to prevent at least some set of users from using the domain name or getting to the content on that domain. And of

course, when you change the DNS result, it's going to affect not only web content, but also any other service that uses the domain name. So, we'll go to the next slide. That's what the resolver would say. We always have to have a pop culture reference here at SSAC.

Next slide, please. So, why is it used? One thing to remember is that blocking is a tool or a technique. In itself, it's neither good nor bad. You can use a tool well. You can use a tool precisely. You can use a tool poorly, like a hammer. Hammer can build you a house and protect you from the weather. You could also hit your thumb with the hammer. You could hit someone else over the head with the hammer. And you can use it locally or more broadly.

So, DNS blocking is used in certain contexts and in local contexts for security. And this is generally a good thing. And it's a common technique. For example, in browsers, you may not be able to go to a phishing site immediately. If the browser knows that you're trying to go to a phishing site, it'll pop up a warning. DNS blocking and DNS block lists are used to protect people from malware and firewalls and apps and a lot of other ways. And that's a case where it's known that there's blocking happening. There may be some transparency. A lot of people have chosen to use that service and use blocking in that fashion.

It's also used for content control. So, at your house, you may have your settings so that your kids can't go to certain kinds of sites. A very common technique and you can have services that provide a list of domains that get blocked in your house. Same thing in a

library. Some workplaces use it to prevent their employees from going to gambling sites while they're on the job. And again, a local use with knowledge of the network operator and usually the users.

Of course, the most controversial use of DNS blocking is when it's used for censorship to prevent people from getting the content that a government or someone believes is subversive, for example. And of course, sometimes blocking is mandated by courts. There may be a court order, for example, to ISPs that says you must block a certain domain. And that's how the ISPs implement that order.

Next slide, please. We want to differentiate DNS blocking from suspending a domain name, which is you put it on hold, it doesn't resolve for anyone. That's something different. But sometimes that technique is used to prevent people from getting the content. So, you know that every day, lots of domains are suspended for abuse and other kinds of problems. That's a different thing. And that's also different from domain seizure, which is where, for example, a court order comes in and asks that a domain be transferred to say law enforcement custody, because there's been some sort of a problem. And a lot of you have dealt with those orders.

Next slide. Just a note. This paper is talking about how the technology works and how it doesn't work so well sometimes. And so, SSAC is not making judgments about whether some of these cases of censorship or legal issues are correct or not correct. Of course, those kinds of conversations are best held in political and

policy forums. So, we're not trying to get into that in the paper. We're talking more about the technology and the implications of DNS blocking. Next slide.

WARREN KUMARI

So, next slide. So, as Greg said, DNS blocking works by changing the response on the recursive resolver. Fairly obviously to everyone in this room, this means that if the user doesn't query that recursive resolver, they're not going to get a changed response. They're not going to get filtered. So, the way that people generally get around or circumvent DNS blocking is they send their queries to a different resolver. In this image down the bottom, the normally the user's queries would go to this recursive ISP resolver on the bottom. There is a DNS block list. It may or may not block a specific query, but they can bypass all of this by just sending their queries somewhere else.

Next slide. So, a couple of ways this happens is users can just change their DNS resolver to a different one. There are a bunch of different options they could take here. One of them is they could use an open public resolver. There are a bunch of well-known examples of this, Google Public DNS, Cloudflare, Quad9, but there are also now some government-sponsored resolvers. The most obvious one of this is DNS4EU, which is a set of recursive resolvers being set up in the EU to provide primarily service to EU citizens.

What's interesting is Geof Houston's APNIC numbers show that currently around 21% of users are already using some of these

worldwide public resolvers. So, it's fairly clear that users know how to do this, and they can choose to change their resolvers to a different one. This is not technically hard. Increasingly, users understand what's going on.

Next slide. If you've watched any sort of streaming service in the past many years, you've likely seen ads for things like NordVPN or Surfshark or any of these other sets of VPNs. These are both to enhance user privacy, but from their advertising, it's also clear that the VPN providers are providing a means to bypass geographical restrictions. If you are traveling and you want to watch content in your home country, you can just fire up a VPN, and now it looks to the internet as though you're in your home country. Or if you are in your home country and would like to watch some content which isn't easily available, for example, Top Gear or-- No, Top Gear doesn't exist anymore. Well, some content. You can just fire up a VPN, and now you look like you're in the UK or wherever.

One of the ways that this happens is, or one of the things that the VPN providers commonly provide is different sets of resolvers. When you fire up the VPN, the VPN software hopefully replaces your system resolvers with their resolvers, and now you're bypassing the content blocking on those resolvers. Next slide. Oh, that's you.

GREG AARON

Okay, next slide, please. So, of course, one of the issues is over-blocking. Now, you can block at the TLD level or the second level or the third level, so increasing levels of precision. And, of course,

if you choose too high of a level, you'll end up blocking some things that are not problematic and people want to use. Also, if you put the wrong names on your blocking list, you may prevent people from getting to where they want to go, and it's a mistake.

And this will happen occasionally. For example, there is a case where, in Italy, the wrong name was added. It was actually an infrastructural domain. It was serving a domain that was a problem, but it was also serving Google Docs and some other Google services. So, when that name got added to the block list, the ISPs in Italy started blocking it, and that meant that people in Italy couldn't get to Google Docs, which was a problem until they pulled the name back off the list. So, that's the kind of thing that can happen if you're not careful.

Next slide. One of the problems, of course, is if you block something, you start to affect people that you didn't mean to affect. And it starts to create all kinds of problems. For example, here in Europe, you have a lot of countries. There are ISPs that serve people in more than one country. They have customers over the border. So, what happens if they get an order at that ISP to block something?

Well, the court order came from one country. How do I keep serving the people in the other country who that court order might not affect? You start to have problems like that. If you just block the domain entirely, you're blocking it over the border. And as we all know, the lines on the globe, on the maps, don't correspond with

how the internet works. We have different kinds of borders, and sometimes on the internet, none at all, really.

So, the second problem is, as Warren reminded us, blocking is going to be ineffective sometimes, because users can get around it. And some users know this, and some users take advantage of the Streisand effect. Once they know about something that's getting blocked, they want to go there and check it out. So, they'll use those alternative resolvers, they'll use VPNs, and there's always a chase.

For example, you may have heard that X was blocked in Brazil several months back. The Supreme Court in Brazil ordered it be blocked in Brazil because X was not complying with the law in Brazil. And as part of that order, we note in the paper that the Supreme Court Justice said, not only do you have to block X, but it's also going to be illegal to try to get to it through VPNs if you're a user. So, an interesting case.

So, as policymakers think about these kinds of things, they need to remember that any kind of blocking is going to be maybe partial in its effect, and they can't assume that blocking is going to work entirely. Next slide.

GREG AARON

So, one of the concerns is, in many cases, instead of just blocking a domain name, the requirement is that the domain name be redirected somewhere else. The general expectation of things like

that is there will be a web server at where it's directed, and it's supposed to pop up a page that the user will see, and then the user will understand why it was blocked and presumably be trained not to do that sort of behavior in the future.

The worrying part with this is we have moved most of the traffic on the internet to be HTPS, basically protected by TLS. If the domain name, for example, foo.bar.com, is redirected to one of these landing page servers, the server, fairly much by definition, isn't going to be able to get a certificate for foo.bar.com. And so, if the user tries to go to foo.bar.com, they'll get the popup saying the site you've tried to get to is not secure or is providing the wrong certificate. This means that users are likely to become confused and click through the "I want to go to that place anyway".

And all we've ended up doing is training users that if they get security popups warning them something bad is happening, they can ignore them or they should click the next button and see what's happening. So, we think that the redirecting users somewhere else is a really bad security practice because it undermines all of the training we've done, all of the like, please only go to HTTPS sites, please ignore, like if you see one of these warnings, please don't go through it. So basically, if you're going to do some sort of blocking, blocking is likely better than redirection.

GREG AARON Okay, next slide, please. And next slide. So, we make three recommendations, and we'll run through them. Oh, they've been

blocked. There we go, thank you. First recommendation is common sense. To anyone who's considering doing blocking at any kind of an entity, you do need to understand how it works and the potential implications of what you're doing. Okay, next slide. So, for anyone who's doing it, please follow these guidelines. And these guidelines are kind of based on the medical idea of do no harm.

First, you have to decide if blocking's going to fulfill your objectives. There might be other ways to accomplish your goals. Again, for example, if you're a policy or a lawmaker, you need to remember that blocking may not be entirely effective. Second, you should have a clear policy about what and how you're going to block things and a well-defined review and decision-making process. Your goal is to minimize risk. We're not going to provide specific ideas in the paper about exactly how it's going to be done because every entity is working a little differently, but they need to make sure that they know what's going to get blocked and how to take things off that list and so forth.

Third, minimize over-blocking or collateral damage to your users. Don't block them from going to things that are not problematic, basically. And then don't affect people outside of your administrative responsibility. Basically, don't block people that you don't have responsibility or authority over.

WARREN KUMARI

And then, next slide, our final recommendation is aimed at recursive server operators and DNS operators. There's a recent IETF RFC extended error codes which allows you to annotate a DNS error or any other DNS message with additional information. This has a number of error codes, one of which is censored, another one is filtered, another one is blocked. And what we're recommending is that recursive operators use these error codes to signal to the user and the browser why a specific DNS lookup didn't work the way they expected.

An incentive or advantage to this for the recursive operator is the user is more likely to understand what is happening and is less likely to blame the DNS operator for the fact the resolution didn't work. And I'm not sure how we're doing for time, but we have some hands already, and I think we're at the end. Next slide. I think the final one is just a QR code and a link to the document.

GREG AARON

Yeah, so if you do have time, we do encourage you to take a look at the paper. We have an exact summary up front and then all the details in the back, but the paper contains a lot of case studies, so you can see different use cases and what happened. There are sections on how people make their lists available or don't and why. There's a section on how people measure this phenomenon, so you can see what is being blocked in various systems around the world and so forth. Danielle, are you running the queue? No?

RAM MOHAN I'm happy to run the queue. Questions? Reg, go.

REG LEVY Thank you. Reg Levy from Tucows. This is interesting. And the security issues surrounding breaking the trust between your recursive resolver-- Sorry, I'm clearly in front of the mic here, so I'm trying to figure out how to not have feedback. The security issues of breaking the trust between your browser and the user and their resolver is definitely there, and the stability of the Internet is threatened by the splintering of the Internet in this manner. But your second recommendation seems to be for governments that are not incentivized to listen to it because their point is to splinter the Internet. Their point is to censor things.

So, how can we in this room help SSAC achieve their goals in terms of not increasing the splintering of the Internet through censorship in this manner? And secondarily, the third recommendation is for recursive resolvers, but if they're in cahoots with the government and often Google and even Cloudflare sometimes are paying attention to these requirements to censor in various areas, then how, again, do the people in this room help you achieve that goal?

GREG AARON Okay. There's a lot there, Reg. Thank you for the question. Let me make sure I try to answer each bit of it. SSAC early on when we were in the work party, we did not try to address the issue of

fragmentation because we realized that would be like a whole other paper and different people define and measure that differently. We kind of started from the premise that governments are going to do what governments are going to do. They exist. They do this kind of thing.

What they're doing it for and with motivations and whether some of them do things wisely in any given case or not unwisely is something we were going to put aside and simply recognize the fact that it's been something governments do for a long time and continue to do it. So SSAC is not taking any position at all on the propriety and whether a certain country should dial back what they're doing or anything like that. And we're not taking a view on whether this constitutes enough activity to be considered fragmentation because we haven't even gotten into that and it would take a while to figure out. Can you remind me of the second bit that you said?

REG LEVY

Okay. So, in each case I was curious what the people in this room can do to further your efforts in terms of this because the recommendations appear to be for governments who aren't going to listen, and for recursive resolvers who either you probably have better contacts with them or they're in cahoots with the government so they are not going to listen. Some of us in this room may be both registrars or registries and recursive resolvers but most of us are contracted parties here within the ICANN space. So,

this is excellent, super great information and I'm going to be taking this and publicizing it. I think ITC is doing something interesting in this arena as well but I'm trying to figure out what we can do to help you and to help the internet.

GREG AARON

So, as we finished up the paper, Akinori Maemura, who some of you know, took the paper into a discussion in Japan. The government of Japan is thinking about a blocking project. They're looking specifically at blocking child sexual abuse images sites in Japan. So, this paper has already been taken into a government discussion to inform them about how blocking works and then they'll decide what they want to do there. We're hoping that people do similar things elsewhere, which is understand the technology, understand how this is going to affect people. If you're going to do it, have good practices.

The public resolvers are an interesting situation because they serve people around the world. So, at the same time, those resolvers exist and are incorporated in a certain jurisdiction. So, when they get a court order, what do they do? They have to comply with the court order, but blocking on their service would affect a lot of people elsewhere. So, those kinds of dilemmas exist. We're not suggesting solutions are the right way to do things, but we are surfacing the issue that things get complicated fast.

RAM MOHAN Thanks, Greg. Ashley.

ASHLEY HEINEMAN Thank you. Ashley, GoDaddy. Kind of a little bit of a follow-up to what Reg was saying but also just to thank you for putting more material out there. I am actually of the opinion that this is helpful. And I also respect that you're trying to be apolitical about this. But to bring the political part in, we're dealing with a situation in the US where they're trying to legislate this as well. And our efforts to date have not been stellar because they're under the impression that this is easy. They go and speak to other governments. And when you speak to the other governments, of course, you're going to be like, yes, our program is wonderful. It's great.

So, I think having access to case studies is going to be really helpful. While I would appreciate it more if folks took the technical viewpoints and perspectives to heart, that is not really working. So, I think having more and more access to this type of material is going to be very helpful. So long story short, thank you. And if you continue compiling this type of work, I think that would be helpful as well to keep it fresh and current. Thanks.

RAM MOHAN Thanks, Ashley. One of the things that we're doing is engaging with the ICANN government affairs team to try and get this material in front of policymakers in multiple jurisdictions. We also presented this to the GAC, and that was well received.

WARREN KUMARI

And I think one of the things that the paper helps expose is governments have often believed that DNS blocking is actually going to be very effective. And if they request something be blocked, that means that people who really want to see it are not going to be able to see it. And it's fairly clear that users are able to work around this. We're also trying to make that when governments do require blocking or anyone requires blocking, they do it in the least harmful way and the least amount of over-blocking and side effects and similar. So, hopefully we can share this wider and we end up with less blocking, because even just from a technical standpoint, apart from an ethical one, it makes the Internet work less well.

RAM MOHAN

Thank you. Edmon.

EDMON CHUNG

Edmon here. So, I thank you, first of all, for the great report. I think it's a great start. But building on what Ashley was saying, I think some case studies of how things are happening is going to be very useful. Especially I'm actually interested, very much interested in the extended DNS errors' part. I think that's a very important piece of the puzzle for this. But I'm curious how well that is implemented. Do we have cases that that was well implemented and can showcase?

WARREN KUMARI

I will try and find the links and stuff. But I know that Google public DNS and I believe Cloudflare implement this for some set of things. They don't do all of the error codes, because there's a significant number and many of them don't apply. But some of the browsers as well are listening to these error codes and will provide more information to the user if they get it. There's a test page set up, which I will try and find and put in Zoom, which demonstrates some of the different blocking things.

I believe it's also implemented in most of the large resolver packages, the open-source ones. And so, you can annotate messages with these relatively easily. It's, I think, useful for a recursive operator to be able to signal to the user why this happened in these cases, but it also provides better debugging information. I guess, in full disclosure, I wrote this along with Wes Hardaker and two other people who've fallen out of my head at the moment.

RAM MOHAN

Thanks, Warren. Joe, did you want to speak about this from a Cloudflare perspective?

JOE ABLEY

Joe Abley here, Cloudflare. Not really, I don't work in the resolver team, and I don't work in the policy team and so anything I could say would be at best ill-informed and be probably unhelpful. So,

we can certainly get somebody from Cloudflare to contribute to the conversation if that's useful, but I'm not prepared to do that.

RAM MOHAN Thank you. Jeff.

JEFF NEUMAN Yeah, Jeff Neuman. Just a quick question. So, Warren, when you say it provides a signal to users, it really provides a signal to browsers or to developers, not to users. It's the hope that browsers and others would then take that error and translate it into something meaningful for the user. Is that correct? And then if that's the case, obviously Google has one of the biggest browsers. What are you doing to get out to them, the browsers and developers, to make sure that they understand and that they should then translate this into something meaningful for actual users?

WARREN KUMARI I was actually just reading through the public bug listing on what the current implementation status is for Chrome. I believe that Safari at least is already showing some of this information. I'm looking to see what the Chrome thing is. I'll try and put a link in soon. But yeah, there's a signal from the DNS system which resolvers can expose to their users. The extended error RFC also

provides a bunch of other debugging information, which is not likely of interest to users. It's only of interest to DNS geeks.

JEFF NEUMAN

And just to follow up on that, because I would think that governments or whoever's doing the blocking is going to want to control the messaging that comes back through that. So, there's specific wording, I'm sure, that if there's going to be anything, if there's going to be DNS blocking but something shows up in its place, obviously not the content that they're blocking but something else, that governments are going to want to somehow tailor that. And does it provide that ability to do that?

GREG AARON

Well, probably the assumption should be that a lot of governments won't. Like in the United States, if a court order comes out and says you have to block a particular domain name, the government's not going to necessarily then legislate, oh, you can't show that it's being blocked through an error code. What perhaps you're thinking about are countries with extensive regimes. But I don't know if we have an experience with that kind of thing yet.

JEFF NEUMAN

Well, and I think also the assumption that court orders are going to contain this, that's going to be-- I agree, it's something that would

be an ultimate goal. It's going to be a tough education to get attorneys and courts to put that kind of stuff in an order.

WARREN KUMARI

One second, I had it here a second ago. So, there are a couple of defined error codes that can be sent back with extended DNS error, which might be relevant. There is blocked, which says the server was unable to do this because it's on an internal security list. There is censored, which is the recursive resolver is unable to do this because of a requirement imposed by an external entity other than the resolver operator. And then there's also a filtered one, which is basically you have opted into this. So, for example, Cloudflare provides 1.1.1.3, which blocks adult content, and it could send back like this is filtered because you wanted it.

These are called blocked, censored, and filtered. Those were the names the IETF came up with. There is a way for additional information to be included as well. So potentially at some point there could be you send back censored, and then the government could have a please display please include this in the body of the message. It's unclear if that will actually be shown to a user or not. But we still think it's useful for the recursive operator to send this to help make it clear if they did it or someone else did it so you know if you should call up your ISP and shout at them, or if you should call up your local politician and potentially ask that things be changed. Or you could shout at them, but that might not be a good idea in many places in the world.

RAM MOHAN Thanks, Warren. That wraps up this particular topic. I want to switch to you, Maarten. And this is a work party that is underway right now in the SSAC. This is on free and open-source software. So over to you, Maarten. He's one of the co-chairs.

SUE SCHULER And as you can see, we're having some issues that the guys are working diligently to try to fix. But the slides do work in Zoom. Everyone should be in Zoom anyway. So, Maarten, you can go ahead.

MAARTEN AERTSEN In that case, we'll skip two slides. Yeah, and another one. So, we're working on a paper that describes the use of free and open-source software in the domain registration and DNS spaces. So, I think many of you know that a lot of infrastructure runs on software that is freely available on the Internet and is licensed under terms that allow anyone to use, study, modify, and distribute the result. And some of us had experiences in particularly Europe that where governments started to regulate software and infrastructure, they didn't consider open-source software at the start. And it turns out that if this stuff is everywhere, then interesting effects ensue.

So, this paper tries to make visible to an audience of policymakers the extent to which open-source software is part of the DNS and domain name registration infrastructure. And the idea is to make

this visible to policymakers, so if they are drafting new legislation or they're having regulatory discussions, they can take these characteristics of the software into account because they are not like physical products and they're not like proprietary software.

Next slide, please. So, we're looking at four areas, basically. Two of them are like survey style, presentation of facts, and the second half is more of an analysis and policy considerations aspect. So, in the first pie, which may be of most interest to you today, we're looking at what are people actually using. So, we contacted a number of you to understand what is in the registry backend. And a number of you provided information that is now in this report. If we haven't talked to you but you would like to be part of this report, please reach out to me or my co-chair, Barry, or any of us.

But the picture that is now starting to emerge is that most registry backends are proprietary. People build their own, but they're built on open-source components. For the DNS side, the view is a little bit different. Most everything is open source. There are definitely proprietary, but if you look at statistics, it's overwhelming. So, we do a landscape description. The second bit is to describe what are actually the characteristics of this stuff. We contrast open source against physical products, and we contrast open source against the DNS stuff that we're talking about.

The third bit is to address misconceptions. So, one misconception that was quite prominent in the EU was the thinking that there would always be contracts. And if you make policy and you assume

the existence of contracts, but people just download software from the Internet because they believe it's the best in class, then your policy is not going to work. And finally, we list some relevant risk factors.

Next slide, please. So, this is a bit of a teaser. We hope to publish ahead of the Muscat meeting. And if there's interest, I'll gladly present what we actually have to say because this was mostly the research questions. In summary, I think we believe that the continued use of this software basically everywhere is a strength, but there are risks to consider. Thank you for your attention, and I'll gladly take any questions you have. Oh, and if you want to be part of this report, please have a chat. It's just a table, but it helps us give accurate representation of the space.

RAM MOHAN Questions for Maarten? Okay, people have caught up on their emails. Let's carry forward and go to the next set of slides. These are Owen and Beth. These are just a few other things that we are working on. You've seen the free and open-source software. The other work party that has just been chartered and is underway, Rick Wilhelm is the chair of that, that's responsible integration into the DNS ecosystem. Rick, do you want to provide a quick update?

RICK WILHELM Sure, Ram. Thank you. Rick Wilhelm, PIR. Responsible integration is-- Do we have slides on this or not?

RAM MOHAN Yeah, we do have a slide. It's just not showing here yet.

RICK WILHELM Sure, or I can talk to Maarten's slides again. They're actually a lot better than anything that I would have produced. I don't even think I produced anything. Responsible integration is about if one is going to integrate any sort of an application into the DNS, into a registry system, then what sorts of things should that application be doing in order to, one, not break the DNS, but also not cause problems for the application's users as they are attempting to use the DNS to get to their application to avoid inconsistencies between the DNS and their application as time goes on.

This came about, people have been integrating applications in DNS for some time, of course, via things like resource records, DNS resource records and such. But one of the things that brings some urgency to this work is that there's a lot of work going on in and around the blockchain space that if there's someone here that's not aware of it, I would probably lose a bar bet. This is taking on increased urgency.

There's similar work going on in the IETF that's more technically oriented. The work that we're doing here in RIDE is going to be more trying to give guidance to ICANN stakeholders, specifically to registries and registrars, that if you're going to be working inside of your registry, registrar to integrate applications into the ICP-3-

rooted DNS, these are some things that you should do to avoid tears and disappointment, whether they be literal or metaphorical.

So, we are just getting started. We haven't done our charter yet. We're going to be taking a little bit of a detour we've figured out into some work where we're going to have to address some issues related to emerging TLDs in contrast to existing and launched TLDs. When we say emerging TLDs, these are TLDs that are either basically going through the launch and delegation process. Everybody here will also say, boy, that sounds a lot like the Next Round, and that's because you're right.

That's of course rather timely, in ICANN time, even though the Next Round is not tomorrow, but kind of today with the AGB coming up. So, we're going to be taking a little detour to work on a document related to that, then we're going to get on with RIDE, which has to do with the ongoing operations of the TLD, and then we'll be handling those considerations. Yeah, that's probably a good enough summary, try and keep it tight, and then we can take any questions. Thank you.

RAM MOHAN

Thanks Rick. I think the intent with the public comment is to provide some specific guidance for ICANN org as relates to the Next Round, particularly with identifiers in the blockchain space. Questions? Jeff?

JEFF NEUMAN

Yeah, thanks. This is going to be a tough one for you guys, well, for the community, because we have to be really careful to make sure this doesn't look like we're trying to protect our space or to not allow innovation. Because sometimes things that ICANN does tend to look like that. I like the title Responsible Integration, because it makes it sound like you're not going to say good or bad, but if you're going to do it, these are smart ways to do it. So, I think that's the right way to go about it.

But the last thing you said, it was either Rick, no, Ram, said that, or maybe I just misinterpreted, something about being different for new gTLDs and existing TLDs. I think we also need to make it clear that we're giving guidance maybe for the new TLDs, but we need to make sure that whatever we're going to say that needs to be or should be implemented in new TLDs must also be implemented in the existing ones. Otherwise, again, we kind of look like we're blocking what they'll say is innovation.

RAM MOHAN

Fair points, Jeff. Rick?

RICK WILHELM

Thank you, Ram. Thank you, Jeff, for the question/comment/concern. I agree and understand where you're coming from. Let me disambiguate the term new TLDs. I'm using that not in the form of as it relates to the term 2012 round TLDs. In the slides that we've been using in the committee and that I talked

about in the Lightning Talk yesterday, I used the term emerging TLDs. So, in other words, any TLD going through a launch, as opposed to any TLD in steady state operation.

So, we also, when we're talking about this within the SSAC, we completely agree with you on the point about not stymieing innovation. Within the SSAC, we're completely in agreement about not stymieing innovation in the DNS. We're actually looking at promoting and encouraging innovation within and leveraging the ICP-3 route because we think it's important. It's hard for us to see here now in 2025, but people have been innovating within the ICP-3 route for a long time.

Steve is very quietly sitting over there with his arms folded, but if we were to give him the mic, we would have to order in dinner because he would tell us extensive stories about the amount of innovation from the time that he started with the ICP-3 route when it wasn't even called, when ICP-3 didn't exist, when it wasn't called a route, when it was just sort of a dream and a promise. So, the amount of innovation that has gone on in the route already is extensive, and we on the work party, we'd like to see it continue. We just want to help everybody do the right thing so it doesn't get mucked up. So, yeah, I completely agree with your concerns and such. Thank you.

RAM MOHAN Thanks, Rick. Beth?

BETH BACON

Hi. Not a question. I just wanted to do a gentle time check. We are rolling gently into our last 15 minutes, and we have about five sides left in this deck, so I just wanted folks to be conscious. I don't want a chill discussion, but just noting that we do have about 15 minutes left, and a whole other slew of topics.

RAM MOHAN

Got it. Thank you. Edmon?

EDMON CHUNG

Yeah. Well, thank you again. I think this is a very important piece of work. I wanted to respond on one particular thing, because Rick mentioned almost in passing the ICP-3 when he was presenting and then repeated many times in response to Jeff. If ICP-3 is what we are building this on, which I think it's definitely the right thing to do, is SSAC going to take a look at the state of ICP-3? Because it was put in place many years ago, and it might need some update, at least in my mind, some update to that might be a good thing. So, if SSAC would review that as well and perhaps provide some advice or recommendation to update ICP-3, I think that might be useful as well.

RAM MOHAN

Thanks, Edmon. This is a great example from the community. If folks think we should do that, write to us, and it gets into our

hopper, and we'll look at that and see if there is value that we can provide if we have expertise and information and analytics that we can provide. So, Danielle, let's take that as a request, and we'll place it in the hopper. Thank you. Let's go to the slide that says CPH topics, and I'll hand it over to you.

OWEN SMIGELSKI

Thanks, Ram. Next slide, please. Okay, there's no more here, so apologies for that. So, I wanted to just hit first, I'm not sure how many of the SSAC members were able to attend the session that the CPH did on Monday, DNS Abuse Community Update. I'm going to drop the Zoom link or the sketch into the chat. For those who missed it, that was when we presented four proposals for community consideration on next steps for DNS abuse potential PDPs. So, I'm just going to summarize them briefly for those who were not there. Apologies for not having slides for this, but those are in that other presentation.

So, we had some guiding principles that the CPH had for this, is that we're going to build upon the ICANN definition of DNS abuse, which came from the SSAC, malware, phishing, botnets, pharming, and spam as a delivery mechanism. We wanted to make sure that they were narrow in scope, so that we wouldn't have the problem of just boiling the ocean and taking forever on that. We wanted something that was technology agnostic, and that was also business model agnostic. There's quite a variation, at least in the

registrar side, of various business models from a retail or a wholesale slash reseller model.

And so, the four ideas that we put forth, first is a requirement to pivot on actionable reports of malicious registered domains. And that would be where-- And these are a lot of ideas that registrars and registries are already doing, and similar to the DNS abuse amendments, we wanted to raise that floor for other contracted parties who may not be doing this. And so, pivoting is where you get an abuse complaint, say it's phishing, then you would do some other tracking to see are there other domains associated with it, either the account or the email or payment information or along those lines. And this would make this be more of an obligation. There's some quirks to work out on that just based upon the different registrar models, but it would be a way of ensuring that if one thing is found, that there would be others that would be found as well too.

Next would be API/reseller agreement mandatory clauses. Right now, it's just possible to set up ungated, unrestricted API access through a registrar, and this would put some sort of friction in there to ensure that anybody can't just sign up and start immediately registering tens of thousands of domain names. And then also if a wholesale registrar has a reseller to put some abuse obligations in there and push through down to those resellers and just to make sure it's clear that they do have to take action that the registrar itself would do.

The third one is mitigation of batch registered domain names generated by a botnet algorithm, and this would be more on the registry side because there would need to be some coordination that's a little bit easier to find on the registry side as opposed to through registrars. And this, I take the opportunity, as these ideas do go forward, we would like the participation of the SSAC because there's a very good intervention by Rod Rasmussen when we were discussing this one that made this idea seem a little more complicated. Oh, and we do have the slides up there. Thank you, whoever put those on there.

And there would be a little bit more complication there, and we certainly would value your feedback and participation with all of these. So just a little call out there once these do move forward through the GNSO Council, just to ensure that you guys are involved in that as well, too. So, this is kind of have like find ways to combat DGAs and coordination through ICANN. There's also some discussion that perhaps this doesn't need to be a policy effort. This could be done now through existing channels. So, there's things to consider about how we can approach this, combating DNS abuse on multiple fronts, not just through the policy development process within ICANN.

And then the last one is best practices for reporting phishing. We've done a couple of sessions, at least the contracted parties and the registrars, for the last two ICANN meetings, and we've come to the realization that a lot of people may not understand what phishing is or how to report it or what types of evidence is needed. We had

a good session, I think it was yesterday, that Sarah led. I'm looking at Sarah. Yeah. We had examples of DNS abuse complaints, and we showed them and talked through them, and we had various groups of communities.

And there seemed to be some broad consensus there about what was a DNS abuse report and then also what was not an actual DNS abuse report. But it's good to have these discussions, and perhaps we can use this as a way. And this wouldn't necessarily, again, be a PDP, but more of an idea or some ICANN guidance on how to do this and ways of it because the actions that a registrar or registry can take are only as good as the type of abuse complaint we receive. Sometimes, believe it or not, we receive a complaint that says, please take the domain name down, and that's all the information that's in there. Those are really not very helpful complaints. So, I will pause here and see if anybody has any thoughts or feedback or anything.

RAM MOHAN Owen, thank you for this. One overarching thing, how can the SSAC lean in on this? I mean, there's so much here that is directly linked to the things that we've been advocating for and are interested in. What can we do collaboratively with the CPH? Should we put a statement together that supports it? How do we do this so that it gets more amplification and more influence?

OWEN SMIGELSKI

We do have more ongoing discussions, and we also did want to solicit feedback. There was a link to a website where community members can go and see. Luc, if you could put that into chat. There is a website where we asked for feedback from the ICANN community about how to do that. And this is just getting ideas in so that we can review and collate and see what's more going on there. Or if we want to do a formal collaboration either with the registrars and the registries as well as the CPH.

We have DNS abuse teams as well, too. Maybe we can liaise that way. But certainly, the more that we can interact and participate and get your knowledge on that. Again, like I said, when Rod brought up some complications we didn't know, it was good to have that out there so we can understand the scope and the extent of certain things.

RAM MOHAN

So, you would like us to comment through the site first, and then after that you'll evaluate and see whether you want to do a collaboration.

OWEN SMIGELSKI

There's that, or we can certainly just reach out directly. That was just to say, hey, we want everybody to know what's going on. Please tell us. But if you would do something formally--

RAM MOHAN

It's your call. We're just happy to help. Guide us which way to go, and we'll direct our work and our efforts that way.

OWEN SMIGELSKI

Sure. I wasn't expecting the question. I'll circle back with you then. Gabe?

GABRIEL ANDREWS

Hey, this is Gabriel Andrews. First, I just wanted to express gratitude for the very proactive nature of this. I think this is actually one of my favorite things that I've seen happen in this particular ICANN session is that there's been multiple constituencies that came forward proactively and really expressed their ideas about what is feasible. And I know that in my various hats I've talked with a number of you before about ideas for this type of anti-abuse action, and we don't always get it right in public safety because we have some ideas about what we think could be palatable and trying to hit the same goal that maybe you are, but our suggestions just might not align with what's realistic. And so, when you come forward and you share what you think is realistic to hit those same goals, it's really appreciated. And I just wanted to say that.

And I had a specific thing that I would really like to have an opportunity to talk more about with you in the best practices for reporting phishing. I think one of the challenges that I've seen happen in my line of work is if we get really, really super lucky and see ongoing phishing campaigns, but then new domains that are

targeting maybe government infrastructure or what have you that haven't actually been used yet, but based off of the history of a campaign we're pretty darn sure are about to be, how can we start figuring out how to action those? Because that's a very different category of evidencing, but still it would be great if we had a path forward on the best case as opposed to just the reactive worst cases. And just food for thought.

OWEN SMIGELSKI Thanks, Gabe, for that. Sam?

SAMANTHA DEMETRIOU Thanks, Owen. This is Sam Demetriou. Ram, to just go back to your question about how SSAC can either weigh in on it or provide some support to the ideas that the CPH is proposing, the ultimate goal for these ideas are to feed them into the GNSO Council's small team, which is doing a gap analysis, examining places where DNS abuse mitigation practices can be addressed via ICANN policy development work.

So, they're gathering input from other parts of the community as well. So, to the extent that you can feed that input into the Council's small team, either expressing support for or potentially even refinements of some of these ideas and the other things that the small team is working on, I think the small team would really appreciate the SSAC's input on that. And however we want to

coordinate maybe in advance of that, I'm sure the chairs are more than happy to set up meetings and stuff.

RAM MOHAN Thank you, Sam.

OWEN SMIGELSKI Thanks, Sam. I'm not as well caffeinated yet this morning, so I appreciate that intervention. I thought there was another hand, but no, there's not. Okay, all right. All right, thank you. Anyone else?

RAM MOHAN I was particularly struck by the pivot analysis comment that you have. Personally speaking, I think that's really a useful thing to do. And my worry is that by the time it goes through the policy process and gets there, in the meanwhile, we have people taking advantage of that. And I wonder if there are things that we can do in the meanwhile while we're waiting for formal policy to get developed.

OWEN SMIGELSKI Yeah, just to respond to that, I think that a lot of registrars and registries are already doing that, and so that's like a best practice. And that's also one of the reasons why we want to make sure that these are targeted type PDPs that move forward and don't take five, six, seven years. These are things that could be done within a year or so. And there's a lot of discussion within the GNSO Council

and within ICANN about how do we get this there faster, how do we make these PDPs go quickly. And then also that can be also a formal model for other policy efforts afterwards outside of DNS abuse of how can we make the PDP process more effective. The AGP limits, that was a quick and done and dirty policy. That's what, three paragraphs, very quick. Those are things that we can do and should get back to doing. So, that's kind of the hope that we can do with that. Catherine?

CATHERINE PALETTA

Thanks. Ram, I think you raise a really good point there. As Ashley said in the chat and as Owen just said, lots of especially the people in this room are already doing this pivoting. Sorry, this is Catherine Paletta from Identity Digital. I forgot to introduce myself. And I'm just wondering, is there some maybe ideas from SSAC perhaps that you guys have about how we can share information about these the success of what we're already doing on pivoting? We don't want to get ahead of the policy work necessarily to say, look, everyone's already doing this, we don't need policy on it. Because certainly lots of us are doing it, but it's having a policy that would mandate it would be helpful and make sure that everybody is doing this.

And so, ways to communicate that, I think SSAC is very well organized and is very good at their communications. And so, love to hear from you about maybe there's data or something. It doesn't need to be right now necessarily, but maybe that's something we can continue to talk about. Thanks.

RAM MOHAN I really like that idea, and we'll take that as a follow-up from our side. Thank you, Catherine.

OWEN SMIGELSKI Thanks. Beth?

BETH BACON Thanks. This is Beth Bacon. I think circling back to the what can we do to support and coordinate, and I think Catherine's getting us down that road, is so let's just coordinate. I don't think that's a question. So, if there are ways that we can have a more regular interim conversations, that's great. If there are specific topics policy-wise or others that we want to coordinate on, I think that vocal support from SSAC is always really welcome.

And if there is something, especially for, as Sam mentioned, the gap analysis work that they're doing, to your point, Ram, if you could say we really think this is great. We could do this. What could we do in the meantime? But also to that end, we love the idea of doing a more efficient PDP. I think that even if there are areas of policy that maybe we don't agree on, which I'm not saying we don't because obviously we agree on everything. Why wouldn't we? The format and the approach, I think, is something that folks should really rally behind in a vocal way. So even if that's something that

could be a contribution to the small team, I think that would be appreciated.

RAM MOHAN I think we'd be quite open to that. These are topics that are close to our heart. I can't speak for the SSAC at this point. We haven't discussed this inside. But my gut feel is that it'll generate both interest but also support for coming in with you and doing this kind of lending our voice, if nothing else, to what you're doing.

OWEN SMIGELSKI All right, thanks. I appreciate that, Ram. Greg?

GREG AARON Yeah, real quick, two things. I don't think we have formal documentation around the pivot now, but we have documentation on a lot of other stuff. And I just want to throw that out as a reminder. Like I heard in the GAC session, they were asking, well, how do registrars validate and verify data? We have documents on that. And so, just as a reminder, if these questions come up on how do registrars or registries do X, it's always worth asking the question, have we drafted something on that? Because a lot of times we have. So, that's the first point.

And then on the second point of looking forward in this PDP process as the work of the small team evolves, I think it would be helpful to coalesce on proposals that have the best chance of

consensus and are narrow, right? So, there's going to be a lot of people with a lot of things on their wish list. There's going to be a smaller subset that will be both effective and have a high probability of consensus. And those are the things I think we should be collectively pushing for to get PDP over the finish line should that be the route that happens.

OWEN SMIGELSKI

Thank you. Greg, anyone else? Okay, just being cognizant of time, we did have some more topics, but this was the priority for us that we wanted to get out there and discuss. So, no need to jump into anything else in this last one minute here. So, I'd just like to thank the SSAC for joining us. We really do appreciate the dialogue. It was good to see us having those open back-and-forth discussions there, and hopefully this can serve as a basis and model of continuing interactions moving forward. And, again, we'll touch base about the DNS abuse stuff and how you can assist with that. Let's keep these meetings ongoing.

RAM MOHAN

Thanks, Owen and Beth. I'd like to actually invite you to come to one of our-- We have monthly meetings. To come to one of our monthly meetings to speak about these DNS topics because we can have an hour or so just dedicated and have an interactive discussion. So, if you're open for it, we'd like to invite you, folks

whom you who would like on that call. I think it would be very productive, and I'm happy to engage with you in that way.

BETH BACON: I think that would be fantastic, and thank you for the very gracious invitation. I think also it really will behoove us to have more regular communication. ICANN sessions are hard, so sometimes if we can get either actual face-to-face time. This has been really wonderful because I don't think we actually see your wonderful faces that often because you hide in the corner and do smart things. But I think, at a minimum, we can also try and do some of those interim calls. We have biweekly calls with the registries. We'd love to have you join us if there's topics for discussion and coordination.

RAM MOHAN: Fabulous. Thank you so much. I think next time we come in, we'll swap the order and have CPH topics first and SSAC topics next, and we can keep rotating. Thank you.

SUE SCHULER: We can end the recording.

[END OF TRANSCRIPTION]