
JONATHAN ZUCK: Good morning, folks. Welcome to the 53rd Plenary Meeting of the CCTRT. Is there anyone on the phone that is not on the Adobe Connect?

JAMIE HEDLUND: Yes, Jamie Hedlund. I'm on the phone and not yet in Adobe Connect.

JONATHAN ZUCK: Thanks, Jamie. Is there anybody with an update to their Statement of Interests? All right.

Then moving straight ahead, we are on the clock because we agreed at our last face-to-face to release an interim report for additional public comment that incorporates the changes introduced by the DNS report and the INTA survey. The timeframe for that was the 31st of this month, which as you can easily tell is well upon us. So, we're going to put some emphasis on the DNS Abuse report, and then when [David] returns from holiday on the INTA survey to see if we can make that deadline.

So, without further ado, Drew, I'm going to let you take it away to talk us through changes in the report inspired by the DNS Abuse study.

DREW BAGLEY: Thanks, Jonathan. Yes, as Jonathan said, we don't have much time to work with this, but we definitely have a lot of data now for this DNS Abuse chapter so that even though our timeline is short, we fortunately have a lot of insight we can now draw.

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

I went ahead and updated the DNS Abuse chapter and expanded it to include as a base all of the notable findings from the report, so this is from the DNS Abuse report, but not from the raw data.

I'm hoping to get my hands on the raw data perhaps this week so we can all take a look at that and draw even more conclusions, but in this draft that I sent around, it is definitely not ready for prime time, but at least pulls out a lot of the conclusions.

And namely, I think the way to think about this as we figure out how to have more inference from our other findings and whatnot is to think about the fact that there were these nine safeguards that were implemented as part of the New gTLD Program, and yet what the data shows first and foremost is that those safeguards alone do not prevent higher levels of abuse in new gTLDs than in legacy gTLDs which do not have the safeguards.

And so instead, but on the other side for the [doomsdayers] out there, it's not that all new gTLDs are bad and all new gTLDs are worse than legacy gTLDs. So, therefore those network operators blocking all new gTLDs would likely be surprised – or relieved maybe – by these findings.

And so I think one of the tasks at hand is to help explain instead what factors do contribute to a mitigation of abuse, and also try to figure out with the TLDs with high levels of abuse why is that so and why can that happen with all these safeguards at play.

And notably, there were two registrars that stood out as having extremely high levels of abuse. One had 93% of the domain names that they had registered to registrants listed on blacklists, and they

eventually lost their accreditation, but they operated for many months before that happened.

And then there was another operator that I checked last week and it was still operating despite the levels of abuse, and I'm trying to find that. Am I the only one scrolling, or does everybody has scrolling?

UNIDENTIFIED MALE: Everyone has scrolling rights, but I can make you a presenter if you wish.

DREW BAGLEY: Oh, no, I don't need to, I'll just find it.

JONATHAN ZUCK: That might be best, to make you presenter so that we're always looking where you're looking.

DREW BAGLEY: Right now I think it'd make people dizzy, but okay. That sounds good. Let me get to my stopping point, then we can do that. Okay, I think I found it.

Well, I will find it eventually, but basically what would be great is obviously everyone chime in, edit, contribute, but in particular for people who have knowledge from other areas that they worked on of things that we can pull in here to tie directly to some of these trends.

Particularly, I'm thinking with the section I want to find is compliance data, because this might be something where we can come up with a pretty good recommendation dealing with how ICANN Compliance might be able to deal with these situations quicker, or how perhaps registry operators themselves might be able to, or even with the existing roles maybe identify that perhaps there's room for interpretation that is allowing for this to happen.

There's a paragraph in the middle of the page on the screen that speaks about what I was mentioning with the two registrars, and the registrar I was thinking of that's still operating is [inaudible].

[inaudible] appears to be very price-specific as to their abuse, and there seems to be a correlation from what the researchers have noted in the DNS Abuse study and from what others have noted in the past between low prices and high levels of abuse so that when a registrar has a sale, then you see spikes in abuse and whatnot.

But for this particular operator, we're seeing very high volumes of abuse, and they've been – looking at the study – they've gone on over time, for very long periods of time, and yet they're still accredited.

So, there's something obviously not working as intended in the process. And so I think that's an area where we can figure out a recommendation. And then something else notable that I need to develop more and would like other people to help me develop more is defining spam where spam has already reached higher levels in new gTLDs than all legacy gTLDs. Whereas with other forms of abuse, there is certainly an upward trend and the rates may be higher, but not the total

number, not the total volume, because the total volume of new gTLDs is of course relatively low even though it's growing compared to legacy gTLDs, and so that's a surprising finding. And so that's something where I think we all need to read a bit more to figure out perhaps what sort of recommendation we could come up with that might help curb that phenomenon.

Otherwise, as you read through this you'll see also the big things that I tried to make a little less dense from the report findings, but those are some of the big things that I think we could actually turn into positive recommendations that can improve the DNS.

Does anybody have any questions?

I do have one recommendation at the bottom, actually. Let me explain that real quick.

A recommendation that I think would be for SSR2 but I'm curious as to whether anyone thinks I should recommend it to someone else – thank you for the arrow, whoever did that – and this is something I know Jordyn and I discussed, and I think Jonathan too after we had our meeting with the Registrar Stakeholders Group was that perhaps we could actually create an incentive structure based around – or maybe with the Registry Stakeholder groups rather – that perhaps we could create an incentive structure for registries to get their registrars to adopt good security standards with regards to abuse by giving those who engaged and implemented best practices a discount on the fees they would pay to ICANN for the registrations versus those who would

not do any of those things, they would still pay the standard rates, or maybe pay higher rates or something.

And so what that could do is really create economic incentives for best practices to be adopted. But of course, figuring out exactly what these best practices are is not in the scope of this review, except to the extent we could perhaps – we couldn't holistically identify all of them, but perhaps we can identify some from this data and instead that might be more directly tied to what the Security, Stability and Resiliency Review Team is looking at.

And so I'm thinking that that might be worthwhile venture for them to identify those best practices so those best practices would be available. I don't know if this is something where we just want SSR2 to take up this recommendation completely to look at and to look at if that even is a good and valuable thing, or if we want the SSR2 to perhaps identify the best practices, and then we want to make a recommendation to the ICANN Board that once those best practices are identified, then perhaps we can define how they should be adopted or whatnot because that might be within our purview. So, I'd love to hear some feedback on that.

UNIDENTIFIED MALE:

Drew, you have two questions. One from Jonathan and one from Jordyn.

DREW BAGLEY:

I didn't see the hands. I have the window [inaudible]. Jonathan.

JONATHAN ZUCK: Yes. Thanks. What is the extent to which we would be able to determine some best practices, examples or something to flush this out for SSR2? I'm looking at your recommendation, and I feel like that's the recommendation I would have made even if we hadn't read this study.

DREW BAGLEY: I think a huge one for example is [without names], the research found that they allow registrants to bulk register up to 2000 names at a time across 27 new gTLDs, and they can be randomly generated.

So, you look at practices like that, and it's kind of hard – at least in the sphere I operate in – to picture anything other than that being done for malicious purposes. And so there might be some sort of best practice where you would not allow for behavior like that, something that would just register DGAs that would be used for botnets and all sorts of other things. And instead, maybe you limit bulk registrations to a much smaller number and not allow –

JONATHAN ZUCK: Why wouldn't we just recommend that? I guess that's my question.

DREW BAGLEY: Perhaps a large company wanting to register a lot of domain names dealing with their intellectual property across something like those 27 new gTLDs, you could see bulk registration being legitimate. It's the randomly generated bulk registration up to 2000 that –

JONATHAN ZUCK: Right. I guess what I'm trying to circle in on is why couldn't we generate a recommendation from this fact?

DREW BAGLEY: Oh, we could.

JONATHAN ZUCK: [As opposed to] taking it down the hill.

DREW BAGLEY: Yes, we could. So, that's what I was alluding to, that we can identify some. I don't think we'd be able to holistically identify every single best practice that was set for this bundle of best practices that would get you your discount.

JONATHAN ZUCK: Okay. Jordyn, go ahead. It sounds like maybe you're responding in part to what I'm saying, that it seems too specific or something like that.

JORDYN BUCHANAN: [inaudible]

DREW BAGLEY: This was only one – the first recommendation I came up with. I'm trying to come up with more and I hope everyone else will too for this chapter, by the way.

JORDYN BUCHANAN: Yes. Jonathan is reacting to your – why don't we make a recommendation against that particular practice. And I think the reason why is because it won't do any good. You could get rid of that practice and then it'll be instantly replaced with some variant on it that doesn't fall directly within the language of the prohibition.

Like if we said, "You can't do bulk random registrations of domain names," someone would just – they'll say, "Oh, [inaudible]" You say, "I want to register Zuck as the seed name," and then it'll give you zuck1 through 1000 or something like that. And that wouldn't be random.

So, I think it would be trivially easy to work around that if the [motivation is] to give people a bunch of throwaway domains.

JONATHAN ZUCK: So, why don't we turn that around and tell me how you would make a recommendation that would help address that? I'm trying to get at not the [inaudible] necessarily, but the kicking the can down the road to [SSR2.]

JORDYN BUCHANAN: Right. I have a question first before we even answer that question.

JONATHAN ZUCK: All right. Go ahead.

JORDYN BUCHANAN: For SSR2, do we even think this would be properly within the scope of that review? I have paid no attention to SSR2, so I don't know what the charter and scope is, but I would be reluctant to kick a problem to them that they don't expect that it would be in the scope of things that they're trying to resolve. And I see Brian raised his hand, so maybe he knows the answer.

BRIAN AITCHISON: Yes, Jordyn. I've been following SSR2, and they are aware of the DNS Abuse study. They haven't really talked about abuse that much in their calls, so I think sort of hesitation to sort of kick the can for them might be warranted, at least in the near term, but it's not really on their radar right now.

JORDYN BUCHANAN: Thanks, Brian. Jonathan and Drew, I have sort of a long-winded theory I guess that I'll outline which might get us to a recommendation, but perhaps it's not my view of how to look at this. And I'll note at the start of this statement that there's a fair amount of speculation trying to connect the dots based on information you have, but there are gaps as well. But I think it mostly makes sense.

I think if you look at what's going on, you see the – and I think this has been speculated, I heard this from the SSAC when we went to talk with them, the DNS Abuse report guys both said they think both prices is a big driver of abuse.

I think within the Review Team, we've held that belief to be likely, although we don't yet really have a smoking gun that directly connects sort of a specific price [inaudible] low prices specific amount of abuse. But we've heard that anecdotally quite a bit.

I think that marries quite well to some of the other data that were seeing though. For example, Drew said like in spam, new gTLDs have really sort of taken over. It's not only that the amount of abuse is increasing, but it's that the spam has migrated to a large degree from legacy gTLDs to new gTLDs. It doesn't look like it's increasing the amount of spam, but it's certainly – the abuse has migrated.

I would guess – and Drew, I don't know if we break out – like I know for malware and phishing we break out compromised versus new registrations. Do we have that for spam as well?

DREW BAGLEY:

I'd have to go back and look because it gets pretty confusing, and part of the report was those things where there are things where they're even broken out by only applying to one blacklist, in some instances Spamhaus where they're talking about that and going through this trend. So, I think we might be able to figure that out from the report, but I'd have to dive back into it. I don't know [offhand].

JORDYN BUCHANAN:

I don't know if we have that data or not, but one thing we do know when we look the place where we break out compromise versus new

registrations, we see most of the activity in the new gTLDs is new registrations.

I would guess – without having this data and without knowing if it's in the report – that most spam is from new registrations, whereas with something like phishing it's really useful to be able to compromise someone's site and then be able to [start] providing credentials to that site [inaudible] an identifier to get the spam out the door, essentially.

And so it wouldn't surprise me at all if the vast majority of spam domains we're also new registrations and therefore since the new gTLDs are largely representing the new registrations, that that's where the abuses happen.

So, [piece] this together, and to me at least it basically says new gTLDs tend to be – there's a set of new gTLDs that are offering incredibly cheap prices – sometimes free, sometimes 99 cents – well under the cost of most of the legacy gTLDs, or essentially all of the legacy gTLDs which we hypothesize and tend to see are sort of charging right up to the price caps that ICANN enforces on them most of the time.

So, that puts them in sort of the high single digits wholesale prices range, whereas like I said, we might see retail prices as low as 99 cents or 0 dollars for some of these new gTLDs. So, obviously if you're a bad person and trying to do something bad, and you don't particularly care what domain you're using for that purpose and you want a lot of them, you would go to these new gTLDs that have really low prices.

What we heard from the SSAC is that we know that .tk which is a ccTLD that's been around for a while have been giving away free domains for a

long time, but they have pretty strong anti-abuse. But despite that fact, .tk consistently shows up really high in most of the abuse reporting that I've seen.

And once again, it's the same mechanism. If bad guys can get free domains, they'll prefer to use those, all things being equal, probably. And now they can get some cheap ones from some of these new gTLDs and you see the exact same mechanism playing out.

What we also heard from SSAC is that .tk has pretty aggressive anti-abuse stances and policies, and so the problem might be much worse on .tk for that, so we could see some migration from a provider like .tk that's giving away free domains that has strong anti-abuse mechanisms to some of the new gTLDs. That may be inadvertently aiding – either inadvertently or explicitly aiding bad actors in their effort to sort of gain market share or gain [inaudible].

I think we also see a bunch of new gTLDs that have either higher price points or stronger anti-abuse mechanisms. There are not many I think that have really strong anti-abuse mechanism. But you see various different deployments.

I know .xyz for example has really tried to up their game with regards to anti-abuse, and I think that's actually somewhat reflected in the graphs I saw. You see an initial [inaudible] surge of abuse on .xyz that seems to be trending down relative as a rate, so they may have effective anti-abuse stance. I don't really know, we'd have to dig into that more.

And so some amount of anti-abuse may be working, and more importantly I think price works pretty well as a deterrent to abuse, at

least when I'm looking at like the Spamhaus data, if I type in any TLD that costs more than a legacy gTLD in the marketplace, essentially the abuse rates were zero for all of them, because if you're a bad person and you're just trying to save money, you don't want to pay extra for a new gTLD.

So, the combination of all of this is that there's a pattern that plays out wherein new gTLDs that are really cheap – or TLDs in general that are really cheap – attract bad actors who want to register domains on the cheap. And therefore, we want to have stronger anti-abuse mechanisms in those circumstances.

And this comes back to the proposal that Drew and I were batting around in ICANN which was something like increase the standard registration price to, I don't know, \$5 or something like that from ICANN to the registry so that that would sort of force a floor that was relatively high in terms of cost per domain that presumably these TLDs aren't going to want to eat the ICANN cost. If the ICANN cost is relatively high, [inaudible] really low prices, but don't want to lose the opportunity for the consumers, the good people who want to register domains and maybe don't want to pay as much money. I think we could also [inaudible] real boon for people who want to get started on the Internet and don't want to have to pay too much money for their domain name. That's great if you can get a domain for free if that's your scenario.

So for registry operators that are willing to commit to strong anti-abuse stances – and once again, I don't 100% have an answer for what that means, but we'd have to think that they're meaning they would meaningfully address – so like you could take the [current

requirements] for registries and registrars to investigate abuse. You might create a new standard which is that the registrars have to actually have taken an affirmative stance to suspend domains if they're used for abuse or something like that. That might be one example.

I'm a little bit hesitant [to a statement] like that, because we know that a lot of the malware abuse that we see for example is compromised domains, and if you force registries and registrars to just suspend them, there's a lot of collateral damage to the legitimate owners of those sites.

But in any case, you could imagine some level of some affirmative – more strong, affirmative requirements and provide a significant economic benefit to registries and registrars in terms of much lower prices as a result of doing that.

In any case, I think that's the sort of framework that seems to make sense for me, which is to acknowledge the price as a big contributor, but also to acknowledge that price has considerable economic [inaudible] to consumers, and try to figure out how to sort of marry anti-abuse mechanisms to the opportunity to decrease prices instead of just saying, "Oh, yes, we want to really favor price and not care that much about the abuse vectors."

Sorry, I promised that wasn't going to be long winded, and it was.

DREW BAGLEY:

Thanks, Jordyn. It was great though. I think that was very helpful. And then while you were speaking, it looks like Brian came back to us to say

that the methodology suggests that the majority of the domain names on the spam blacklist would have been registered as bad – maliciously registered rather than compromised domain names.

JORDYN BUCHANAN: Right. Good. That matches my intuition.

DREW BAGLEY: So that matches it. I know. That would have perhaps changed it a bit. Yes, I agree with all of that, and at the very end I particularly like what you said, that especially we need to definitely add some language acknowledging the benefit for consumers of having low prices as we talk about price.

So right now in this chapter, the barebones version of the new DNS Abuse chapter where my priority was to extrapolate as many facts as I could out of there and knowing that I would hopefully – we would all have more time to add context this week after we got that out there. And so with the pricing, I don't have much written on that as it stands now.

However, the researchers have cited other research for that, so I think we can safely put that out there as a fact about the correlation between price and abuse from everything we now have with us.

And then I think we would need to figure out how we would – if we were going to solely take this on, our Review Team as far as the concrete recommendation, we have to figure out how would we even come up with whatever the numbers should be or who would redirect

that to come up with this happy medium number as to what the ICANN fees should be raised to.

And I guess that's what I struggle with, where I absolutely – you and I talked about this idea, the data matches up to suggest this would – our idea will curb abuse. However, I guess I'm still kind of lost as to how we would defensibly come up with a good number for that. Jonathan.

JONATHAN ZUCK: [inaudible]

JORDYN BUCHANAN: Sorry, Drew, I was just going to briefly respond and say I don't think we need to get the exact right number at this phase. I think if we throw the general framework of the idea out in the [inaudible] that'll give us a response from folks. And also, I imagine it would be sort of in the implementation phase that people would sort of peg the number down. So, I think that's sort of a future problem that we don't necessarily need to get to.

We can give examples of sort of the order of magnitude. Like we would have to be in this range of dollars in order for that to be true.

DREW BAGLEY: So, who would we recommend or address this recommendation to? Generally, the SSR2 as everyone suggested, if there's no guarantee perhaps that they're even looking at this issue in the same way we are, would we just make a recommendation you think for the ICANN Board?

JORDYN BUCHANAN: Yes, it's a good question. I think it would be worth asking [inaudible] whether they think this would belong in the subsequent procedures.

DREW BAGLEY: Or to a PDP.

JORDYN BUCHANAN: Yes. I don't really know the answer whether they would think that's in their charter or not.

DREW BAGLEY: And then from what you have seen so far – and I know that perhaps you haven't had much time to spend with this chapter, but are there any other recommendations that you think we should be making as a team? And especially even if they require us to develop the language a bit more to get there. But is there anything else that comes up? Because I anticipate I'll have more as I edit this this week.

JORDYN BUCHANAN: The other I guess sort of – I'll throw out a controversial statement I guess, which is I think most of the existing safeguards fall into the sort of feel good category, and I think this data somewhat bears that out that there – there were suggestions that came about either through community consultation or directly through GAC advice in some cases [inaudible] the process. And I think they were implemented in a way

that were intended to be not that burdensome to either registry operators, registrars or ICANN organization itself in terms of implementation. And I think recognizing the role of DNS intermediaries as opposed to like content host – web hosters or other people who have a much closer nexus to it.

But I would say it seems pretty obvious to me, like if you look at the rates of abuse that if there is a desire for abuse to exist on new gTLDs, the new safeguards don't really seem to have much of an effect in preventing them. And so from a cost/benefit perspective, I would certainly sort of make us question why are we doing these things if they don't seem to be working very well, and try to get ICANN to have a more cost/benefit-centric way of thinking through safeguards instead of doing it just to say, "Oh yes, we're doing something" even though it doesn't do anything useful. Like somehow figure out a way to ensure that safeguards are actually going to be meaningful before rolling one out like this.

DREW BAGLEY:

Yes. I've struggled myself with trying to kind of match up the safeguards with the data, because looking back at the old reports and discussions, of course the "issue" is that we anticipate with the new gTLDs was related to providing this – the fear is that this would provide a new attack vector for cybercrime and whatnot, then the recommendations that were developed address different parts of that but not the part that we really have the meat of now.

We have data that's showing the actual cybercrime in and of itself. However, the safeguards themselves, even the [inaudible] shows us [inaudible]. I still haven't seen anything to indicate that the safeguards were bad at all in terms of – they just seem almost like a bare minimum that maybe did not go far enough to directly address the real potential problems.

And so in such a way you might think about really technical things like prohibiting wildcarding, and even the DNSSEC deployment. The DNSSEC deployment as it was done of course was only required at the top level, and not required throughout. But now what we're seeing of course with this data is, oh, perhaps even if you have it at the second level, maybe it's just the bad guys going ahead and signing their own stuff. Who knows, the researchers don't make a definitive conclusion.

But I haven't necessarily seen that any of the safeguards were completely a waste of time or resources, just that there weren't enough safeguards in place to address the biggest problems at hand, I guess. So, have you seen anything to indicate that the safeguards appear to actually be a waste of resources or money, or actually have some sort of negative effect?

JORDYN BUCHANAN:

I think the negative effect is – I do think they're a waste in that I don't think they're actively harmful in that they don't make security problems worse, but I do think they're costly in terms of implementation and they don't seem to be doing anything useful I guess is the way I would express it.

So, I certainly know – and it could be as simple as just getting better guidance throughout the domain name system of what to do, but there is for example the Spec 11 (3)(b) requirement that registries actually sort of monitor their TLD or to see whether there’s abuse existing within the TLD. But then what do you do with that information once you have it?

The registry doesn’t have a direct relationship with the registrant. You could just suspend the domain, and if you’re sure the domain’s been registered maliciously, maybe that’s the right thing to do, but what if it has been compromised? Do you reach out directly to the registrant? Do you tell the registrar and hope they do something?

That whole chain of causality between the, “Okay, we discover there’s a problem,” and then being able to actually do something to remediate it I think is really poorly defined today.

So right now, you have a bunch of registries sort of doing a ton of active monitoring, but I think there’s very little follow-up there, and there’s been a huge amount of discussion within ICANN as to what exactly those requirements mean, how they’re implemented, whether there should be third party trust providers.

I would say thousands of person hours have been spent on trying to figure out exactly what that means, but I don’t think it gets at the heart of the problem which is there’s no real way for registries to be a meaningful actor in resolving most forms of abuse today. And until we solve that problem, I think sort of debating about what exactly the monitoring looks like is the wrong problem to solve.

DREW BAGLEY:

With that said though, I think perhaps we should revisit all that language to see if we could come up with recommendations about that because of – as you’re suggesting – how useless they can be in its current form.

For Spec 11 (3)(b), I definitely want to figure out a better way forward with something like that, but I absolutely agree that a big priority would be what you were speaking about a moment ago with regards to figuring out a good recommendation to deal with that idea we floated around in Johannesburg as far as prices go, since we do know that that appears to have the strongest correlation.

And then of course registration restrictions, which like with prices, whether there’s obvious benefit for consumers to have low prices, there’s an obvious benefit to consumers to have open registration policies for anyone to register them even though it has to be balanced, of course, with the effects that registration restrictions can have in curbing abuse and figuring out that happy medium.

And maybe the registration restrictions matter a lot less when prices are high, which I would guess would be the way I look at the research is about that, or maybe just see if I can look at the data itself and figure that out, even anecdotally like we’re doing, with plugging in some of those TLDs.

But yes, I think that’s absolutely a conclusion that these nine safeguards put in place do not appear to line up in terms of mitigating the actual

problems that have popped up in new gTLDs. Or I guess just the eight safeguards, because the one is just a proposed one.

Waudu, I see your hand up.

WAUDO SIGANGA:

Yes. Thanks, Drew. I'd like to make a comment about the recommendation, the way you're putting it here. I think it will not be good to really pick out on the low prices. You say [in your conclusion] that we should identify problem [inaudible] new gTLDs and registry operators with statistically low rates of abuse to create best practices for [inaudible] operators.

I think there's a limit there because some of these best practices may actually be coming from domains with high prices and some may come from domains with low prices. So, [inaudible]. I don't think we should assume that domains with low prices [are instantly having the] bad practices.

So, [inaudible] such practices would mitigate increasing domain name abuse associated with low priced and free registrations.

DREW BAGLEY:

Thanks, Waudu. [inaudible] We don't want the language to suggest an oversimplification of the correlation, so yes.

WAUDO SIGANGA:

[inaudible]

DREW BAGLEY: [inaudible] a very high priced one that costs \$1000 a year would likely not have any abuse, and so we wouldn't want that to be mistaken for a best practice.

So, one way around that obviously as we flesh out this chapter more is to revisit the data looking at whether we can determine from the data any lower price zones that also appear to have low levels of abuse, and perhaps still are relatively [open] with registration restrictions.

WAUDO SIGANGA: Exactly.

DREW BAGLEY: But perhaps they're employing some sort of helpful proactive anti-abuse practices such as perhaps preventing bulk registrations.

WAUDO SIGANGA: Yes.

DREW BAGLEY: Or perhaps screening against repeat abusers so that if someone is registering with the same credentials and they've already been kicked off for hosting malware in the past, that perhaps start scrutinizing those registrations. Or there might be practices we're able to see there, and perhaps that this would then be worded in a – perhaps then we could word that [sentence] in a better way like you're suggesting.

And then for the prices, as Jordyn is pointing out – and it goes to your statement, perhaps the practices aren't going to matter as much, but the price is a driving factor, so we should make sure [inaudible] are addressing those two separate concepts. So, thank you for that. That's really helpful. Do you have any other thoughts? Because I know you really spent a great deal of time with the original version of this chapter and really had a lot of good insight when we were working on that.

WAUDO SIGANGA: A few other things. [Not really a recommendation, but just in your paper, I want to say it's an early version,] but maybe a few small [inaudible] corrections. They're not big numbers, but from what I can see on page seven –

DREW BAGLEY: Oh, yes. [inaudible]

WAUDO SIGANGA: Okay, no problem. [inaudible] Page seven, can you [stay somewhere in the middle] there? [inaudible] results demonstrated the nine aforementioned safeguards alone – can you see those letters?

DREW BAGLEY: Yes.

WAUDO SIGANGA: Yes, I think [inaudible] changes everything. We can't do a guarantee.

DREW BAGLEY: Sorry, what was that?

WAUDO SIGANGA: [I think the word not should be there.] [inaudible] the word not between the – [inaudible] somewhere in the middle. [inaudible] slightly different from the one on the screen.

DREW BAGLEY: [I know the exact thing] you're referring to. Let me see if I can [inaudible]

WAUDO SIGANGA: Yes.

DREW BAGLEY: Okay.

WAUDO SIGANGA: Maybe we can make a note and [inaudible]

DREW BAGLEY: [inaudible] you're correct. Do not guarantee. That [should be] do not. Yes, that is a major typo. Thank you. [inaudible] that changes everything. And I'm sure there are more typos in here. Absolutely needs

more scrutiny, so thank you for that. I'll fix that. Thank you. Anything else? Jamie.

JAMIE HEDLUND:

Thanks, Drew. First of all, I thought your chapter was excellent, particularly given the time constraints. I think you and whoever else worked on it with you did a phenomenal job digesting complicated and sometimes confusing material.

My concern that I have and that I imagine will arise in the public comment is particularly with the last sentence of the recommendation, which seems could be interpreted as dictating outcomes that wouldn't normally come out of either a PDP or perhaps contract negotiations between ICANN and registries.

So, I think it is definitely the mandate of this group to identify abusive practices, identify shortcomings in existing safeguards and tools available to compliance to enforce against abusive conduct.

I share some of Jordyn's concern that you may identify one thing [inaudible] and just push it to something else. It's not covered. And that low prices in and of themselves are not necessarily conducive to bad behavior, especially when you look at how pricing is bundled with other services. But where there are free domains, there is often abuse. That's clear.

But I think where we can get into trouble is dictating what to do with the data once it's – or the best practices, and we might want to get away from that term because that also has a specific meaning in registry

contracts dealing with the Registry Stakeholder Group developing best practices.

Anyway, assuming you identify things that are clearly abusive and practices that should be avoided, recommending that the PDP or that the Board during directing staff to negotiate contracts consider an incentive structure I think is perfectly appropriate, but telling them that they should do that I do think oversteps the boundaries of the mandate of this group.

Having said that, nobody wants to enforce against some of these behaviors more than ICANN Compliance, and I know ICANN Compliance struggles with limitations on our authority and existing policies. So, I think it's absolutely important that all this stuff, the abuses and how they happen and where they are absolutely be transparent and surface to the community. I'll stop that one there. Thanks.

DREW BAGLEY:

Thank you, Jamie. I absolutely want your perspective on all of this for the dose of reality. And so with everything that you just said as far as obviously – I think the recurring theme with some of the things you always try to remind us of, of course, is actual scope of these contracts and the actual scope of ICANN's mandate.

But with all that said, either way we need to revisit language. This is a very rough draft, and so far I'm the only one who's worked on this chapter, which is why for better or worse it's a very rough draft. I know that all of us as a group are going to make it a much better chapter, but with that language – so if we incorporate a lot of what Jordyn and

Waldo just discussed with fine tuning the language or distinguishing between these price variables and separate perhaps registration best practices that might just include – I’m still throwing it out there I’m sure in an overly broad way that won’t be what we actually write, but it’s something where we’re saying, “Hey, stop letting these repeat offenders just register domains over and over again instantly and randomly generate a bunch of domain names.” And [inaudible] we come up with something concrete, we can get that language right, and we all come to a consensus on the fact that perhaps these ICANN fees could actually play a positive role even if we’re only talking about nominal discounts, but a nominal discount with a high-volume registry would create a pretty strong incentive structure to adopt certain things or even just meet certain metrics or something. Then once we figure out that part, how would you suggest we actually do the second part and direct or suggest the implementation of those ideas in a meaningful way where we would actually see some positive outcomes.

UNIDENTIFIED MALE:

So, thanks, and again you’ve done a phenomenal job at pulling together this paper. I guess at a minimum, it’s our obligation or mandate to identify the problem and make it clear to everyone in the community that certain practices lead to abuse, and there are ways of combating it.

The question then is, how do you get the community through policy development, through contractual negotiations to implement it? And I think that mandating a solution from a Review Team is not likely to go well, but figuring out how to make sure that the community does in fact give deference to these findings and consider what should be done is

something we should do, and that includes the subsequent procedure PDP and the future negotiation of contracts between ICANN organizations and the registries or registrars.

My guess – and it’s just a guess – is that tying it to fee-based incentives would be attractive to a lot of people, but again, one issue that some are going to raise is that the existing policy is that ICANN doesn’t regulate prices. This would amount to price regulation.

So, getting it to the folks who are responsible for developing the policy, negotiate the contracts, making sure it’s taken into account I think is critical.

DREW BAGLEY:

Right. So, and I guess even with this language, we would want to ensure that the language dealing with the pricing would be more focused on creating a tier with discounts rather than something that would provide any sort of vehicle for price regulation if price regulation is not warranted, and within the mandate from some other policy development that ends up going on in the future. Or even with that, [we] want to narrow our recommendation in that sense. Thinking out loud.

UNIDENTIFIED MALE:

I’m talking so much about the fee reduction incentive as the impression that you’re telling registries how to price or not their [inaudible] names.

DREW BAGLEY:

Got it. Okay. Yes, and then of course that's the other end of it, that still goes back to and it completely complements Waudó's point. Let us not wind to state something about price that mistakenly implies that a \$1000 a year domain name is the way to go because there's clearly no abuse and that alone is a best practice. So, thank you, that's really helpful.

I will absolutely rework this recommendation. If anyone else has a suggested alternative language to use that still tries to accomplish this goal – which of course then we'll have to come to consensus that we want this going out in the drat anyway, but we have a pretty small group today.

If anyone else has anything else that would help with that language, then certainly shoot me an e-mail. In the meantime, I'll try to rework the language with what I've heard so far today and come up with other ones.

And Jamie – and I can just shoot you an e-mail with specific questions I come up with. I don't know if going through this you've had any ideas about some even compliance data maybe that our review team's already been given that would be good to incorporate into some of the findings here, or other compliance data you know would exist that might be helpful for us. Because that might be really helpful for looking at some of these problematic registrars.

And we of course have the example of the one that eventually was suspended, and better understanding that process and how with

everything, with the existing rules and restrictions how it actually works, and potentially identifying ways to improve that.

JAMIE HEDLUND: Yes, I'll definitely shoot that back. And I think we'd be happy to give more [inaudible] the suspension of that [inaudible] registrar.

DREW BAGLEY: Okay, great. Thank you. And Jordyn.

JORDYN BUCHANAN: Yes. I was just going to say briefly, on the one hand I'm sort of cognizant that Jamie is correctly channeling a bunch of real perspectives that I think parts of the community are going to represent within ICANN.

On the other hand, I would be really reluctant to sort of – as I said before, I think most of the safeguards that exist now are roughly the result of a similar level of [sort of compromising] and saying, "We know there's a problem X, but ICANN's role isn't to do whatever, content regulation or something like that."

So, we'll put in something that's sort of halfway between an actual solution and not doing anything at all, and as a result you just get a bunch of stuff that takes some effort and isn't actually useful. And I think it would be a shame if that's sort of where we end up in our recommendations as well.

I think there's a way to sort of frame recommendations such that we don't necessarily – Jamie is right, this group doesn't have the ability to just give a recommendation and say, "Must be like this, otherwise..." Because we don't have any actual policy making authority within the ICANN Bylaws.

But at the same time, I think we could give like a recommendation saying, "Here's the set of influences that we think are causing problems, and here's the type of solution that we think would be useful. Here's an example, or here's even our recommended approach," and sort of acknowledge that our recommended approach is not necessarily binding on anyone. But at least it gives people a starting point to try to solve the problem as opposed to just sort of being a little too soft in the recommendation. That then forces the entire conversation to start from scratch in some future group, which I think would make it much less likely that we get a successful outcome.

JAMIE HEDLUND:

Jordyn, for what it's worth, I agree with that completely.

DREW BAGLEY:

Thanks, guys. Anything else? Because otherwise, as far as I see now we're 10 minutes past the hour and we still have a lot more to cover in the meeting as far as the other sections with Jonathan and Jordyn's papers. If not, then I will pass the time back to Jonathan.

JONATHAN ZUCK:

Thanks Drew. Thanks for your efforts on this paper and keep at it because we all agreed that time is short. And if I can folks, if you have not had the chance to read Drew's paper, please do so as soon as you can and write feedback as soon as you can because we are on a very tight deadline. So the time to make your comments is really in the next couple of days, so please read this paper when you get the chance.

Next on the agenda is just a revision of the data driven analysis recommendation and so this is hopefully quick, but what I did was just incorporate the discussions from the last plenary into the recommendation in the end. So a lot of what that was about was standardizing the use of language and not saying entity in some places and initiative in others.

And so this is the new text here at the bottom. I don't know if everybody has typed [inaudible] it's just me. But if everybody does, then please just scroll down to the left side.

I also have a little bit of text about the success of the recommendation, which is something that as a reminder, I think it's important for us all to incorporate into the recommendations that we've been putting forward, which is how do we measure the success of the recommendation as well. But take a look at this. I don't think you need me to read it to you and see if it addresses the issues that you had from the previous draft.

Any questions or further comments on this recommendation? Okay. I'm inclined to consider this approved in the absence of any hands or

[inaudible] comments in the chat. Okay. Thanks everyone. We'll get this into the form –

Go ahead, Jamie. There he is. Go ahead, Jamie.

JAMIE HEDLUND: This could be difficult. Now, just one minor thing you state in the middle where ICANN staff should proactively collect data to justify policy and issues. I'm not sure that ICANN staff's role is to justify anything, so I would wonder [inaudible].

JONATHAN ZUCK: Yeah, I know, that's right. Maybe it's a wording problem.

JAMIE HEDLUND: Just put the [inaudible] defensive a little bit.

JONATHAN ZUCK: No. What I want to do is put proponent policy into the defensive. I see what you're saying now so I will look at that. That should roughly take data necessary just to –

JAMIE HEDLUND: Just related to or you know.

JONATHAN ZUCK: I guess the point is what's the point of the data and one point of the data is to actually quantify a problem such that it's worthy of a new initiative. That's what I'm trying to get at. The other reason for collecting data is to understand the success of the initiative. So what I mean here is that one of the reasons to collect data is to justify a new initiative using data. So I need to take this back because I see what you're reading here, which is not my intention but that's the idea is that new initiative should be justified with data.

JAMIE HEDLUND: Yeah, they should monitor or audit them as well as –

JONATHAN ZUCK: Yeah, all right. I'll take into the swing of that.

JAMIE HEDLUND: Thanks.

JONATHAN ZUCK: Okay. Let's move on to the Parking paper. Jordyn, I don't know if you want to [enter] this at all or whatever if you want me to repeat. It's always difficult to present pros but if you want me to go over the way that I did yesterday, I can do that.

JORDYN BUCHANAN: Yeah, I think your [inaudible] yesterday was fine. Go ahead and do that.

JONATHAN ZUCK:

Okay, thanks. So folks, this is a paper that's gone through some variety of revisions, first by Jordyn with input from Laureen and then I took sort of the final swat at it, which in large measure was really just trying to turn it into less of a Christmas tree of passive language that results from community draft. So this is an attempt to kind of a more direct version of the Parking paper. Again, I really encourage you to read it in its entirety because it's not that long. But I would just draw your attention to a few things.

I think one of the number one goals of this section is to get across the point that parking is a – especially in the broad way that we've defined it is a significant practice. And in fact, the majority of domains fall into this broadly defined categorization of parking. So part of what we wanted to do is get across the points that it was a very broad definition. But given that broad definition, the numbers were so high that the Review Team found it necessary to at least look at parking, which is something that Kaili has been trying to draw our attention to since day one.

And so the first step at looking at parking was to see the degree to of the contribution of parking by the New gTLD Program. So our first objective was to see whether or not the situation had changed significantly with the New gTLD Program since it's our remit to look at the impact of the New gTLD Program.

And in doing that, we found that there was in fact a 20% difference in increase in this practice from the New gTLD Program. We don't know

why. It could be just because it's new but the new gTLD saw a 20% increase in this.

So that made it worth studying further and so then there are a number of hypotheses that could be developed about what the potential impact of parking is on the competitive landscape. One potential negative correlation to be that park domains are less likely to be renewed, which would suggest that the competitive effect of this new registration is being overstated in the other parts of the paper. And so that was suggested if we were able to identify a strong negative correlation between parking and renewals then we will use that correlation to somehow control how we counted these registrations when calculating market share and concentration.

Another hypothesis is that the subset of park domains that our pointers to existing domains or sub-domains are actually harbingers of domains that will be dropped. People don't drop domains right away because there's existing links and e-mails, etc. But over time and thus, so you might make the assumption that a new domain pointed to an old one is sort of a harbinger of that old one being replaced. And you therefore use that correlation to downgrade the way that you counted the legacy domain in the competition calculations.

And then finally, there's a potential hypothesis that the existence of speculation has a benefit to competitive effect outside of specific market share and concentration numbers which is simply that it helps to bridge newer and smaller niche-oriented TLDs to their full maturity, which if you remember, we mentioned also in the paper that it often

takes three years for a new gTLD to reach maturity and speculation could be helpful there.

So those are just some ideas or a hypothesis and so those are now included. We did one cursory test of negative correlation between parking and renewals. And we didn't find a correlation. So one of the tasks of the supervision was to kind of suggest that it would have been more interesting to find a correlation than it was not of find one. In other words, we don't really know anything more after doing this test. We simply didn't learn that there was a correlation but we don't know that one doesn't exist. And so trying to clarify that language was part of the purpose of this new draft.

And finally, the calculations that we did that basically excluded all park domains, which no hypothesis supports, got moved into the footnotes and downgraded from being in the text of the paper where the other calculations live. So they're still here but they're in the footnotes, relegated as a kind of extreme case because it's not only an extreme definition of parking but a very extreme control of parking that's not in any way reflective of reality or any legitimate hypothesis of the impact on parking.

So those are basically the changes to the report besides clean-up was to kind of make those things clear in the hypotheses, the nature of the test that we did and the graceful [inaudible], if you will, of the calculation of the market share and concentration to footnotes given the extreme nature of those calculations.

So that's the new paper. I'm happy to open up for conversations and discussion. Calvin, please go ahead.

CALVIN BROWNE:

Okay, just the small things that I saw there and it redirect to a domain in another TLD and I think it can just be to another domain. It doesn't have to be in a different TLD, a small thing. Let's go right [inaudible] anymore.

JONATHAN ZUCK:

I see what you're saying. Yes, I guess the reason for that language, Calvin, is because we were looking at the competitive impact of the New gTLD Program, which would be in some measure at least based on its impact on the market share of legacy TLDs. In other words, when we did these calculations, we saw that half of the new registrations or I guess it's been up to as much as 61% of the new registrations were new gTLDs versus legacy TLDs. And so the question is would you count those numbers differently based on parking? And so in the negative correlation to renewals then you might control for non-resolving TLDs because some percentages of them wouldn't renew. And that would seem that 61% number.

If you were taking this positive hypothesis that says that a pointer was a harbinger of a drop, then that would decrease how you counted the legacy as a domain, if that makes sense. Well, not in the new registrations, but in the existing market share registrations, you would discount the legacy domain and so that's why vis-à-vis I guess the new and the legacy is why it says in a different domain. I don't know if any of that makes sense.

Waudu? Go ahead. We can't hear you yet. I think you're on mute.

WAUDO SIGANGA: Okay. Just a few triggered items. I think it's page 7, we have the table with the parking rates. There's a rate of all new gTLDs. I think that should be 68%, not 58. Is that correct? On new gTLDs, this should be 68%.

JONATHAN ZUCK: Yes.

WAUDO SIGANGA: Parking rate.

JONATHAN ZUCK: Yes, that's right.

WAUDO SIGANGA: Okay. And then the other thing is on this last page, somewhere in the middle there, we have a bullet point that is talking about HTTP connection. You can see, right? Yeah, there's a sentence that starts with, "In a small number of cases." I would suggest to remove this phrase, "In a small number of cases." Just how these pages may also be used as a vector to distribute malware. When we talk about a small number of cases, again, we need to maybe [inaudible] the percentages that we're talking about, maybe we leave that out. [Just how] these pages may also be used as a vector to distribute malware.

JONATHAN ZUCK: Okay.

WAUDO SIGANGA: Okay, just think about that suggestion. Then there's another page, I think page 8. The page that follows the parking rates data, somewhere in the middle there, just before the big space in the middle. There is a sentence that I'm not quite sure about it. It says, "Despite high rates of parking, the new gTLDs overrule rates of malware propagation remain low in new gTLDs than in legacy gTLDs. But this troubling correlation warrants further attention from the ICANN community."

I don't quite understand that because it looks like we are trying to say that the fact that the propagation is higher in legacy gTLDs is troubling. And this is our focus in this study and what we are doing is with the new gTLD. So why should we be worried about troubling situation in legacy gTLDs? Try to think about that. Okay, thank you.

JONATHAN ZUCK: Is this meant to be, Jordyn, the higher rates of spam rather than parking?

WAUDO SIGANGA: What I think is that if overall rates of malware propagation are low in new gTLDs, then that's a good thing for us because we are studying the new gTLDs' impact.

JORDYN BUCHANAN: Right. Drew or Brian can confirm that the situation as described in the DNS Abuse paper is that in general, in new gTLDs, malware is less common than in legacy gTLDs. But if you look amongst the new gTLDs and look at parking rates, you'll see that of the malware that's occurring, it's more likely to occur in ones with higher parking rates, so very slightly.

So it's the fact that there are maybe some correlation between parking and malware but that is not as strong and effective as the overall trend, which is that new gTLDs have lower overall malware distribution rates than legacy gTLDs. And Drew or Brian can confirm but I think that's the correct summarization.

I don't know if it's good or not, but it is the correct conclusion that it remains the case that overall malware is less common in new gTLDs than legacy gTLDs. That's a separate statement from the fact that there is still some correlation between abuse and parking rates.

WAUDO SIGANGA: That's great. Okay.

JONATHAN ZUCK: So maybe we just need to maybe restate the correlation at the end of this paragraph. That might be the issue. That might be the cause of confusion.

WAUDO SIGANGA: Okay.

JONATHAN ZUCK: We just need to add it to the DNS Abuse findings portion of this as well, which is what you just said, Jordyn. So I'll take another [swat] of that.

Okay, other questions and comments? Yeah, Jordyn, I see your point about making the data up to date, the 58% may not be an incorrect calculation but a calculation based on older data.

Okay, we have other questions or comments. Drew, go ahead please.

DREW BAGLEY: Yeah, just going [with] what Jordyn said a moment ago. We should just add a few more sentences that give context to the precise [inaudible] the way Jordyn just described what the DNS Abuse study showed. Since there is this weak positive correlation between DNS abuse and parking, this is very weak. But the context that Jordyn presented is much more helpful where you've showed the overall trend of domain names registered maliciously to have them be correlated with malware blacklist in their correlation of parking. I think that would be a good way to address that there and then that fits into that broader consumer trust paradigm that's described in that opening chapter for this section.

JONATHAN ZUCK: Okay. All right. Thanks, Drew. Any other questions or comments?

Okay, let's move on to the roadmap to the final reports. So Jean-Baptiste, I don't know if you want to talk about the state of the current roadmap. We don't have a support slide for that. It's still in process, but remember, we have two tracks going on here. So we're trying to get to an interim report [add] for public comment just on the new sections related to the DNS Abuse and the INTA survey.

So be on your toes in the next week here as new drafts come out on that because we are trying to hit a deadline of August 31 for opening of a public comment period on those revised sections. But in parallel, we're also trying to make sure that we get recommendations done and updates to the paper for a final draft in the Abu Dhabi timeframe, which is pretty soon as well as you are running from [inaudible] travel from whom you probably heard.

So you've all got assignments that you received from Laureen and from Jordyn. Remember that assignments include going over the comments that are related to the recommendations on which you hold the pen, making notes in the spreadsheet about how that comment is being handled in the paper, and then with each recommendation, given the justifications of the recommendation and the measure for its success. I know that everybody is road weary at this point. We need to make sure that everybody's on top of this task because time is tight and we really want to get this paper out before Abu Dhabi.

So if anyone has questions about what needs to be doing, please reach out to Jordyn or Laureen about that but let's try to really get on top of the homework here in the final stretch, the sprint at the end of the marathon here.

Also, I really love to see our meeting start on time. It feels like we've just gotten used to starting at 10 or 15 minutes after the hour and there's no reason for that. The staff were on the call before the time so think of yourself that the person that lives close to the school that's always late. And if you got problems with connections and dial-ups and things like that, then you know that by now so start the process before the top of the hour so that we can try to get going sooner if possible.

Let's try to push through and think of these tasks and homework assignments done. Okay? Is there Any Other Business?

All right folks, thanks a lot. Thanks for your input on today's call. Bye-bye.

JORDYN BUCHANAN:

Bye.

[END OF TRANSCRIPTION]