ICANN Singapore Meeting
Best Practices to Address the Abusive Registration of Domain Names
TRANSCRIPTION
Thursday 23 June 2011 at 11:00 - 12:30 local

Note: The following is the output of transcribing from an audio. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.
Coordinator:

Marika Konings: Okay. Good morning everyone. We're gong to get started. Can I ask the operator to get the recording started?

Coordinator: Yes. We're good.

Marika Konings: Okay. Then we're going to kick this off. So welcome everyone. This is the Workshop on Best Practices to Address the Abuse of Registration of Domain Names.

I just want to brief you the agenda for today's session. We'll kick this off with a little background and initial outline of the discussion paper by myself and my colleague Steve Sheng sitting here at the other side of the table.

And then we'll go in through - into a panel discussion with - where the different members of the panel will present their respective perspectives on this issue. So we'll first have James Bladel from Go Daddy talking with the registrar perspective on this issue.

Jeff Neuman from Neustar will present the registry perspective. A commercial user perspective by Martin Sutton. Wendy Seltzer will be presenting a non-commercial user perspective.

Then we'll have a perspective as well from those involved actually in the development of best practices in other environments, which will be given by (Rod) Rasmussen and Greg Aaron. And after that we'll have as well open mike and then opportunities for asking questions or comments from the floor.

So we'll start off with a little background to this issue and an initial outline of the discussion paper. And although my name is here and Steve Sheng's name is here, I just want to emphasize as well that other members of ICANN staff have been involved in this effort and have been providing input; amongst others, Margie Milam who is sitting next to me and Dave Piscitello who's in the audience.

So I'll encourage them as well to speak up if, you know, if there's anything that Steve and I are leaving out of the list of issues or comments they want to make as part of this discussion.

So moving in first to the background. This is actually an issue that was brought to the GNSO Council by the Registration Abuse Policies Working Group. One of the recommendations that they brought to the GNSO Council was that there should be an effort that looks at the creation of non-binding best practices to help registrars and registries address the illicit use of domain names.

So the Council took action on that and in its meeting on the 3rd of February it actually ask ICANN staff to prepare a discussion paper on this topic so they could use it as a basis for further discussions and deciding on next steps to address this specific issue.

So in addition to the recommendation, the Registration Abuse Working Group also provided an extensive list of issues that they felt should be considered as part of that effort emphasizing that, you know, it should consider but not necessarily limit to these items. And not going through them because some of them we'll touch upon as well when we go through the initial outline of the discussion paper.

So staff has been working on that paper. Our initial aim was to actually get it out before this meeting so it could be actually discussed her. But due to workload issues were unable to complete it. But we wanted to take the opportunity to actually provide you with an outline of our most current thinking on what we believe should be in the discussion paper and the different topics that should be covered.

But already socialize those with the community and get some input from your perspective as well if, you know, we're addressing the right topics or if you have specific views on them because some of the items we're, you know, raising a number of questions or outlining different options. If there are any strong views on, you know, if there's a certain direction we should encourage more than another, we would really welcome that as well.

So we're really hoping to take the input from today's meeting from everyone here on the panel, also from those of you in the audience, to take that back and update that paper and then finalize it for submission to the GNSO Council.

So moving into some of the content. So I think first of all on the more general notion when talking about best practices, I think one of the notions or the issues we need to address in the papers. Okay. How do we - what are best practices? What are just practices and what makes something a best practice? I mean there's certain definitions that talk about practices as something that has been tested and has been measured and has a long value.

So but how does it work in the ICANN context? What kind of definition do we see as appropriate in this context where we're also talking about, you know, addressing malicious use? What would be appropriate in that context? So and which one of those practices that we know about - which ones are the best ones?

So should we develop a kind of a process for that and how we would go about that? As well considerations in relation to the scope and (like ability) of industry practices. As Steve will talk about later in this presentation, you know, we have identified a number of practices but do they apply to all or do they apply to certain segments of the industry.

You know, for example there might be certain practices that might be more appropriate for new gTLDs or small registries or big registries. So - and do we need to give consideration to that or are we just talking about a very general notion of best practices that apply to everyone?

And then there (comes) about defining the non-binding nature of best practices. And I think we had already some discussions on that on Saturday as well because what does non-binding mean? Do we mean that we just, you know, post it somewhere on a Web site and say oh, hey, you know, go and have a look at it and, you know, do with it what you like?

Or do we explore all the models where you say non-binding but also mean that you provide certain incentives for people to adopt those? Or do you say they're non-binding but as soon as you adopt them, you know, they are then enforceable.

So there are different kinds of models that, you know, we might want to look at and explore that, you know, might be appropriate and - because I think the real idea here as well is that we have something that helps registries and registrars address domain name abuse.

And then as well what is the role in ICANN of all of this? ICANN I think can have different hats. I mean we can just be a convener I think as we are doing here now trying to get the different groups together and share their points of views.

ICANN can play a role in, you know, gathering, collecting all these best practices. Could also play a role in updating, modifying, you know, providing incentives are the ways that ICANN can help in educating and promoting those best practices. So I think that's another item where we would really appreciate input where the community sees ICANN's role in this effort going forward.

The Registration Abuse Working Group recommendation specifically talked about, you know, resources needed for this effort. Specifically talked about ICANN resources and I think a question we're asking as well apart the standard, you know, policy staff resources at the GNSO has available for working groups. Are there other resources that are foreseen in this effort?

You know, we were going into lots of discussions are there, you know, I think we're talking further down as well about potential studies or surveys that might need to be carried out. You know, should there be more resources allocated to such an effort. If we foresee those, we can plan for those.

Community process. Again, the recommendation itself talks about a community process but there are different ways well of going about that. You know, the standard process in the GNSO is to go through, you know, a working group kind of model.

But in this area you might want to consider as well expert groups. I mean having the SSAC where there are a lot of technical experts that might provide advice. I mean the people as well that have been very active in developing in other sectors.

So what would be the best kind of model of taking this effort forward? What kind of community process would you need to really make the outcome broadly applicable but also ensure that you have broad input from the community in it?

And then there's (unintelligible) to talk about security and trust. I mean how do you share information between parties where in certain instances you might have confidential or information you might not want to share with the public.

You don't want to give, you know, bad guys a guide to what you're planning to do. But at the same time, you know, they probably know already how, you know, what the next steps might be and they plan for those things as well. So another couple of things that are more on the practical side. How can you make an effort like this work and what do you need in order to make it work?

So then talking about, you know, the scope of the best practices. I said the Registration Abuse Working Group already identified a list of efforts and I showed you that list already before. Are there any other areas that should be considered?

There's a - Steve Sheng will talk about a preliminary inventory of practices that we are identified. But there might be others that we, you know, have overlooked or are not aware about. So any input on, you know, what is already out there would be helpful.

The discussion paper - the focus will obviously be on gTLD registries and ICANN accredited registrars. But consideration might also be given to how this could apply to resellers or how this can be promoted vis-à-vis resellers as they're often involved as well in these processes and they might benefit as well from many practices in this area.

And then we came up with a whole list of issues I think from our, you know, going through the different items and thinking about this, some other issues that we think should be considered as part of this discussion.

So one thing we spoke about as well there are many other industries that do already have models for industry practices and, you know, how to create them, how to update them, mechanisms for enforcing or encouraging them as well assessing their effectiveness.

So should we be looking at some of those other industries and try to see if there are any models or any elements that might apply or might be a useful starting point for of course this initiative that we're looking at?

Another item as well like, you know, and how much detail do we need to go? How high level should these best practices be? And - or how detailed should these be worked out?

Or there you might need to look at as well in areas of what information do you provide publicly and what kind of information you might need to, you know, keep more at a trusted level to ensure that those that need to know how its done know it but it's not something that is, you know, a guide of how to avoid certain things.

And very important as well like how do you update and make sure that ongoing improvements are incorporated? Because especially in these environments very quick changes. So how do (can) make sure that practices that we develop and then, you know, if we have a system for labeling those best practices, how can we make sure that they always keep up to date and remain relevant?

We spoke already before about, you know, how to move from getting actual practices into best practices, what is required there? I think that again talks as well about how can we assess, you know, what works, how effective things are and (comes) to, you know, cost versus benefits.

Is there any guidance we should give on certain practices you might, you know, they're very costly, they might get little impact; these are very easy measure but get a really big impact. So is that the kind of guidance that should be considered as well as part of this effort?

And I think - so we spoke about as well before I think, you know, promotion and dissemination would be crucial. Once we get to the stage where we come to a kind of model or system for creating, developing these best practices and having them out there, how can we make sure that these are incorporated?

What kind of incentives are needed? What kind of mechanisms need to be applied? How can we work as well I think with, you know, registrars and registries and maybe some of our stakeholder groups to get those programs out, help with education and make sure that people understand, you know, why we're doing this and what the benefits are.

I think there's some as well specific questions as well talking about, you know, how you identify trusted abuse (reports), talking to each other about liability?

And there's a question that also comes up in when you develop mechanisms how can you make sure that you have the appropriate balance between, you know, addressing abuse but also ensuring that innocent parties don't get harmed or caught up in the mix.

So then I'll hand it over to Steve who will just talk a bit about - and it should say here and I actually forgot to change it here because we're saying preliminary inventory of best practices but just to emphasize these are practices.

I think we just want to make clear we're not saying these are the best practices that everyone should adopt and these are great. These are just a list of practices that we've been able to identify from a number of resources that we think might be considered as this effort goes forward as a first step.

And I'll hand it over to Steve to talk a little bit more about what we looked at and what we found.

Steve Sheng: Thank you Marika. The approach we take is first look at the eight areas that the Council requested in their report. So for example, you know, practice for identifying stolen credentials, for identifying and investigating common forms of malicious use. So there are a list of eight areas that the Council asked - the report asked. And then we look at the current practices that has been identified primarily by three sources.

The first is advisory committees of ICANN primarily from SSAC, the Security and Stability Advisory Committee. The second one is the current registry or registrar practices. So for example, some of the anti-abuse practices that has been put in place for some registries and registrars.

And the third course is, you know, industry groups such as the APWG and the Messaging Abuse Working Group. So taking those - the eight categories given and look at the - each of these reports - going to each of the reports and look at what are some of the practices being suggested. Next slide.

So this is a preliminary inventory for this list. In this we have four columns. We identify, you know, what that practice is being suggested and what year they are. Because the thread landscape is changing quite rapidly. So it's important to have a reference and know when that suggestion is made to evaluate whether it's applicable to a current state. The third is identify its source and its intended audience. So that's a preliminary list.

What we would really like feedback on is, you know, as Marika mentioned earlier, whether there are some important sources that we did not consider. So that's one thing.

And second, whether, you know, we should add more columns to this table, you know, other than the four columns here identified. So those are the types of feedback will be really helpful.

I think that's it Marika.

Marika Konings: Yeah. So I think one of the questions that was raised and that's something we might, you know, welcome - we would welcome your input on as well. Some people asked on Saturday when we gave an update to the GNSO Council on this topic, how - have these practices been widely adopted in the industry? Or - and how are they being used?

And I think at this stage, you know, we don't really have any insight into that. I mean it's - so if anyone has any feedback or, you know, maybe studies have been done.

And maybe looking as well I think to (Rod) and Greg maybe in their presentation they might be able to talk about some of the APWG recommendations or practices and they might have a better idea of, you know, if these have been widely adopted and what kind of process they might have in place for, you know, checking who's using them and as well getting feedback on how they're being used and how effective they are in addressing abuse.

So I said before, you know, this is - this effort is really intended to have, you know, learn from the different perspectives around the table and from you in the audience. Really hoping we can have a quite free flowing discussion on this.

Based on the feedback we've received or will receive today, we'll update the paper and submit it to the GNSO Council. We really hope as well to be able to provide them with some concrete recommendations on next steps on how to take this effort forward. And again, I really would appreciate your input on that as well. And then it will be for the GNSO Council to consider how to move forward with this effort.

So before going into the next presentation just looking at Margie and Dave, I don't know if they want to add something at this stage.

Margie Milam: No, I think you covered it accurate - pretty well. I mean the staff considerations that we've had at this point, I'd be interested to get reaction from, you know, the panel. And so we'll interject as the discussion goes on.

Marika Konings: So I think that we'll move on. I mean do we have questions yet? I don't know if there are any questions of like clarification because I think I would like to leave the overall discussion or comments on some of the items that I covered to the end. But if there are any questions on, you know, something that wasn't clear in this overview, feel free to raise your hand now. And otherwise we'll first go into the panel discussion. And James your up first.

James Bladel: Thanks Marika. Thanks for - and thanks to the rest of the staff for kind of laying the landscape and setting the context for what we're trying to do. And didn't prepare any slides. I have a few talking points here. But I was hoping this would be kind of an interactive session if not now then later on in the groups.

So I wanted to - I'm sorry. I'm James Bladel from Go Daddy. And I'm here to bring a registrar's perspective. Certainly registrars are a broad and diverse group. So claiming to speak for one or even many registrars is probably dangerous. So I'll just say that here is a generic perspective from a generic registrar. And we'll see if we can flesh it out from there.

I do want to challenge one thing and it's maybe a small point. But it's the title of this session. Is - can we pull that up somewhere? It's just - it says something I believe the session is...

Marika Konings: (Unintelligible).

James Bladel: ...sorry. The session is Registration Abuse. And I just want to point out that - or I'm sorry. What is the actual? Go ahead. Use your mike. This is important.

Marika Konings: I have to put the caveat that I think we're only allowed to put like I don't know, a very limited number of characters in the title of this. So I had to really abbreviate that.

James Bladel: Well that's good because I'm going to help you make it shorter. Because this is about the abuse of registration of domain names. But in fact in many respects there's really only one way to abuse a registration and that is to commit the one crime that is defined in ICANN policy, which is to have incomplete or inaccurate WHOIS data.

What we're talking about in effect the abusive use of domain names which is a different animal and implies services and content and all kinds of other things that are somewhat beyond the reach of what ICANN can just put in the paper and address through policy.

So wanted to point that out because I believe that in some respects, and this is a position that we took on the Registration Abuse Team, is that ICANN is not always the most appropriate or most effective venue to address abuse issues.

You know, for one thing it has an obligation to conduct its deliberations out in the open and be inclusive. And right away those are two things the transparency and participation that I think most of the security experts on this panel and the community will tell you are not necessarily the best way to deal with the bad guys.

But it can serve an important role in bringing a cross section of this industry and ecosystem together to share ideas, exchange some of their best practices as we've discussed and facilitate some cooperation and dialog in this area, which is important.

As a registrar, we're on the front lines. And we have not only the burden of addressing these issues facing them head on. But we also have the burden that we are competitive businesses. So additional cost, additional risk, additional liabilities are definitely not something that we can just disregard or treat lightly.

I think that one example that we've given if I knew there were 1000 spammers on a given network and I had a system that was 99.9% accurate at addressing those, you know, from a registrar perspective and I think a community, that's a pretty good system.

However, that one false positive could lead to a lawsuit that could wipe out the gains at least commercially and all of the efforts for wiping out and no one gives you a gold star for having killed the other 999 spammers. You have to pay the price for the one false positive.

So in that respect, the economics on combating online abuse, the economic model's upside down. It is expensive and risky to be a good actor and a good citizen in this regard. It is cheaper and less work to just turn a blind eye to some of these activities.

So I think that that's something we need to be aware of and that's something that we need to address and I think Marika talked about how can build incentives for the good guys, build, you know, build sanctions I guess for the bad guys. But all that's typical - difficult to do, you know, outside of a policy context.

So with that, I just wanted to put out some just very generic best practices. I hope there are registrars or other service providers in the audience. And I hope that they can help me build on these during the Q&A. Maybe see some heads nodding as we go forward.

The first thing is is that, you know, registrars and other service providers need to designate who in their organization is responsible for abuse. You know, that needs to be a person or a team. And it needs to be very clear. This needs to be communicated to other industry perspective - other registrars, registries, law enforcement and security firms.

The pushback that I hear on this sort of issue is well, I'm a small operation. I'm just a one-man shop. Well, the answer is then you are the person that is responsible for abuse and you get to wear that hat along with the other 12 hats that most entrepreneurs wear.

Registrars should develop standard operating procedures and use them consistently and uniformly. I mean that is one of the - I'm not a lawyer but I know I'm surrounded by them up here on the table and I would say that inconsistency and the non-uniform application of policies and practices are what can get you into trouble if you're ever in a situation where you need one of the (ladies) to my left or right.

Abuse and abuse issues and abuse activities need to be given a high priority within an organization especially emphasizing speed and quick action. The harms of online abuse can multiply over hours or days of inactivity as well as most of the bad guys out there know which service providers are slow to respond.

And I think that - a person who opened my eyes to some of this stuff was Mr. Aaron here as I sat through some of his APWG presentations. They know where the weak spots are and they're learning. And they're smart. And in fact the bad guys in many respects are several steps ahead of the folks coming to - trying to make this difficult for them.

This is another important point. Make sure that all registrars are required to have a registration agreement with their customers and associated with each domain name. But you know, there's some discretion I think on what that can contain. And I think it's important that registrars construct those agreements to give them the necessary latitude to combat abuse when they find it or when it's brought to their attention.

And this also extends to other services. So for example, a lot of registrars are also Web hosts or DNS service providers and maybe since those things are slightly outside the purview of ICANN policy, maybe those agreements, the terms and conditions can be developed in such a way that gives the registrars the ability to act or remedy situations in other services.

So for example, if you feel like well maybe I don't have the tools I need in my registration agreement to address this as a domain name registrar. Maybe I have the ability to take down the Web site as a Web host.

And then the last one I think is - for registrars is already happening if you're in this room or listening on the audio cast is to get involved. There are a lot of groups. There are a lot of industry consortiums both public and maybe some that are not quite so public that are bringing people together to address these issues and bringing organizations together so that they can get the benefit of economies of scale in the resources and that they don't have to fight all these battles on their own.

At Go Daddy were involved in not only APWG and ICANN but all of - a number of other different groups that are going to be presenting here and were mentioned in Steve's slide there.

But I think that together this industry with those groups, with law enforcement, you know, we can all kind of pull together and disrupt the - frustrate the activities of online abusers and disrupt the economics of online abuse.

Marika Konings: Thank you. And we got to the next speaker Jeff.

Jeff Neuman: Hi. Good morning. I'm Jeff Neuman. I'm with Neustar. Like James I'm going to speak primarily on behalf of my registry and not necessarily on behalf of all the other registries and also from a gTLD perspective more so than a ccTLD perspective although we actually operate one of each.

You know, registries are in a very unique position, you know, that we - mostly deal - at least gTLD registries mostly deal only through our registrars. In fact when we do take actions against abuse, oftentimes it's a visceral reaction by the registrars if we're going to do that directly.

So, you know, if we do take action and take down names, we sometimes get a lot of flack from our registrars for taking action against their customers. So that's something that we all need to be mindful of.

But that said - all that said, as a registry, we have a unique insight into activities that go on across registrars and really we are the protectors of our brand. You know, as gTLD registries we actually have much more of an incentive to stop the abuses that go on than a lot of our registrars.

Right. If we're a small registry, you know, let's say .biz versus a .com, you know, we have much more of an incentive to stop any abuse in .biz than a registrar that may only sell a couple names in .biz every month. And so that's critically important.

And all of that said, as a registry, you know, I'm here to say that we actually do have a lot of practices or best practices that as registries we already engage in. You know, Neustar for example has policies against malicious conduct on malware, phishing and pharming. We have policies against child pornography and for the prevention of child pornography on our domain.

We are engaged in a number of groups now for stopping the illegal sale of pharmaceuticals online at least within our spaces. Policies against spam. You know, (unintelligible) working group. We are an active participant in that. We have policies against fast flux and we monitor and detect and delete those names.

We have anti-tasting policies and we do other things like monitor for abnormal traffic from registrars which is usually an indicator of either something going wrong with the registrar or could be something like a denial of service attack.

But what I want to talk about now is just kind of some general principles. I know James went into some fairly specific even though they said they were general. These are more principles that I think in this environment of how to go forward with developing best practices.

And the first thing I want to say is actually competition is one of the best ways to generate best practices. If you think of what the world was like before there was competition amongst registries and when there was only one registry or one registry operator. You know, since then we've - you know, there was no concept of a thick WHOIS in gTLDs prior to the .biz, .info and the other gTLDs that were introduced back in 200.

There was no uniform standard for the communication between registries and registrars. There was nothing called or it was just in development call ETP. And in fact it was - I'd like to say because of the competition we actually got the incumbent operator to do - to go on to ETP.

Things like redemption grace period, I think that is a classic example of the best practice. That was never a consensus policy. But, you know, the allowing for domain name registrants to restore their names if they were accidentally deleted. That was - that came out of the registries and registrars working together.

DNSSEC. You know, I think again competition or even the market itself is a good indicator of - or for developing best practices. You know, DNSSEC was something that had been around for, you know, ten years developing - or in standard phase but it really took some incidents in the market and realizing the vulnerabilities to actually speed up the implementation of DNSSEC.

So registries actually already engage in best practices. You know, we - just as James said, in a number of organizations we have a number of discussions within our group about best practices. We have informal workshops and James' organization, Go Daddy, does an informal workshop every year that brings together certain registries and registrars to talk about best practices outside of the ICANN environment. You know, there's organizations that James had talked about.

So the principles I have is it's critical and I think registrars might agree with this too, it's critical that registries do not feel like they have a gun pointed to their heads to develop best practices.

If registries believe that others are going to try to force the adoption of best practices through a contract in which severe or strict penalties if they don't, you're going to - the registries are going to avoid participating in that. Most of them will. Nobody wants a gun to their head. It feels more like regulation than, you know, industry best practices.

We also need to understand we need to allow for multiple practices without pre-judging necessarily which one is best. And on that note, we need to be flexible in the mechanisms that we have to allow for innovation and market the differentiators where appropriate.

You know, it may be that certain registries want to develop these enhanced best practices whether it's things like voluntarily adopting the high security zone - TLD zone requirements because they want to differentiate themselves in the marketplace as being more secure than any other registry out there. You know, come to us because we do these things.

We shouldn't automatically assume that because there are some registries that go about and beyond that we need to take every other registry and make them all go above and beyond. It's not the right way to necessarily look at that.

You know, we need to also stick to the what and not the how. Meaning what is the behavior that we're trying to prevent or what is the behavior that we're trying to address. That is what we should be looking at. Not necessarily the mechanism of exactly how to do that.

Again, it provides a flexibility. We're not saying that this is the only one way that you have to do this. You know, and I think, you know, APWG has some good examples that I know (Rod) will talk about where they do focus on the what as opposed to the how although in some of their documents they do focus on the how and I think that's where they got a little bit of pushback in I think it was 2008. I think, you know, (Rod) will talk about that.

We also need to allow in this process for baby steps. We can't force the complete addressing of an issue immediately. We need to be happy with the baby steps. We need to be happy that steps are actually being taken. And sometimes in this ICANN environment we want the whole enchilada.

We want everything prevented and we get a little bit intolerant of proposals that in their mind don't address the whole thing. An example is domain tasting. Right.

We had - Neustar had adopted something that eventually became a consensus policy, which was allowing, you know, up to 10% of the deletes of registrars to get a refund on that and anything above that would - they would have to pay for the registrations.

There were a number of members in the community that immediately attacked us and said, “No wait a minute that’s not going to solve the whole problem, you know, you need to allow 0% we need to get rid of the whole redemption grace period to allow registrars to restore their names.”

And in the end it turned out we were right, you know, the registries and registrars were right if you adopted that policy in a baby-step that actually eliminated the whole practice.

We need to understand our practices are always evolving so whatever best practice we have we need to understand that that best practice today may not be the best practice tomorrow. It actually may hinder. So to the extent that people are thinking these need to go into contracts; that's actually a bad thing. If we don't have the flexibility and we have to keep going through the contract process to amend it.

I'll give you an example with the Conficker Working Group, when we all decided that the best way to address that was to actually pre-register the names, you know, our contract had required us to pay ICANN for every registration.

And so we went to ICANN and at first it was a lot of reluctance because when we said we're going to register these names and we don't want to pay the fee because we're not really using them, we're just keeping it out of the registration pool so the bad guys to register. And Greg may remember this as well, ICANN's first reaction was well you still have to pay us for those names.

And it took an education process to actually get that out of the way. So to the extent - and I think - and I do want to give some kudos to ICANN, we actually did develop an emergency process to deal with that in the future so we actually have addressed that but at the time we didn't.

And then again as far as what ICANN should be the role, ICANN should be a facilitator not a regulator. It's okay to engage in education, it's okay to bring the parties together, but as soon as it gets into the attitude of we need to regulate, we need to put these into contract, and we need to step in and have compliance all over them, I think that may be going too far in a number of circumstances.

And then, you know, I agree with the notion of whatever process we develop we need to allow for the confidential exchange of information.

There's a number of these practices that actually get at the heart of our information and our systems and to the extent we can facilitate that with things like non-disclosure agreements or, you know, things where we can do this outside of the public realm I think that's a really good thing.

I think with that I'll let you turn it over.

Marika Konings: Thanks very much, before going to Martin just, you know, to give both you and Jeff maybe some food for thought for the discussion afterwards because I heard James talking about, you know, the economic model being upside down and not much incentives to being the good guy. You know, Jeff's talking about the Best Practices developed through competition.

Well where does that leave those that are at the bottom, because I think all our time to, you know, gather this (unintelligible) now one's that are on the table here are doing many good things, they're often not the problem but how do you raise the standards still allowing for competition to do even more than that and making sure that there is indeed an incentive to, you know, do the good things.

So but, you can think about that maybe we can come back to that at the discussion. So with that, I'll hand it over to Martin.

Martin Sutton: Thanks Marika. My name's Martin Sutton from HSBC. I'm also a member of the BC but today I'm just going to try and give you a perspective from Financial Services Industry and try and see where some areas of possible learning points to come and add to this discussion.

I mean, you're probably very aware that the Financial Services Industry's probably one of the most heavily regulated industries, so we're used to having to work very much around a highly regulated environment which does in itself add column and cost to your business.

So the preference wherever we can is to look at self-regulation which includes identifying problems, issues proactively, and addressing those issues within that industry by adoptions of minimum standards and Best Practices.

One of the key aspects there is that it is sharing a lot of information selectively amongst groups of banks. Probably one issue here is that it's more localized, I mean, I do appreciate that ICANN is a global many-stakeholder group and trying to coordinate these aspects coming to the core. But that would be something that would need to be worked on.

There's a couple of remarks earlier one by Jeff in terms of competition and allowing some of these things to work themselves through competition. I wouldn't like to think that fraud and abuse was a competitive area, you don't really want to compete on fraud and abuse. So I do believe that those areas that are noncompetitive that do allow parts of the community to come together and work through these issues and establish Best Practices.

In the Financial Service Industry we regard this as ideal to allow us to protect our industry and our industry's reputation and I think that is valuable take away in terms of trying to pursue the Best Practice Initiative.

The other aspect is in terms of data sharing you've already touched upon it with Jeff and James, but it is important to understand what the issues actually are before you try and work out what you want to apply to address the issues.

That does require a lot of data sharing and in the Financial Services Industry we work very well together to get the facts into one place so that we can actually issue information collectively through an association that works on our behalf again on a localized fashion. But does put facts out and therefore that does allow you to prioritize some of the issues and concentrate your efforts in particular areas that demand adoption of better practices or new practices.

So rather than based on the hypothetical issues actually find out what the core issues are what are the actors that are involved in that? Because it may not just be something that you can overcome by a single entity, single stakeholder group, it does often require a lot of work with external parties. So again with the banks we often work with law enforcement, registries, registrars, ISPs to actually understand what the issues are and who plays what part in the process.

Because it's not always easily obvious to some individual entities -- hey and that could include one bank -- as to what the scope - what the scale of the problem is. You actually have to put the pieces together before you can actually start to work out what may be the better solutions to mitigate that thread.

I think just going on to one other point that James mentioned in terms of what ICANN's role in this is and that it should just be limited to a facilitator. I would like to open the question up then in terms of the affirmation of commitments there's references to working in the public interest and so I think that this is certainly an area that does bode well in terms of ICANN's role with that regard. And I think that that could well be a topic for discussion and taking further.

And in enforcement - that was it - the issue about adoption. I understand concerns as to how that could be enforced in contraction what with the issues that may create. But in other ways if you have Best Practices that can be adopted and not adopted by some players when something goes wrong that is tied to that Best Practice, I do believe, and that could be a role that ICANN plays in enforcing the adoption of that Best Practice.

So it's on an exception base rather than an up-front base, and that's an alternative about approaching adoption.

In terms of adoption, I also think it's important to bear in mind that we may be looking at a list of items on display earlier of Best Practice (unintelligible) sort of an issue from SSAC maybe WG (unintelligible) other sources.

The one issue there I would have is to make sure that it is easy to find, it is in relevant languages, to be able to be picked up and this is so important with the new detailees coming up to be able to give new registries and any new registrars that emerge a pack that will help them create their policies and procedures up front. Rather than to learn the hard way when things go wrong give them the information and tools to enable them beyond just the policies that they've got to work with.

And that's it for me.

Marika Konings: Thank you very much Martin. So we go next to Wendy.

Wendy Seltzer: Thanks Wendy Seltzer here from the Noncommercial Users Constituency and here to talk from the perspective of the interest of noncommercial registrants and users of the domain name system. And I wanted - first picking up on James' point about the title of the session. I think it's critical to distinguish between the content layer and the addressing layer.

Abusive use of domain names is something that happens at the content layer. It's often the content of Web sites or other resources, the use, traffic bent through the net, which is outside of what ICANN controls or has jurisdiction over. And ICANN's remit is the unique identifier the addressing system.

And we get into problems when we try to address content problems at the addressing layer because we tend toward solutions that are too broad, too blunt, and that sweep in legitimate users and uses along with the illegitimate and the abusive. So I think as we look for and support those who adopt carefully targeted solutions to addressing abuse, we should not reach too far and use systems like the DNS to address content problem.

And I (unintelligible) because the users and registrants have an interest in the security, stability, and consistency of domain name resolution. We want to know that when we register a domain name, so long as we continue to engage in legitimate activity that that domain name will resolve. That we will be able to communicate through it and be found. That when we go looking for resources we will continue to be able to find them at the same place the registrant put them and overbroad responses, the take down of thousands of domains because of a complaint of activity at one of them, threatens that stability and consistency.

Nonetheless ICANN has taken on this issue at many, many ICANN meetings and panels on DNS abuse and in the Registration Abuse Policy Working Group we recommended that ICANN look at Best Practices. Perhaps provide a forum for the discussion of Best Practices and do the things that ICANN does best.

Operate as convener, facilitate information sharing, promotes transparency around the process, and the communication to users of the system about what is permissible to users about the parameters of permissible use and to the users about what has happened and what to do in the event of concern or mistake.

And the Best Practices that might develop in such a system would include due process. Before taking down a domain name give the registrant an opportunity to know the complaint against him and opportunity to be heard.

Or if it’s a situation that requires immediate action if there’s, you know, criminal activity taking place that appears obvious and to pose an imminent threat we wouldn’t recommend, you know, leave the name up until a full court trial can be heard. But well documented response so that mistakes can be challenged afterwards.

Transparency not of the details of the process to allow the would-be abusers to find the loopholes in the system but transparency of the framework. What should the registrant know in order to stay on the right side of - not to engage in abuse? And how to challenge the process if accused of abuse while engaged in what the registrant believes to be legitimate activity.

Transparency to the public of what has been taken down and why so the public members - members of the public going to look for a site can learn why it’s not there when they encounter that. Help them learn, you know, how to challenge if they believe that there’s a problem.

And transparency of standards many of the attempts to regulate abuse operate by black-list. User attempts to visit a resource and gets redirected with no opportunity to learn why. There should be no blacked-out black-lists. We should at least be able to discuss the causes of take down and to discuss the general problem, if not to reproduce the content itself.

And so in general we think the registrants and the user community should be a part of these discussions and can help to define good conduct and its limits because we too are part of the consensus that helps to shape the Internet and it’s productive uses. And in all of this we should leave room for generative and creative new uses of the net while helping to press back against abuses.

Marika Konings: Thank you Wendy. Now we are moving on to to hear a bit about those that have been involved in the development of Best Practices and other environments although just as well as Greg Aaron I think is part of the registry perspective as well in his turn but we'll go first to (Rod).

(Rod): Thanks Marika and Chad I have many points of agreement with my esteemed colleagues on the panel here. On a few things we probably have some differences over but I wanted to talk a few generalities, and then a few specifics from the Anti-Phishing Working Groups perspective. Well in my own background as a security professional.

So I wanted to just kind of take one step back and talk a little bit about why we're here in the first place. The RAP Working Group had a very involved process; we went through many different types of abuse out there. And we weren't quite unanimous on everything in fact right to the definition we were talking about the title of this session. And you know the use versus registration versus these sorts of issues.

And so one of the things we came out of things that were not necessarily going to the PDP or were contract process et cetera. Was taking a look at how can we codify a lot of these good ideas that we come up with and do it in a way that would not be contractually binding but would help advance the cause of making domain registration and the environment a better place, right?

So and one of the reasons we're doing this is we're in a evolving landscape. Threats are becoming much more complex. Dealing with fast-flux phishing is really easy in comparison, you know, we've had major arguments in this forum around that but it's really easy in comparison to the things that are coming out now.

I mean we've got lots of different ways that criminals are abusing domain names in particular in conjunction with malware and injections in the Web site and doing all kinds of fancy stuff with it. But it's really hard to get your arms around, describe, and put into a scalable fashion the ability to respond to it.

So we've got even bigger problems coming down the line. And so these are things where you have an evolving set of practices around it and, you know, that gets to be the whole idea of Best Practices. What are they and what are their purpose?

You know, what you typically have is you have some sort of situation or issue, may be a threat, might be just dealing with a process or what-have-you where it's an emerging thing and so different people are trying different ways of doing it; different practices.

Over time consensuses build around well this is what seems to work best or better and you evolve into Best Practices that may very well be adopted by an industry even more formally that help govern where people known as their government help them - help guide them in their daily processes and work.

Some of those end up actually if they're something that makes sense, they get codified under regulation or law or what-have-you depending on the environment. Others over time just remain as practices; other may just disappear because whatever the issue was at the time is no longer relevant. That happens in all walks of life.

I think there are some good worldwide examples that we can take a look at especially in the health care profession there's lots of worldwide policy. Best Practices are just zipping around the world and research. There's issues where people come to consensus on Best Practices and adopt them around the world, so and that question was raised I think, Martin, you brought that up about local versus international so there's some good models out there.

So the idea here, I think, was not necessarily really a contractual issue at all, some things may end up being developed in the PDP eventually what-have-you. We've seen that over time. But they usually start as a practice and then a Best Practice.

I think that one of the things that we've seen in the abuse community is that the folks that show up at these meetings typically are using Best Practices for the most part. And there's some actors out there that aren't. And they can often, you know, either through ignorance or intent are part of the problem instead of part of the solution.

And so having a central resources referenceable is very helpful. I can't tell you the number of times that one of our team has called a registrar or a hosing provider somewhere around the world that is dealing with a domain name is clearly registered by a criminal and I said well, ICANN doesn't say we have to do that so we're not going to do that.

And you're right, ICANN didn't say that you didn't have to do that, but if you have a centralized resource that says here's what the industry thinks are good things to be doing as far as part of your practices go, it's very helpful to have that as a referenceable document from a trusted source.

So I think that’s one of the reasons we’re looking at ICANN for one of those, for assistance on that. And again, it’s more of a repository role and a developer and facilitator rather than a dictator of those practices. The industry needs to develop the practices not be handed it from the top-down. It’s a bottom-up process really on those kinds of things.

So I just wanted, more specifically I wanted to take a look at the APWG's recommendations from three years ago that we developed in conjunction with our members including input from the registries and registrars.

And the top five I was going to run through real quickly and give just a little bit of a comment on where we are. And sorry I don’t have it on a slide so you’re going to have to memorize exactly what I say here.

The preferred number 1 was time and response of domain takedown requests by shut down authorities and law enforcement. You know, duh is all I can say. You know, quick response that involves lots of things, having a team, a lot of the things that James and Jeff both were alluding to and do.

And we’ve seen a tremendous improvement I would say in general in the industry in that time frame the last three years about responding to abuse issues very quickly.

As you may have seen some of the reports that are given out what will happen is that bad guys will find some other - somebody else to pick on some other resource to abuse and they’ll move on there and you have an education process to go through with that registrar or registry or what-have-you to get them kind of up to speed with what everybody else is doing. So it would be nice to have, again, a central, kind of, area that people could refer to especially as they become a registrar or in the case of a new detailee is we may have, you know, hundreds of new registries out there. It'd be really nice for them to have a reference to be able to pick up from day zero or day one what are the things they need to be worried about and implementing to avoid becoming the next victim of criminals moving along.

The second one was proactively use available data to identify and shut down malicious domains. That would include sources of, you know, sources like APWG and Cerbal and a whole bunch of other places that commonly list things that are being abusive.

I would say we've seen some take up in that by some of the more involved players in the industry and that's certainly almost a competitive advantage in that they're very responsive and very quickly seeing that particular resources are being, you know, run by criminals or likely to be their bad self so they scrutinize those transactions a lot more and will often find credit card fraud and things like that involved with it and be able to avoid losses themselves.

That is not universal however, that is typically some of the more involved larger registrars.

The number 3 was share frauds in the domain registration information with law enforcement. I know this goes on behind the scenes a fair amount with some registrars and registrees in particular. But that is actually kind of hard to do in that there's not a very good centralized resource for that.

There are a couple, if you know who to work with but that's hard to as it's kind of hard to say that that's something that's been easy to adopt.

Protect your customers from being phished. One of the big concerns we have is takeovers, hijackings of the domain names and DNS resources. I'd say the record there is fairly mixed we have had a few things an innovation like the registry lock function.

But it's been fairly slow, we've not seen a lot of multifactor authentication techniques or other things in that front that we, you know, would be helpful for protecting registrars, but there has been some progress there I would say.

And then prohibit or minimize the use of fast-flux domains was the number 5 recommendation from that. And, you know, Jeff mentioned the Neustar policy we've seen that put into policy in various forms or by various players in the industry so we have seen some of that.

The use of fast-flux domains in phishing has virtually disappeared. It is still being used in other forms of abuse. And but it's certainly in phishing it's gone away but that's because I think that one of the things about it that we found is that it is so easy to detect these things.

Once people had systems up and running to do it and then people were automating their own systems on the back end to (unintelligible) and suspend them that this became a non-issue for a lot of the players out there.

The, so I think that there's been a lot of progress on that probably for multiple reasons. So those were the top five.

That last point brings up something else interesting, that's one thing I think that we'll want to as a community and other communities will want to address is other forms of abuse. Because I was talking marginally about phishing here, Anti-Phishing Working Group perspective.

The Anti-Phishing Working Group is actually, we've considered a name change but we're continuing with the current name but it's really we're anti-ecrime, right. So but we have an issue when especially with dealing with people in various communities whether it's a registrar, registry, hosting provider, ISP what-have-you, what is abuse? How do you define it? What's the taxonomy of it?

And there's actually a discussion that just started up a day ago on APW2 list about that very thing. We have challenges there because there are things that are going on that are not well understood in the industry. Not every kind of scam you can call a phishing scam.

There's lots of different kinds of abuse going on out there, so I think, you know, it's a little tangential the Best Practices was hard to define Best Practices if you don't - aren't speaking a common language about what your trying to curtail or effect.

So we do need to - and careful definition and go to I think, Wendy's point there is very germane in that you have to know what you're talking about you have to be very precise in what you're doing to not cause collateral damage.

So I think taxonomy and process is very important, and that's where Best Practices are really helpful because they help you to prevent you from making mistakes.

We've seen some rather large mistakes done by law enforcement in the last couple of months. Where people's domains and hosting facilities were adversely affected by court-ordered actions. And that's a problem. And we as an industry need to do a better job of making sure that it doesn't get to that level where somebody who may not know the best way of doing things comes in with a court order and causes a lot of collateral damage.

So that's one of the reasons that I think the self-regulatory scheme is very helpful in getting that and putting together these kinds of practices can really help avoid those kinds of problems in the future. That's what I have.

Greg Aaron: Hello my name is Greg Aaron and I'm going to be speaking as a security professional. I'm on the security commission of the Anti-Phishing Working Group. And my work is also as a registry operator creating anti-abuse policies and then carrying out operations.

I do that in Dot-Info and also provide some advice and operations for some other TLDs, gTLDs, and ccTLDs in this area. So I'm someone who's doing policy but I'm also on the front lines day to day seeing what bad things are happening. So I think as this paper comes together one of the first things that should be in the paper is to summarize that issue of registration issues versus use issues and the

Registration Abuse Policy Working Group which I chaired did a good job of delineating those issues.

We’re talking about as far as malicious use is another way to put it perhaps is criminal activity; dealing with distribution of malware, phishing, the creating and direction of botnets.

Well criminal activity is defined differently of course, in various jurisdictions, in general the goal of these activities is to create damage, steal money, and those kinds of things which I think all reasonable people can agree are problems for users and make the Internet less safe.

Now for me one of the main features of Best Practice is flexibility and the organizations that do Best Practices including the IETF and many others do focus on flexibility.

Security and ecrime are very dynamic areas. The bad guys are always figuring out new things to do and new ways to do it. And that means that the good guys have to figure out countermeasures to deal with those problems. We must constantly evolve.

And so a mandated set of specific practices is very difficult to maintain by the time you figure out what those are the bad guys have moved beyond them. One of the issues in flexibility is that, you know, every registrar and registree does have a different goal in its business. It has a different business setup. The issues that a registrar faces can be very different from its fellows.

You know, a registrar that has a reseller program, for example, has a very different set of issues to deal with than a registrar who does now. Registries are sometimes differentiated by price. Sometimes they have a specific audience, and so they have registration requirements and so on.

And those all contribute to the levels and the kinds of abuse that happen in those TLDs. So in one sense, all of these registrars and registries do need to understand their businesses, and they do need to understand what problems they may face. And then ultimately, they're going to have to decide how to deal with them.

Now one of the issues is that this does occasionally lead to some non-uniformity. In my work, when I discover a problem, one of my first steps is to document it, then I bring that documentation to the registrar and I say, "We seem to have a problem here. Here's what it is and here's some proof of that."

Because I want the registrar to understand what's happening, it needs to know what its customer might be doing, and I want the registrar to also, you know, take it seriously and perhaps make a decision about whether that domain name should be suspended or not. Now, some registrars respond very well. They're professional, they have a staff that can understand these kinds of things, they deal with the problem.

Some registrars are completely unresponsive. And after five years of doing this, that can be frustrating sometimes. But on the other hand, I've come to a certain peace about it.

Because, you know, systemically, we are not going to get everyone in the world to act quickly enough or in the same manner. That's just the way the world works. This is not unique to the domain name industry.

You know, if you call up ISPs, they all have varying policies, they respond differently. And we see that in a lot of other industries as well. It is what it is.

Now I don't want that to mean, though, that we should give up, because I can also attest that education and sharing are absolutely effective. I mean, five years ago, my company didn't know anything about this arena and started seeing a lot of problems in its TLD. But one of the places I've learned about the issues and how to deal with them is here at ICANN.

I met people like (Rod), ecommerce providers who come here, and so forth, and now I know a great deal about it. And this is a place where people should come together and share that information. We will not always have a perfect environment, and indeed, e-crime is something we cannot solve but we can make a much better situation for ourselves and Internet users.

I think in this process, we're not starting from zero so if we do have a working group, we're not creating something from whole cloth, there are a lot of things out there that can be brought in quickly. Also, we're not going to be talking about binding practices. You know, when we have working groups here and we're talking about putting something into a contract or having a consensus policy, you know, that requires very close examination and some parties have their interests.

Here, we're not talking about quite the same thing. I'm hoping it's a little less contentious. As Martin says, security and dealing with these issues should not be, hopefully, a contentious process, it should be something where people can collaborate and come together.

So I'm hopeful that if we do have this kind of an effort, it wouldn't take a lot of time, not the two years sometimes we see with our working groups. I do like the idea of ICANN as a facilitator for this kind of thing. We haven't done it a lot in the past, but I do think it's a place where the players naturally come together and we can share ideas.

And I do think the world is looking at the domain name community to do this kind of thing. Our governments are very interested, our law enforcement people are very interested, and Internet users in general are interested in everybody doing their part. And this is one way we can do our part.

So this is also something I think that it's the right time to do. We will have our registry operators applying for new TLDs starting in January, and then they'll come online at a certain point after that. Some of them are going to want to get out there as soon as they can.

So I think working on this effort now, it's the right time. If you're a registry operator in the future, you need to know what you're going to face before it happens to you. When it happens to you, it's already too late.

So I think we have to get those new operators thinking about these kinds of issues now. I mean, it is gratifying that, you know, four years ago, ICANN - we didn't have meetings about security in these issues.

Now we have them all the time because awareness has been raised and people are taking it seriously. So those are my thoughts, and thank you.

Marika Konings: Thank you very much, and thank you to everyone on the panel. I think I'll now it open it up to the panel for further comments or questions or discussions between each other but also for the audience. If people want to contribute to this discussion, they have a microphone here, so I mean - if you can just introduce yourself and - thank you.

(Rod Turner): Hi, I’m (Rod Turner) from Trusteer. A comment actually from Jeff's points on the difficulties of having ICANN take on a regulatory function - it might be feasible, and this is - I don't know if everybody's able to comment or not but - if candidates of best practices are offered, whichever the characteristic that they are painful for any individual participant to implement, but are beneficial for the entire group, these are never, ever going to be adopted by an individual organization's pursuing their own interests.

But the obvious example is the WHOIS rules, which are routinely (unintelligible). It's against the interest of some registrars and many registrants to provide accurate and current WHOIS information and yet there's a clear abuse prevention interested in doing so. So what I'd suggest that in the context of this effort, is to establish two separate regimes, if you like, for best practices.

Those that are fairly widely believed to be in the interest of those organizations who adopt them, in which case ICANN's function is clearinghouse and promulgator of voluntary best practice, versus those where one or two bad actors are damaging the environment for everyone and prompting, for example, code enforced action against a large (unintelligible) and doing damage. I can't think of any examples and it's more something to keep an eye on, but rather than ruling out completely the possibility of these kinds of things that ICANN might get involved in, pursuing if not enforcing participants to comply, to separate out this class of potential best practices that would be - that was willing to push people to use, rather than not.

The barriers are set pretty high, right? There's got to be a very clear damage being done by having a small number of bad actors continue to act. But the way it should be treated is a completely different animal to the best practices that are being promulgated as being that self-interested participants who are looking for guidance would seek.

Marika Konings: Do - anyone respond - well...

Man: I think that's a good point. I think it was Martin that raised, when I was talking about how the market can work out certain best practices, I didn't mean to imply that the market can work them all out. And I do agree with you that there are certain best practices that it's in an individual entity's best interest to put into effect. And I agree that in certain circumstances, I think it's fairly limited.

There may be certain incentives to not engage in those practices because it's more in your financial interest to do so. There aren't too many examples of that, although I do hear members of the community claim that that exists a lot more than I think it actually does. But I take your comment, I think that's right.

I think there are certain examples where the only way to step in is to "regulate" but that is done in a mechanism maybe through the consensus policy process, as opposed to ICANN staff dictating so this should happen.

Marika Konings: James wanted to respond, then we have Dave in the queue and (Margie Iles) has a remote question, so James?

James Bladel: Okay, so I'll be brief. Two points - first, I wanted to challenge your initial premise that organizations will not necessarily adopt best practices if it's counter to their own interests. You know, we - just an example of our organization - we spend considerable amounts of money and large resources and individuals to things that, you know, just looking at a black and white dollars and cents equation, do not pay off for us, okay?

This is part of our contribution to what we believe is an important, you know, the viability - the long-term viability of this industry and this community. And that includes sponsoring some of the events like Jeff alluded to in his presentation, where we bring people in from all over the world to discuss best practices. I saw where we held this event, it wasn't cheap.

So - and when registrars are operating on very razor-thin margins, so this is important. The second thing, and I want to just point this out relative to best practices versus regulation or contractual obligations - something to think of very carefully is the - and I think we see it all too often in the ICANN circles - is the law of unintended consequences. So be careful when we do something, the backlash is sometimes worse than the problem we set out to solve in the first place.

A classic example in this regard would be a race to the bottom. As opposed to what Marika said is lifting the standard for all of the folks, if we start to put something into contract that says here is the level of, you must do X, okay, then that poses an interesting economic question to registrars like my own company who are exceeding X. Do we continue to and make the investment to go above and beyond what is in a contract when our competitors are not?

And do we then lower our existing efforts to the bare minimum of what it is that we're contractually obligated to do, as opposed to setting the standard and continuing to, you know, raise the bar for these issues? And so I think that when those things start to go into contract is when registrars start to ask themselves those types of questions. Thanks.

Marika Konings: Could you be brief in your response?

(Rod Turner): I'll be very brief, actually. There's a big theme at the race to the bottom which is interesting, but I won't touch on. Just what my premise was - my premise was not that no registrar will act in ways that are broader than their own accompanying interests. It's that some registrars or some participants, registrars or otherwise, will not.

And it's the existence of typically a small number of bad actors who are acting in their interests against everybody else's interests who are the problem. And generally those are not the people in this room. Those are the only people - the only situations where anything that looks like regulation or coercion is appropriate, and they are a very difficult and contentious issue.

So my point is just to separate that class and say bad actors do exist and the ways of dealing with them need to be dealt quite separately from (unintelligible).

Marika Konings: Dave?

Dave Piscitello: Dave Piscitello, from ICANN. Martin brought up, I think, a really important point here about ICANN's role in serving the public interest. And one of the things that I tend to hear when I'm at ICANN is a very, very emphasized concern about the registrant.

And the registrant is part, you know, part of the public, but it's not the entirety of the public. In fact, the user is the broader, you know, broader community of the public that we ought to serve if we're all collectively administering a resource that is consumed globally and is vital to the operation of the Internet. So when James gave an example of one in 1000 domains that are handed off by a security or an intervener or a responder, and that one in a 1000 is actually not identified as part of a botnet but it represents a legitimate site, and there is a false positive, yes if you do not act, you actually preserve that one registrant's Web site or Internet presence.

On the other hand, those other 999 that you are either taking no action on or waiting for a court order, now continue to, you know, assist or abet in a malicious activity. And that malicious activity could range from anything from child pornography or human trafficking or illegal pharmaceuticals, not just spam and phishing. One of the things I really worry about is that we are all so inundated with, you know, concerns about phishing and anti-piracy and spam, is that we're becoming desensitized to them.

The numbers of them are so large and we see them. You know, we have to remember that acting, even when there is there is a chance of false positive, in some cases may be extremely valuable and extremely preventative.

Marika Konings: Thanks, Dave. And we had a remote question. If you could just ask your question and then we'll go to the panel on response, okay? We can maybe take it together.

(Margie Iles): Oh, this question's from Danny Younger. His question is, "While I understand that nonbinding best practice recommendations can serve as a catalyst for change, I'm not aware of any study on the degree to which recommended best practices are actually adopted within the ICANN community. Are there any such metrics available?"

Marika Konings: Wendy, you wanted to respond to Dave?

Wendy Seltzer: Thanks, I wanted to respond to Dave on a couple of points, because I think the interest in the community is broader than you described. Certainly the community has an interest that there not be abuse. The community of users also has an interest that legitimate sites stay available at the domain where they have legitimately been made available.

And so trying to figure out the ratios and precisely how much collateral damage is permissible in the fight against abuse is a challenge, perhaps. But I also wanted to take issue specifically with your statement registrars who - or registries permitting abuse of domains are aiding or assisting or abetting in the abuse themselves.

Dave Piscitello: That's not what I said. No actually, I said that we have to be careful that we don't end up, you know, indirectly aiding and abetting. So it's not - you know, I'm not an attorney, and using that term in front of five attorneys is probably a good way to end up with scorched fingers, but if you take no action and the site remains, then the criminal activity persists. Agreed?

Yes, that's the point I was trying to make. But you actually brought up something that I wanted to make - wanted to add and I forgot. And part of the remedy here, and maybe something that we ought to consider, is the notion of a safe harbor. There ought to be a way for a registrar in a situation like this, where the registrar honestly believes that the compelling information is such that taking action is the right thing, and so doing the right thing and not being penalized for doing the right thing is okay.

Marika Konings: So your raising safe harbors is an area that I've spent a lot of time studying in the context of copyright takedowns, and safe harbors themselves set up interesting incentives. They set up an incentive not to investigate and not to take precautions to protect legitimate activity, because the safe harbor protects any action taken. And so in the context of copyright takedowns, we see plenty of political speech and parody and fair use quotation of copyrighted material taken down under the Digital Millennium Copyright Act because the ISP or hosting or search provider who received the complaint knows that the safe course is to take down.

And so I would not - or just to cause that kind of insecurity for domain name registration. I'm really sorry, but we're really running out of time.

So I still have a few people in the queue, I have (Carlos), (Tim) and Martin and then we still have as well the question of Danny Younger, if anyone on the panel has a response to that. But if we could just ask maybe all of you to keep it as brief as possible as we need to wrap up shortly? Thank you.

(Carlos Alvarez): Sure, Marika. (Carlos Alvarez) from ICANN. First a question to James and then a comment to all the panelists. James, I didn't quite understand what you meant when you said that registrars have certain laxity with regards to the content that should be included in their registration agreement.

And I said that I didn't quite understand that in light of the provision in the 2009 RAA that determines the minimum content that should be in the registration agreement. That's the first question. If you will allow me before...

James Bladel: Yes. The registration agreement between the registrars...

(Carlos Alvarez): Between the registrars and the registrant.

James Bladel: Yes.

(Carlos Alvarez): Did you understand my question?

James Bladel: No I did not.

(Carlos Alvarez): I understood that you said that registrars have laxity with regards to defining the content of the registration agreement that they enter into with the registrants.

James Bladel: They do.

(Carlos Alvarez): Yes, but there is a provision within the RAA that obligates the registrars to include a minimum content, that's 3.7.7, so I didn't understand your question...

James Bladel: I think the only - there's a few aspects that are required to be in there with the (QDRP) and by consensus policies, and there's something - in 3.7 it talks about business dealings. But no, I mean, we can add a provision, for example, that addresses abuse specifically that's not required by ICANN, and that's what I was driving at. Thank you.

(Carlos Alvarez): My only comment, and I'll be very short, is that it seems to me like the proposal of the best practices that may not take into account cultural differences and - with regard specifically to registrars from China or Russia who might not see their business as an American, big, well-established company might see it, or a British company or a French company. I believe that a Chinese registrar or any other nation or Russian registrar would not be so willing to implement best practices and in many cases, malicious conduct comes from those countries. So if you could take that into account it would be great I think.

Marika Konings: Tim was next in the queue, he's in the back.

Tim Ruiz: Tim Ruiz with Go Daddy. I guess I'm just a little concerned about the discussion about collateral damage. And while I think, you know, there might be some valid need for a discussion of that nature, just to caution - to have some caution in that area, because I don't think anybody here or any of our customers consider themselves just a statistic or collateral damage.

And some small businesses, even just a short takedown of just a few days could devastate them financially or ruin them financially. So I don't think it's an easy thing to solve. I don't want to be too callous about just considering it statistics or collateral damage. Thanks.

Marika Konings: Martin? There's only you in the queue.

Martin Sutton: Just a comment, really. Just a slight twist on the issue of, you know, one in 1000 events, turning it the other way, we know and have heard that there are lots of activities that were undertaken day in and day out within the registries, within the registrars. What we don't know collectively is how much is being done, like getting those metrics together to understand some of these issues.

It also provides you with some information about the scale of activities that are undertaken already within the industry. And that is a positive spin that can be applied, but it also reveals the gaps that need to still be addressed.

Marika Konings: Yep, quick.

Man: Actually Martin, I think that's a very interesting idea. If as one possible best practice, not a requirement, but best practice for the larger industry players, not just in ICANN but, you know, out there in the industry too, to maybe start reporting some of the frequencies and statistics.

You know, as businesses, we tend to keep these things pretty close to the vest, you know, because it is likely that some of these things could be mined for vulnerabilities. But if we could sanitize those and get some use but retain the useful information, I think that's a great idea.

Marika Konings: Any other last remarks any of the panelists want to make before we have to - (Rod), go ahead.

(Rod): Yeah, I just wanted to emphasize that we heard a lot of - in the discussion we heard a lot of concerns and issues raised are very legitimate and that's I think why we're talking about best practices. That's the goal here, is to be - instead of forcing people to do things is actually work together to figure out what best approaches work so we don't have collateral damage, or whatever you want to define it as, that we respect people's rights, that things get done in a positive manner. But do it in a flexible way so that we can evolve as the threats are evolving.

Marika Konings: Well, on that note, I would just like to thank the panelists for their contributions, the audience for listening in, and if you have any further comments, you know, let me know and then we'll take everything back and try to come up with a good discussion paper that would lead to further discussion. So on that note, thank you very much.

END