Registration Abuse Policies Working Group
TRANSCRIPTION
Monday 14 December at 15:00 UTC

Note: The following is the output of transcribing from an audio recording of the Registration Abuse Policies Working Group meeting on Monday 14 December 2009, at 15:00 UTC. 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. The audio is also available at:**
http://audio.icann.org/gnso/gnso-rap-20091214.mp3
On page:
http://gnso.icann.org/calendar/index.html#dec

All recordings and transcriptions are posted on the GNSO calendar page:
http://gnso.icann.org/calendar/index.html#dec

Present for the teleconference:
Greg Aaron - Registry stakeholder group - Working Group Chair
James Bladel - Godaddy Registrar stakeholder group
Berry Cobb – CBUC
Mike O'Connor – CBUC
Rod Rasmussen – individual
Faisal Shah – IPC
Robert Hutchinson – CBUC
Martin Sutton – CBUC
Caleb Queern - Registrar stakeholder group
Philip Corwin – CBUC

ICANN Staff
Margie Milam
Marika Konings
William McKelligott (guest)
Gisella Gruber-White

Apologies:
none

Greg Aaron: And why don't we begin with our roll call please.

Gisella Gruber-White: Absolutely. Good morning, good afternoon, good evening, to everyone on today's IP call Monday the 14th of December.

We have Greg Aaron, Caleb Queern, Robert Hutchinson, James Bladel, Berry Cobb, Martin Sutton, Mikey O'Connor, Faisal Shah.

From staff we have Margie Milam, Marika Konings, William McKelligott, and myself Gisella Gruber- White. And we do not have any apologies for today.

If I could please also just remind everyone to state your names when speaking. Thank you. Over to you Greg.

Greg Aaron: Thank you Gisella. I think everyone is on Adobe except perhaps Robert at this time. If you can, log into both the phone line and Adobe Connect. Thank you.

Gisella Gruber-White: And Rod Rasmussen has just joined the call. Apologies, sorry.

Greg Aaron: Okay, thank you. Hi Rod.

Rod Rasmussen: Good morning.

Greg Aaron: Okay. Over the weekend we had a flurry of material come in which is great. So we'll talk about much of that today.

We also received some - some material in from the ICANN compliance staff. William McKelligott is on the line with us today. William is a compliance staff person. He works out of ICANN's DC office.

And the staff has been able to answer three of the five questions that were posed to it. And they're working on the other two questions.

What we thought we'd do is maybe go over those briefly today. You probably haven't had a chance to read them yet. And since William's on the call he, can answer any questions we may have.

I want to do this just briefly if there are no objections. The first question was we wanted to make sure we had collected all of the reports that ICANN has done over the last couple of years about the availability of WHOIS. And we have Phil Corwin joining.

And staff says yes, these are the relevant support. And an additional report will be coming out at the end of the year.

The second question was about a question about how does ICANN look at availability of WHOIS?

And answer is that the ICANN staff has built a tool that goes out and queries registrar Port 43 services to see if they are responding. The staff has lists of four names for each registrar. They go and check those on occasion.

Occasionally staff finds that there are Port 43 servers that are not responding or not responding consistently. There are no SLAs as we know associated with response.

But what this seems to say to me is then ICANN then if they see a significant problem they contact the registrar. In many cases that registrar responds and fixes the problem. There are some white listing issues that maybe we can ask William about.

And then the Question Number 4 was how many registrars have gotten breaches of notice letters over the last couple of years? The answer is 11.

So why don't we go to William since he’s here with any questions. William I think and I have a question in response to Number 2.

It sounds like when you guys go to a registrar and you say you’re WHOIS isn't working, sounds like most of the time they get it working. Is that the general gist of things?

William McKelligott: That would be correct. And then the registrar that actually received the enforcement notices or breach notices are those that are either habitual, you know, habitually prevent members of the community or ICANN from accessing there WHOIS server or just fail to remedy the deficiency altogether when we're, when we approach them.

Greg Aaron: Now you say they actually prevent access. What does that mean?

William McKelligott: So we get complaints from the community, members of the community or registrars stating that they have been blocked from a registrar's WHOIS server.

And when we try to access or retrieve data on registered names from that registrar we have no problem. So it's clearly of a case of specific IP addresses being blocked or prevented from retrieving data.

And what usually happens when we reach out to these registrars, they tell us that they've actually flagged specific IP addresses for multiple queries over a short periods of time and, you know, indicating that perhaps, you know, again this is one of those a little bit of a gray area. But the registrars usually tell us that they have reasons to believe that these queries are for reasons that are beyond would be reasonable or permissible under the RAs.

So they think that they may be harvesting data from a registrar's WHOIS server so they just prevent the IP addresses from conducting any queries.

When we reach out to these registrars and we indicate, you know, that the - it's a member of the community that's just trying to retrieve data on registered names and we - there is perhaps no reason to believe that there's any malicious or any cruel intention behind these queries, then the access to specific - the access for a specific IP address is restored usually.

Greg Aaron: Okay. Okay thank you. Does anyone have any questions about that?

Caleb Queern: Hey Greg this is Caleb Queern at (Surveillance).

Greg Aaron: Go ahead.

Caleb Queern: I have a question. At the document we're looking at right now there's as you said, 11 links there. And I take it to mean that these are 11 cases where folks have not been keeping there WHOIS information available or are these 11 total notices where they've been in breach of compliance with ICANN?

William McKelligott: So these were the 11 registrars that were breached from, you know, ICANN sent them breach notices. And so these are registrars that just failed to correct the problem altogether or had a long-standing history of preventing access to data on registered names and other breaches to their RAA with ICANN.

Caleb Queern: Okay. Thank you.

Greg Aaron: Okay. Does anyone else have any questions for William?

Okay. If not, the staff is currently working on two other questions for us that they think they'll be able to get back to us no later than January 8. And at that point we can look at that material and see if we have any questions about it.

In the meantime anyone who's interested in WHOIS access background can look at the links listed in Question Number 1.

So if no more questions for William, William thanks for stopping by. We appreciate it. And we...

William McKelligott: Thank you.

Greg Aaron: ...look forward to the additional material coming in soon.

William McKelligott: Absolutely.

Greg Aaron: Okay. Thank you so much.

Okay just, this is Greg. What question Number - one of the things that Question Number 2 raises is the issue of registrars and registries blocking access which is actually - or controlling access to WHOIS in some fashion. And that’s actually a very common thing.

If you go to most registrar’s Web sites for example, and most registry WHOIS’s you'll see a capture which is an attempt to prevent people from minding that WHOIS interface.

It’s also not unusual for people to block access to Port 43 or to rate limit it in some fashion. If you get too many queries coming in it can actually - and it’s not done in a rational way or in a sensitive way, it can actually equate to a Denial of Services tag on the Port 43 server which is not a good thing.

Also one of the problems is people trying to mine the WHOIS data which that’s not supposed to be happening. So that - some parties are trying to limit access.

And what I think we heard William say was some parties will be blocking IP’s because they think the WHOIS getting mined. And in some cases that turns out to probably to be correct. And in some cases the (querier) was trying to get data for perhaps legitimate purposes. So William told us a little bit about how that’s worked out sometimes.

Okay if no questions on WHOIS let’s move on to offensive (bytes) and gripe sites.

And Faisal sent in a document. So if we can put that up on the board, thank you. And Faisal I'd like to turn the microphone over to you. Can you tell us about your document and walk through this...

Faisal Shah: Sure...

Greg Aaron: ...through it for us? Thank you.

Faisal Shah: Sure. I worked on this with Martin. And I think the first issue was trying to define what all the different abuses where.

And, you know, we had gripe - we've got gripe sites, Web sites that complain about a company's product or services and uses the company's trademark. That was one (for that) company sucks.com.

Photographic site, Web sites that contain adult or pornographic contact and then have the trademark and the domain name maybe.

(Sent those strings) and we decided that maybe what it is what we're talking about here is like registration of dirty words within a domain name or with or without a brand name. So it may not even have a brand name, may even be a standalone name, dirty word.

And then there was another one that came up in the research that has been doing and that was registration of deceptive names.

And those are like, you know, for example somebody trying to mislead somebody into going into a pornographic or offensive site or a minor into a harmful site.

So for example using, I think (Ecarini) way back when used Teletubbies to attack those Teletubbies to get them to a pornographic site.

And then on the deceptive names for example, I think the famous one with that was probably the whitehouse.com.

So we kind of threw out - and I guess we were just trying to get as much in here as possible so that we can actually talk about it. And then we can figure out, maybe we can whittle it down if that's what we want to do as a group.

So the issue then became from what I could, you know, what we discussed was whether, you know, these were all just simply a form of cyber squatting or whether or not, you know, the registration was a really separate form of registration abuse and whether, you know, some kind of policy framework has to be developed addressing this category across all the registrars and registries, ICANN accredited registrars and registries.

So...

Greg Aaron: This is Greg...

Faisal Shah: ...on the background...

Greg Aaron: This is Greg. I've raised my hand.

Faisal Shah: Oh.

Greg Aaron: So at the top you've split out gripe sites and then pornographic sites and offensive strings. In the issue summary though they're grouped altogether.

Faisal Shah: Yes I...

Greg Aaron: But you call GO.

Faisal Shah: Yes. I kind of put them altogether because I think I - it - yes I kind of added them altogether. And you'll see that when I get into the issues or any of the background I started really kind of discussing it.

We - it - I would say a number of these really fall into cyber squatting. And then maybe, I mean we could take them all. We could put them - we could actually put them there or we could actually take one of them and pull them out or maybe a couple and pull them out.

So yes, I think that’s what I did. And maybe that was taking a little bit of a liberty there. I just wasn't sure if I wanted to start separating each one of them out into the issues.

But to look at whether, you know, here we’re talking about cyber squatting or whether we’re talking about individually or as a whole registration abuse for each one of these.

Greg Aaron: Right. I guess my - as we walk through, one of the things I think is interesting is they all represent perhaps some speech issues.

Faisal Shah: Yes.

Greg Aaron: But the gripe sites are the ones that present the trademark issues. So those for me have this different component to them than...

Faisal Shah: Yes.

Greg Aaron: ...the pornographic or offensive. I think they may have some issues in common but they also have some issues that distinguish them, that’s all.

Faisal Shah: Yes.

Greg Aaron: Okay. Go ahead please.

Faisal Shah: I think that’s right. I think, I just see it actually, you know, even in pornographic sites, you know, that's, you know, to some degree it’s a speech issue as well. I think that’s right though Greg.

The so on the - I - we kind of went through and looked at the gripe complaint Web sites. And we talked a little bit about in our working group about, you know, the freedom of speech issues that come up there. And that’s really where the big issues are.

And I would say that, you know, in looking at a lot the different cases and WIPO you'll see that there’s a, you know, freedom of speech really rings as being the big defense that keeps coming up.

And in a lot of cases in a lot of the WIPO rulings are trending towards the freedom of speech. But like you pointed out Greg before, there is this - there are inconsistencies. And, you know, we are seeing a lot of these - a lot of cases that were coming out on either side.

The other thing that we saw or we discussed was the fact that, you know, some of these gripe sites are really, you know, can be a value to some of these companies. And, you know, they use those gripe sites to go in and take a look at, you know, what customers are saying.

So there is some value. There are some freedom of speech issues that keep coming up. The UDRP is there to try to deal with it. But UDRP as you can see and some of the court cases really kind of go all over the place in connection with this with the, you know, with them falling on a lot of different sites.

But one of the things that I did look at and I was kind of trying to figure out why some of these cases were kind of falling, you know, could go either way on the freedom of speech issue is because sometimes like if you look at the RadioShack case they’re not really griping.

But they use RadioShack sucks but they're not really griping. They're just using pay per click and then there's competitors on there. And so that's skewing kind of what's really going on.

If they're truly, somebody's truly putting a gripe site up and is actually griping and complaining about a particular company and they've got , you know, RadioShack sucks or whoever, you know, it is, then I think it, you know, it might a little different.

And we also...

Greg Aaron: So...

Faisal Shah: ...added some - go ahead.

Greg Aaron: So this is Greg. So when people - when you have a UDRP case and the person really has built a complaint site, are those decisions consistent or inconsistent?

Faisal Shah: Well it seems to me like those cases seem to be relatively consistent. I mean I haven't looked at every single one of those cases.

But if it's truly a gripe site, and they really are griping with, you know, put aside any other liability issues they may have, that seems to be a little different than putting, just using the sucks word and then suddenly using it completely differently.

But there are some exceptions to the case. You look At the Air France case. And but, you know, but then those cases, that case kind of came down to what does the word, you know, sucks - what does sucks really mean?

So you could have panelists kind of, you know, kind of going off on a tangent. But the way it should work I would think is if you really have a gripe site then that's kind of the way it, you know, and it's you got the sucks word or whatever it is, then it's the freedom of speech rule is rule.

Greg Aaron: Okay got it. Thank you.

Martin Sutton: Hi. Sorry it's Martin Sutton here. I had the mute button on. Just to interject there. I think the only real cases that we came across that had a deviation of that main theme was if there was any slanderous accusations within the comment.

So that would take in itself a separate course of action. It wouldn't necessarily mean the removal of the domain name from the existing registrant to the complaint.

So I think the whole thing that we were coming across tended towards the idea that if it's set up as a gripe site and that's the purpose that is there being presented, then that's tends to be a no-win situation for the complaint. It's left to run.

Greg Aaron: Right, right. And the - and slander of course, the definition of that varies widely. The rules and Great Britain for example seem to be very different than in the US -- a little more tough it seems. That's all.

Faisal Shah: Okay. Martin did you have anything else?

Martin Sutton: Not on that point, no Faisal.

Faisal Shah: Okay. So the other I guess we then took a look at, you know, like you - as you talked about Greg, you know, we then realized that wait a minute, you know, you got the gripe and complaint sites. Those really are the freedom of speech issues where those freedom of speech issues really coming in.

Now you get the pornographic offensive strings, registration deceptive names. Suddenly we're coming into a whole different territory here. And how do you really deal with that?

I think we talked about at one point that maybe one - in one category you're dealing with a potentially certain harm that may affect maybe companies or brand holders or whatnot in the gripe sites.

But then when you start coming to this other category maybe you have the more direct impact on consumers.

And so I mean, you know, when you really take a look from a brand holders perspective, if you have an offensive word and it's got their brand in the domain name and then it points an offensive content then, and then maybe there's a logo in there, then obviously there's, you know, brand holders perceive that as the tarnishment of their brand.

Again, you know, the UDRP is one mechanism that can be used to be able to remedy that. Obviously here's a, you know, I put a article in there that talked about that specific thing.

And if you see, you know, in here it was free, I think it was FreeLegoPorn.com. And one thing I wanted to point out was this was a, you know, this is a porn site, but the interesting thing about it is, it's not really deceptive, because under the deceptive laws which are the - which I'm going to come to in a second, you know, if you have porn or sex in there you're not, the domain name isn't really misleading.

So this kind of falls into that other category which is really just a pornographic site that's kind of pointing to pornography and therefore, you know, maybe falls under B.

Again maybe the cyber squatting rule, maybe if you put this in a cyber squatting context and maybe this - it's addressed and remediated using the UDRP at this point.

Now you fall into the other two which is the deceptive names, maybe offensive strings, and then we talked about that a little bit as well.

And United States government obviously has the Truth in Domain Names Act which is - which regulates misleading domain names, try to prevent kids from viewing obscenities, trying to prevent adults from being misled into certain sites obviously it becomes a crime.

And one of the things that, you know, we were thinking is maybe these are a little different. Maybe these need to be handled a little differently.

Also we talked a little bit about in our working group the potential ccTLD registries. And there's more than just the US. But the US actually seems to blacklist the registration of seven dirty words and appears to be additional ccTLDs that are out there that I've seen that actually regulate how you use dirty words within the domain name.

I don't know Martin, do you want to - I don't know, you probably want to jump in here because this is kind of where you're - where you had some thoughts about what we should do in this area?

Martin Sutton: Faisal), yes it's Martin here. Yes, from our discussions last week we had a bit of a rethink here. Because I think if you look down the definitions of the four categories that we've now got here, this one category, offensive strings, was one that was causing us some problem last week.

And when we step back and have a look at it again, this I think needs to be treated with the sense that this is irrespective of brands because we're going down the route too much about cyber squatting and how brands are affected.

I really didn't want to look at it that way. I wanted to look at it from a consumer perspective. And in a non-virtual world you don't tend to go down the high street and see shops called F-U-C-K or other expletives that your families and friends have to witness down the high street.

And yet with the Internet being as vast and open as it is it’s all out there. And it’s so easy to register these expletives terms where you can’t anticipate what’s going to be on the site in terms of content.

But it seems to promote the idea that you can do anything you like on the Internet. And I think perhaps this is an opportunity for us to explore how more of a corporate responsibility attitude needs to start evolving with the use of the Internet.

And as we started to have a look around, and certainly .us has got some policies against that. Others have, but these maybe are ccTLDs. We thought that this is an area to explore. This isn't them going down the cyber squatting root this is really a consumer harm area that we’d like to explore further.

So that’s been put in the issues log there for your comments and to feedback on. So really be interested in other people’s views.

Faisal Shah: Also, Greg, go ahead.

Greg Aaron: I was going to say the floor is open. If you’re not speaking please put your phone on mute so we avoid background noise. And I see James’s hand and then Phil’s. James you’re on.

James Bladel: Oh I'm sorry. I thought I was behind Phil. Thanks guys.

Man: Go ahead.

James Bladel: Martin. Hello? Am I on?

Greg Aaron: You are.

James Bladel: Okay, thank you. Martin to your point, I think there's some validity to the idea that, you know, that there's certain - that the Internet is especially in terms of domain names a free-for-all in terms of what you can register.

I do just get a little cautious when we start talking about what we can do about it. And I think that we keep coming back to the only action to be taken necessarily is preventing the registration of certain letter combinations.

And I want to reemphasize that these are strings, not words. And sometimes strings can look like words. Like sometimes strings can have meaning associated to them or they can be identical to words.

But from a technical perspective, sometimes adding or concatenating strings together will give the impression that there is a word. And there's a couple of famous examples of that as well.

So I just want to say I'm a little cautious. But, you know, that said Go Daddy I think, you know, does monitor those kinds of things. And we will occasionally block or investigate things that we feel are unnecessarily offensive.

Martin Sutton: Can I just respond to that Philip before your turn? Is that all right? It's Martin here? The - I think you're right there. There is a - we have to be cautious in how to approach this.

But I think it's one that we shouldn't ignore. We probably need to investigate further. And perhaps one of the suggestions would be to see where certain policies have been applied already. Have they been effective in any way? What has it prevented? And if there is anything useful to take from that to explore how to broaden that as best practice or minimum standards -- something like that.

The strings...

Greg Aaron: Right.

Martin Sutton: ...the different languages I think is all problematic. There’s something that we can actually do something about in steps and stages.

So if we do some research I think first of all and then perhaps come up with some more stronger recommendations. But I think only thinking that through this week, it was useful to just take it away from any of the brand related issues. Because I think that tends to - that plug us down somewhat.

It’s not a brand issue. This is where it’s the consumer harm that we’re focusing on on those specs. And that’s why I think it’s one of the different categories that we've got in the paper here that we could do more investigation on.

James Bladel: Okay. Thank you. And I did want to mention as well, in addition to, you know, the known offensive words that there is this concept of the ever-changing landscape of slang and other types of, you know, vernacular or acronyms that are used in, you know, chat rooms and things like that.

And it can be, you know, it’s not a static picture. It is changing. So I think that that’s something that we should also bear in mind.

And I wanted to throw one more idea out there which is that if we were to somehow have a way to block all registrations at the second level of offensive terms would be a relatively straightforward matter to put half of the offensive string in the second level and then create a sub post that had the other part of it - so that you have a dot perhaps in the center of that offensive string, but to the human eye it’s a - it is, you know, indistinguishable from the offensive string itself. So...

Martin Sutton: Then they all look (the same), yes.

Greg Aaron: Okay. I think Phil’s next.

Phil Corwin: Yes, thank you. I think this is an area where we need to be very, very cautious particularly in the area of trying to cut it off at the registration stage which is what this group is all about.

And I don't remember all my - obviously US law is just one law here, although certainly with .com its - if anything goes to court, that’s the law that’s going to apply if it’s a US-based registry.

But the general, you know, remembering what I do of First Amendment cases and Internet related First Amendment cases, the general rule in the US is no prior restraint of speech is generally permitted. You can only deal with it after the fact.

And pornography is not illegal. Only obscenity is illegal. But that’s under a very archaic standard of community standard and nobody knows what the community is anymore.

In the Internet context, looking at these various categories on a complaint side. If somebody registers trademarks sucks.com, there’s no way the registry or the registrar’s going to know at that stage whether it’s going to be used in a way that under US law is permissible which is to be a legitimate criticism site of the company or the service or whether it’s going to be used in a way that probably wouldn't withstand scrutiny which would be to show PPC as a pornography or something like that not related to a legitimate free speech purpose.

Again pornographic and offensive sites in the US, there’s no law against being - to protect people from being offended. If they see a URL that they think might for a Web site, that might contain content that would offend them, their best defense is to not to click and go to the Web site.

Pornography is not a legal. Only obscenity is illegal in the US.

Again, offensive strings, I don't know what the rules are in the broadcast context, you know, there were the seven dirty words that the FCC outlawed. But that was in the context of public airwaves which doesn't apply to the Internet where there’s no shortage of bandwidth.

And deceptive is the one that probably under US law that gets away from speech and into deceiving people often tied to scams.

There’s been a general distaste for sites which are designed to attract minors. There are some sick people out there who register sites that give no warning that there might be illegal content. It’s a name that might appeal to a minor and they click on a site and they see something very shocking to a 7 or 8-year-old. Nobody likes that.

But even there the US Congress has tried to pass a number of laws aimed at restricting Internet speech to defend children. And generally they’ve been struck down as overbroad.

So this again in the context of what a registry or registrar should do at the point of registration, this is a very tricky area particularly when you’re dealing with a TLD that’s housed in the US.

I'm not trying to defend any of these, I'm just saying that when you get into free speech and particularly US law which tends to be the most permissive, you’re really in a minefield.

Greg Aaron: Thank you Phil. I think Mikey was next.

Mikey O'Connor: Thanks Greg. This is Mikey. I was getting ready to say pretty much the same thing as Phil said just now. But he did a much better job of it than I can except to amplify I did have some experience with the seven dirty words legislation because I was involved with community radio at that time. It followed the trajectory of that suit through District Court and Supreme Court.

And Phil points out the essential difference between seven dirty words kinds of law. And that is that that was in the context of broadcasts which is a limited spectrum that's managed by a federal agency whereas the Internet does not have that.

So just to reiterate what I've been saying on all these meetings, I'm fine with running down the cyber squatting leg of this argument. But I am extremely uncomfortable with any of the speech kinds of things and would continue to register very strenuous objections to anything in this regard.

Greg Aaron: Thank you Mikey. James, I see your hand is up.

James Bladel: Yes, just very quickly I wanted to echo a lot of what Phil was saying earlier, especially the note that he made about prior restraint on free speech. It's a very, I think very important consideration that we have to consider while we're doing this.

I wanted to add just two quick items. One is that there are just probably some practical approaches to addressing this issue that maybe step beyond policy a little bit and avoid some of the free speech issues.

For example, one might be a new registry or a new TLD could preemptively register anything that it determined was offensive, like for example the seven dirty words or something like that and then just, you know, keep those on file, you know, as a perpetual renewal on, you know, on their reserved list that they don't resolve.

And that has I think the same effect of taking that, at least those strings or whatever strings the registry chooses out of circulation without, you know, stamping all over the idea of their available but we're going to block people from registering them.

And then the second point would be that a lot of registrars, especially the large ones are also hosting firms. And there a lot of independent hosting firms as well that are not necessarily ICANN accredited registrars.

And most of these folks will have terms of use or sensible use policies or terms of service that will describe content that is acceptable or unacceptable.

And it's usually a much more straightforward method to just make - send a complaint to the hosting firm rather than the registrar to get some action taken on these names.

They usually have a lot more latitude under those agreements then they might under law or under ICANN policy. So I just wanted to throw those out there. But otherwise I wholeheartedly support a lot of what Phil said.

Greg Aaron: Okay. Thank you James. This is Greg. I have my hand raised. I mean personally I think Phil has raised some very interesting policy and legal questions. James has also raised some technical questions.

I mean one of the technical issues is well which names do you block and where do you stop making that list? You could have literally hundreds to thousands of strings you could block because there many different languages in the world.

One of the issues that people have raised in the past is if you block a name aren’t you blocking some legitimate registrations? For example if you block the word breast you cannot have any Web sites about breast cancer. So there’s some issues there.

I think - I have seen on the ccTLs deicide that some ccTLDs do have policies against these offensive words. Some of them block a few that they’re really worried about.

I think very few of them block at the time of registration and may address it afterwards. For example, that may be what .us does. It probably doesn't block strings that contain certain words but they may be able to address it after the point of registration. I don't think a lot of them do it at the time of registration. I think there’s a fundamental difference though between ccTLDS and GTLDs though.

The ccTLD is generally considered a public resource for the citizens of that particular country. And the country or the domain overseer has a right to do that kind of thing based upon the local laws and the wishes of its government.

And then and that’s kind of analogous to the situation the Phil brought up. He said, you know, broadcast is different because that is using a public resource. And that’s why you can have those seven dirty words not on broadcast television.

The ccTLDs are one thing. The GTLDs are very different. They don't belong to a particular country. That belongs to the Internet as a whole.

So I think the ccTLD analogy and their practices only are applicable so far. I don't think it’s quite the same as the GTLDs.

The issue of the seven dirty words is actually, I'm sorry one more thing. The issue of the seven dirty words is actually addressed in 1999 in .com.

At that time network solutions was the registry operator. That’s before it got split up and VeriSign became the operator.

But at that time the registry blocked the seven dirty words and was sued by someone who said that was a restraint of free speech. And the registry changed its policy to allow registrations containing those strings.

Okay. I see Phil’s hand up. Was that who wanted to speak?

Phil Corwin: Yes, yes I just wanted to add one thing to illustrate, you know, what a strange area it is. On the FreeLegoPorn case, now apparently they lost the UDRP and they didn't appeal.

I'm not sure what - if they had appealed to a US court they may well have been able to keep the site and been able to keep showing what they were showing there.

There was nothing deceptive about the domain name. Lego might not like the fact that Lego blocks were used to create figures engaged in adult activities.

But, you know, this is the kind of thing that you sometimes see in art museums around the world. So I think we’re all a little uncomfortable because the word Lego would adopt - might attract minors to this site.

But there was really nothing obscene much less you could even argue whether it was pornographic. So it’s just - that’s a case where they didn't exercise their legal rights to go to court.

I think under US First Amendment law they - the registrants that they had wanted to fight to keep that Web site and keep the content they had there, I'm not sure how that case would've gone.

But again in the context of registration, I don't think registries or registrars want to be in the position of being asked to arbitrate First Amendment issues for US-based registries.

I agree that CCs are very different. They’re owned by the nation to which they’re assigned. .US of course can’t have rules which conflict with the First Amendment in the United States.

But other countries with their CCs are entitled I would imagine whether we agree or not to adopt whatever rules they want for domain names that can be registered or barred from being registered. But generic TLDs are quite a different story.

Greg Aaron: Thank you Phil. Anyone else?

Faisal Shah: Could I just continue on here Greg?

Greg Aaron: Well I have a question Faisal. I’m not - I don't necessarily want to cut off discussion but we’re about 45 minutes into the meeting. We’re halfway through.

You have a document out there that goes through the background and then it has three recommendations. And we do have some other material we want to try to get to today.

We've had some discussion I think which has zeroed in on some substantive issues. Would everyone be willing to take this conversation to the list and talk about any suggestions they have for the background and also whether they like or dislike the recommendations?

Faisal Shah: Well can I just go through the recommendations real quick and so everybody understands them?

Greg Aaron: Absolutely, go ahead.

Faisal Shah: Well I think there was really three recommendations. I think it kind of tracks what we’re talking. It’s not really different. But one of the things - we do think that maybe some of the offensive site and gripe names, that it probably should be addressed in the context of cyber squatting for establishing consistent registration abuse policies in this area.

Number two, to some extent based on what we’re seeing in terms of some inconsistencies, maybe the UDRP should be revisited to see what policy changes need to be made to make it more consistent in connection with gripe sites, offensive sites, what not.

Maybe there needs to be a procedural change or substantive change in terms of being able to bring some kind of rapid takedown mechanisms or whatever you want to call it, suspension mechanisms and then of deceptive domain names that mislead adults or children to objectionable sites.

And then the third recommendation was really us just saying look, you know, Martin and I thought it'd be probably be a good thing for - from an internal best practices or maybe additional research needs to be done for registries - registrars to consider restricting these - the registration offensive strings in order to mitigate the potential harm to consumers and children, especially minors.

I guess we weren't making this a mandatory but just a, you know, maybe a best practice should be instituted so that we should look at how we can help minimize consumer harm. And that - those really were the three recommendations.

Greg Aaron: Okay. Thank you. First I'd, Phil do you have anything else to say? I see your hand raised.

Phil Corwin: Oh no sorry. I'll take it down.

Greg Aaron: Okay. No problem. Oh just for the record I want to note that Berry Cobb has joined the call a little while back.

Okay. So first of all thank you Faisal for writing this up. It gave us really substantial stuff to work our way through. So...

Faisal Shah: And Martin as well.

Greg Aaron: Appreciate that, and Martin as well. Thank you both.

What I suggest we do now is we walk through the main issues, the recommendations. What I'd like to do is take this discussion to the list and ask the members to comment back on the material and we'll kind of get a feel for whether you want to see any changes or you have any ideas for modifications, et cetera like we always do.

So if that's okay I'll put that down as an action item for all of us. And we can move on to the next item.

Next item is fake renewal notices. And I'm going to turn that one over to Mikey. Mikey, we've had discussion of what these are. Can you tell us what new material you're bringing to the discussion and kind of get it down to brass tacks?

Mikey O'Connor: Greg this is Mikey, yes. This document that's in front of you -- and thanks Marika for putting that up on Adobe --, came out of the action item that I had from the last call where we wanted to get some examples of the written fake renewal notices that sort of predated the electronic mail version that I put in the write up.

And so I just went out on the net and got a few easy to find ones including the famous one back in the day when VeriSign was slapped by the FTC for doing this.

So it's really just an appendix. I haven't seen the main document at all. This is just a flushing out of more examples with no particular commentary except that, you know, I've found some from as early as 2002.

I found a peppy little article by (Kiran McCarthy) before he worked for ICANN describing the VeriSign one.

I found an example of the Domain Registry of America letter that sort of built out the portfolio along with the email that I had in the last document.

And then just because I wanted to get something that was a little more current I think the main Registry of America one is the most current one. That one's dated 2007. But then there are other flavors of the same letter coming from in this case, the same registrar but a different name.

It's - the last one in that little pile is the Domain Registry of Canada, a slightly different format of the same thing.

So there's really - this is really just a documentation of the no change to the original document. Greg, back to you.

Greg Aaron: Okay. So the - my recollection from the last time was that we have seen it seems mainly resellers engaged in this practice.

The infamous is the Domain Registry of X, you know, Canada, United States, New Zealand. They're a reseller as far as I can recall. I don't think they've ever been an ICANN accredited registrar in any fashion...

Mikey O'Connor: Greg, this is Mikey.

Greg Aaron: ...or is that wrong?

Mikey O'Connor: No, it turns out they are a registrar. And I don't have my original document in front of me but I name it in there.

They - you know, whenever you go through this process you are directed to the registrar. It's a funny name, (Darien Gray) but that's not quite it.

Greg Aaron: Brandon Gray.

Mikey O'Connor: Yes, Brandon Gray, thank you. (Darien Gray) is something else.

And so it strikes me that in this particular case the notion of an ICANN enforcement action based on existing policy probably still works. I'm not sure that we need anything new. We may just need to refine this a bit so that it's clear what the enforcement action is.

In all cases it appears that the easiest enforcement path to pursue is inappropriate use of WHOIS data because that's the source of the names and addresses.

Though the very first letter, the one from VeriSign was posted by a fellow. And if you follow that link he is describing the fact that he never ever used the domain names that they are slamming him for.

And so the only way that they could've found out about it was by mining WHOIS data in order to get his contact information.

And so I don't think that the substance of the write-up from last time has really changed much.

Greg Aaron: Okay. This is Greg. So is WHOIS mining or, you know, misuse of WHOIS, the only enforcement option that is currently available to deal with this deceptive practice?

Mikey O'Connor: This is Mike again. I think that's right. It turns out that from a deceptive practices law standpoint, these pieces of paper and emails are very carefully constructed not to violate the law.

VeriSign was sued and they were not found guilty. And most of the - at least the ones - the cases that I reviewed -- and I'm not a lawyer so I'm not good at doing the definitive review of this -- but at least the ones that I could find on the net, it's actually easier perhaps for ICANN to do something about this than the courts. And the WHOIS data seems to be this - the main leg to stand on here.

Greg Aaron: Okay. Does anybody else have any comments or questions?

Okay, I'm not seeing any. Well so Mikey does that then translate into a recommendation that ICANN look into these cases from compliance standpoint?

Mikey O'Connor: Oops, I was very eloquently speaking into mute. I think that that should get added to the list of recommendations that we had on the original document.

I'm feeling like an idiot for not having that document open in front of me. So I can't remember what the recommendations were.

But clearly that should either be reinforced or added to that list.

Greg Aaron: Okay. Well maybe the best thing to do then is pull up the document and make whatever changes would be appropriate that you feel and then post up a new version.

What'll end up happening is your document will be then dropped into a master document that Marika will have like all of our other work.

And so if you have the overview background and recommendation section then, you know, we'll drop that into a master document and we'll run through it again probably next month.

Mikey O'Connor: Greg, hang on just about 5 seconds and let my computer bring the document up so that I can just check really quickly to see.

Marika Konings: This is Marika. It's also up on Adobe Connect. I think that's the...

Mikey O'Connor: Oh, thank you, thank you.

Marika Konings: one we discussed last week if I'm not mistaken.

Mikey O'Connor: Yes. If you run down to the Disposition Option List, what we were puzzling about last week was whether to distribute this to other working groups, essentially breaking the issue up into parts and handing it off to the working groups that might be interested.

And I guess where I wind up on this is to say that we should keep it in a single issue just because it risks getting lost in the shuffle in the other working groups and then adding the recommendation not ICANN should perhaps take a little bit more aggressive approach to enforcement on the WHOIS data side. And I'll add that to the list if that's okay with people.

So what I would do is I would highlight that the last bullet on that list to keep in the proposed RAP PDP be the one that we recommend and then the final one talking about increased enforcement. And also that would been one that we recommend. Does that sound like a good approach to those of you on the call and then following along?

Greg Aaron: No, that sounds good to me.

Mikey O'Connor: Consider it done.

Greg Aaron: Okay. All right. I'll put you down for that action item. Thank you Mikey, good job.

Okay, if nothing else there, we can move on to domain tasting and kiting. And what we do have from ICANN is we have seen some statistics about how the new add grace period excess deletions policy has changed the landscape.

Marika also sent out a note. And correct me if I'm wrong Marika, but when registrars do incur excess deletions it's usually we don't know why they had those excess deletions.

If they do want an exception to that policy they have to send in a request. But those of been very few and far between so far.

So if they do have excess deletions we don't know why they were deleted. Could've been, you know, somebody didn't pay for their registrations or they could've been abusive or we just don't know. Is that an accurate summary Marika?

Marika Konings: Yes, that's correct.

Greg Aaron: Okay. So I guess my question is what do we need to be talking about if anything regarding tasting and kiting? We have some definitions now that differentiate between tasting and kiting.

I sent around some notes about that info. And I looked for examples of kiting. Kiting would be where you're getting a free registration because you register it and then delete it in the add grace period and then you immediately reregister it and you could string it out.

I did a study in info. I could not find any examples. And the examples of re-registrations, I couldn't tell why they were reregistered. They didn't go on forever. And I think in some cases they're probably just possibly glitches or credit card issues or something not necessarily abusive. It's hard to tell. But I didn't seem them string out for a long time.

Did anybody have any questions about that data I sent out?

Okay. Not hearing any, so I guess a question is are these - do we need to make any recommendations about these? Do we have any recommendations about tasting and kiting?

Mikey?

Mikey O'Connor: This time I actually have the document open that I wrote last time. In there we said that our choices were to refine the definitions. And I think we've done that.

Another was to check with other working groups to determine if follow-on studies have definitions and data that we could use. And I think we've done that pretty well, especially with Marika's research.

And then our last possible action was to conduct broader research at the registry level to determine what extent domain kiting is the problem. And we've at least done a bit of that with your .info research. And the conclusion at least based on .info is that this isn't a problem right now.

And so I think the only tiny little remaining nail that we need to put in this coffin is perhaps to hit one more registry and see if, you know, or - and see if it's documentable there.

But I wouldn't feel terribly strongly about doing that given the results that you've had in your research Greg.

So we may want to add a final consensus conclusion to the little write-up that says no action required at this time or we could just put it in our report summary and then refer to this longer document as a background.

Greg Aaron: Okay. Thank you Mikey. I see James’s hand raised?

James Bladel: Yes Greg, thanks. This is James. And I thought that one essential avenue for recommendation would be to include these definitions in any review of the excessive belief policy and just to make compliance or ICANN staff aware that there are other possible abuses of the add grace period that they should be looking for and just make sure that they’re on top of any new abusive or exploitative procedures as they come up.

Greg Aaron: Okay, thank you. Anyone else?

Okay. If there’s no additional questions, it sounds like all we need to do Mike is do you need to maybe touch up your document? Maybe you and James could work on James’s recommendation if that’s okay. And then it sounds like we’re wrapped on this topic.

Mikey O’Connor: This is Mikey. That’s fine. James and I can do that. And one other one that we might consider tossing in and maybe we'll put in the draft came to mind when James was talking.

And that is that maybe we want to collect, right now we don't collect the delete data in such a way to be able to tell whether this is going on. We might want to reconsider the way that the lease data is collected for the monitoring that ICANN already does. So we'll tinker with that a little bit and see if we can come up with something here.

Greg Aaron: Okay. I have a note about that one actually. Wouldn't that require the registrars to report to ICANN why a name -why names were deleted or are you just talking about why the excess ones were deleted?

Is there - I mean what's...

Mikey O’Connor: Yes, well it’s Mike again. I have to sort of puzzle through this. I mean what would really be probably required to get to the bottom of this is essentially the sort of scan that you did of the registry on a periodic basis to find those and report them in whatever number you found them.

And I don't know if it’s - I'm teetering on wondering whether it’s worth the trouble I guess where I'd get to.

Greg Aaron: Well the registry can tell you how many names are deleted in add grace period. And they’re already required I think to report those in the ICANN reports every month, have been for a while I think.

Mikey O’Connor: Yes.

Greg Aaron: So we already know. I mean the real issue is why were they deleted? Only the registrars can tell you that.

Mikey O’Connor: Well what I was thinking is rather than going after the why, that instead you could just go for that pattern that you want of names that were repeatedly renewed within the AGP and just count them. And say okay, in the last month or last quarter -- whatever that of was -- we saw six names renewed more than X times, say five times within the AGP and just tack that onto the report.

But rather than pulling out the motivation, just look for the behavior because that would be so much easier to do from a computer standpoint, be an easier scan of the database. But I can...

Greg Aaron: Why don't we ask another registry to take a look? Maybe we can get another registry to do the same kind of thing I did.

Mikey O'Connor: Yes, I think that would be fantastic. I mean clearly the one that would be spectacularly fantastic would be .com because if it's going if it's going to happen anywhere, it's going to happen there.

And if the answer came back no, we don't see it either, then I think then this is done with a capital D.

Greg Aaron: Well let's - maybe we can get somebody else to look at it too then.

Mikey O'Connor: Well we'll add that to the report and get back to you.

Greg Aaron: Okay, all right. I would really like to move on to the next topic then which is use of stolen and fraudulent credentials.

And Rod Rasmussen took this one on and he sent some material up to the list.

And I see it coming up, thank you Marika and Gisella. And Rod, would you like to walk us through?

Rod Rasmussen: Sure. Thanks Greg. My apologies for of course waiting till the last minute to get this out to the list. But hopefully we could at least have something to frame the discussion we've had here for the last couple of days or a couple of sessions on this.

I tried to concentrate on getting a good set of definitions for what, you know, these credentials are that we're talking about, because the terms credentials has many, many meanings, most of which I actually didn't include here but tried to keep the - keep it down to what actually makes sense given the uses we're put - we're - or the uses we're discussing.

The - and I put some helpful definitions in. So I grabbed from a couple places on the Internet for what credentials are. But getting down to what action matters, I think that we - there's three types of credentials.

And we've largely been talking in the - in this group in the last couple of weeks about the third set which is more financial credentials, which ironically I mean you're looking up definitions and credentials is very loosely described where the other kinds aren't - the other two identity credentials and access credentials have a bit more meat on them so to speak when looking up various definitions of credentials.

But I think all three are important for looking at what needs to be or what's to be discussed I think as far as the domain registration process.

So I identified those three types, identity credentials. The idea there is these are things that describe a person or entity. And they're used to establish that identity, think of things like your driver's license or passport or identity cards. Things like that are typically used there.

This kind of just editorializing, you know, you can think of this as the things that are used to verify both transactions and to establish things like in the domain registration world, WHOIS information.

Access credentials are the - this is the area were very familiar with and the abuse fields. These are the username or passwords are other ways you get into systems or services that give you the ability to do something with those services. And they're what's in the US called a protected system or in other words a computer.

And that is actually extended a bit with the Patriot Act of all things to a - be very specific on what abusive of access credentials is, in other words, hacking into computers, why that's illegal and et cetera.

And then financial credentials gets you to credit cards, debit cards, various ways of accessing financial systems that you have the ability to do using these kinds of credentials.

So those three are the ones that seem to be germane to domain registration, you know, the identity who you are, access, ability to get into a system that perhaps does domain registrations and then financially being able to do registrations using some sort of a guaranteed payment system.

Those are - I - my argument, I took this to - they're fairly disparate as far as, you know, there are different ways of going after these things that the bad guys use to purloin them. And as such, we want to look at them separately as to how you would deal with that from both a - well actually first of all I went into looking at how they are actually abused.

And then from that you can take a look at how you'd actually want to deal with any policy, best practices, et cetera, for dealing with issues when it comes to domain registration.

So I've outlined some of the uses. I think there are - or some of the uses and abuses of these various credentials by each type.

The - basically it's, you know, with identity credentials you've got, you know, you've got a bad guy or a monster -- or whatever you want to call them -- using somebody else's identity to perpetrate their particular crime or scheme or whatever they're up to.

And, you know, there's a few different ways you can do that. And in the world of domain registration you can use that to help heighten the authenticity if you will, of your attempt to deceive.

Use of access credentials, that has a couple of different ways of being used in the system.

Obviously if you have access to somebody's domain registration and account, that's a pretty direct way of being able to abuse the registration system.

And if you have access to either an account that is used to verify that you are who you say you are, say for example somebody's email account, you can get the domain to make the changes based on sending you an email and you approving them.

Or you have access to a machine that's actually tied directly into the domain registration system. And a good example of this would be a domain leased, or a reseller of a registrar who system has been hacked.

And then you can do all kinds of registrations without the - really the permission of the registrar or the person who may be impersonating.

And then finally on financial, I think the financial credentials - those are fairly straightforward and you're basically stealing somebody else's money to get what you want with domain registrations.

And I think that we've spent a lot of time talking about the financials credential, use of credit cards and the like because that's what we see the most as far as, you know, people setting up lots and lots of domains. They use stolen credit cards typically to do that.

But I think that an important observation we've had here in the anti-phishing, anti-malware world lately is that a lot of the recent kind of attempts at getting access credentials at least is to get into infrastructure elements.

We’re seeing a lot more attacks where they’re going after people who have control of various systems through these access credentials that they can then turn around and reuse for whatever they want to do with it. And that, you know, and that’s not just for domain registrations but all kinds of systems.

I've seen a lot of attacks against ISPs and things like that. So there’s certainly a shift I think within but criminal element of what they’re attacking. So that’s something to take note of.

And then I kind of did a little bit of analysis. I tried to include some of the things we've talked about as far as, you know, how we might want to address some of these things, you know, as part of the working group.

There was a lot of discussion on free market forces. And I put that in there as well. I think that’s really important that you don't want to come up with a system especially when you’re talking about trying to prevent crime and fraud that’s fixed because that gives the bad guys a great opportunity to know what the system is and then work their - or circumvent it.

I think that - I mean I - there’s - you could dig through that for some other information I have there.

And then of course we have the disparate kinds of business models that are being used by different domain registrars and their resellers.

I think what makes sense is to take a look at the kinds of abuses we’re seeing and the trends we’re seeing and just - and concentrate on those rather than kind of the hypotheticals of well they could do this or they might do that, you know, in some sort of a - an odd scenario.

And then I've got some placeholders to finish out the work there. There are some models from other industries I think that can be looked at as far as how members of the different - of a specific industry are - handle abuse issues like this.

One of the interesting things - I didn't have it down here on the paper here yet, but the PCI, the Payment Card Industry standards actually have some interesting relevance here and it’s been brought up in prior discussions.

But one of the things that is interesting is that there’s a standard that is met but you have to actually go through some testing to meet it and verification which and that doesn't - so not all merchants for example are PCI compliant although new credit card companies would like them to be.

So there’s some wiggle room around and there are some that might be looked at as far as whether or not you want to do something more stringent than just suggesting things or actually having them, meeting a specific standard.

And then I've got some placeholders in here for, you know, we could look at best practices or minimum standards or - and there’s a few particular things about data sharing.

I think one of the interesting things about the domain registration space versus other merchant spaces that might be - or other ISPs spaces or things like that that might be attacked using stolen credentials is that there are informational elements as part of the domain registration process that can be used in conjunction with looking at the actual credentials to help determine the validity or invalidity of a registration attempt.

And those deal with, you know, WHOIS information, how the domain is being registered, name server information -- things like that that you could tie back into.

And I think one of the - and this is a theme that I think encompass a lot of other areas of abuse. One of the issues that we see in the fraud world is there's not - or in the anti-crime world that ideal in all the time, is there's not a kind of a universal clearinghouse model. This is being discussed in lots of different places as far as being able to do data sharing.

One of the things that I think might be important to establish at some point is just the basic ability for there to be data sharing. And it's not really clear whether you can or can't.

It would be nice to have some direction on that so that some of those efforts that are looking to do that are supported by that. So that's one of the other things I have in here is the ability to allow data sharing between registrars and resellers, et cetera.

It's kind of a - one of those ideas for how this particular issue is - could be affected by policy/best practices, et cetera.

I think that's about it. I've covered all the highlights on that. Off to you Greg.

Greg Aaron: Thank you Rod first of all for writing all this material up. I thought the definitions at the front were also very useful background.

First let's open it up to questions. Martin?

Martin Sutton: Hi, Martin here. Yes Rod, I think this is really well done in terms of breaking down the key elements and into different types of credentials.

With regards to the stolen access credentials, is there anything that we can extract out of the (ISAC) report? There is that (ISAC) 040 I think it was that talks about the security elements within registry, registrar, mainly registrar I think, areas, but also the registrant responsibilities which you've covered here in terms of specific areas of - areas to look at.

I'm just wondering if that would lend itself to applying sort of best practice at least or so minimum standards?

Rod Rasmussen: Yes, I think that the (ASAC) report had lots of specific recommendations within it. And I believe those are being looked at in some other context as well. But I think certainly during the registration process that would come to the fore when you have somebody who's illegally obtained access to somebody else's account.

So yes, I think that might be a good place to refer some of those recommendations to or at least use it as a basis for make a few recommendations or jump off points for further development of policy, et cetera.

Greg Aaron: Okay, any other questions Martin?

Martin Sutton: Sorry. I was on mute again. No, thanks Rod. I think it is a paper worth running through and seeing if we can extract anything of relevance to the specific areas that you've listed here. But that was my one comment.

Greg Aaron: Okay, thank you.

Does anyone else have any questions or comments for Rod?

Mikey?

Mikey O'Connor: This is Mikey. Just a comment that this was a great treat to read this morning Rod. It was a very nice piece of work.

And I'm hoping that a lot of the ideas can turn into recommendations for people going forward. Because I think that, you know - and this goes all the way back through things like the fast flux working group, holds a lot of those threads together, and this need for a better way to make our community a little bit more nimble in the way that we respond to these threats, so just a hearty (atta boy) for me.

Greg Aaron: Anyone else?

I mean I'll add my 2 cents. This is Greg. Oh I'm sorry, Caleb, why don't you go ahead?

Caleb Queern: Hey guys. Hey Rod. How are you?

Rod Rasmussen: Good. I'm on mute just because I...screaming in the background.

Caleb Queern: Sorry about that. Yes my question for you is are you aware of any tools or exercises that have been carried out to determine validity in aggregate, kind of collections of WHOIS data?

Say for example you have 100 WHOIS pieces of data right, or 100 different domains and, you know, eye-balling it, there appears to be something fishy or at least that there’s some things probably not genuine in the date itself, that maybe was falsified, not necessarily stolen but just false.

Are you aware of any tools or sort of things that have been done before by others that would help legitimize or test the validity of such kind of collections?

Rod Rasmussen: Well I know that there’s been, you know, ICANN has actually been looking at the - that particular issue in-depth of a series of studies they’re right in the middle of right now. So there’s something contemporaneous for that. And there certainly have been various studies over the years.

I don't know of any super comprehensive ones that looked at say, you know, a vast chunk of the WHOIS data. But there certainly are ones that have been done. And typically in, you know, ones I've - most of the ones I've seen have been in support of people pursuing anti-cyber squatting actions were they've found, you know, patterns of abuse so to speak, you know, across - and this is mainly in the pre - during the tasting days, et cetera, when people were doing large numbers of registrations very rapidly.

And so I know there's various cases that were brought by various companies going after particular individuals who were, you know, abusing their trademarks and actions.

As far as criminal stuff goes I'm - the a - I know that that's something that pretty much everybody in the industry collects data on that.

My - actually I believe actually that even the - no, I'm thinking back. I believe the APWG actually did do a bit of a study on this in conjunction with SecureWorks if I remember right. I have to - I'll see if I can dig that up.

I remember one of the things that we were - that came out of that particular study was that we were looking at uses for WHOIS and in fraudulent cases.

And one of the big things that we came out with is that -- and this is a WHOIS access issue came out is that one of the biggest use for WHOIS in domain - or into looking into investigating crimes with domains is that we contact the actual registrant of a particular domain who's been hacked or attacked and that a lot of people were assuming we wanted to look at WHOIS simply to find criminals. But so that was a big thing that came out of that.

But I do believe there was a study that would - had, you know, a certain number of randomly selected domains and the like.

I'm sure there are others that have been done by, you know, university professors and things like that over the years as well.

Greg Aaron: Caleb, this is Greg. Those studies that Rod refers to are doing - they're actually doing things like they're taking a representative list of domains and they're actually trying to contact the people who are listed as the registrants to see if they registered those domains, if they're who they say they are and so forth. So the results of those studies will be very interesting.

Some registrars do have systems to kind of check validity at the time of registration. It's one project that some registrars do.

One of the issues that they sometimes have is that there are not good databases that cover all the world. And if your registrar has got some registrations in from various places, there aren't good ways necessarily to match people up with addresses are to even validate addresses. So those are some of the issues involved.

Rod Rasmussen: Just let me add to that real quick Greg. This is Rod again. You know, I forgot to answer your other part of your question is that yes, there are certainly tools like data registration time that look at lots of the demographics about how something is being registered, geo-IP tools, cross referenced to WHOIS information, cross referenced to the credentials being used. There's a lot of ways you can do that and a lot of, you know, kind of off-the-shelf software is available for doing validations.

And as Greg pointed out, it's not quite universal in some cases. But in many of the cases it is very helpful at curbing bad guys from trying to take advantage of your system.

Caleb Queern: Great. That's very helpful. Thank you guys.

Greg Aaron: Okay. We're coming up near the end of the meaning so I think one of the questions then is what - now that we've got this background material I think I would suggest that everyone read it if you haven't had a chance already. It's still quite fresh. It was just posted. So please do read it over.

And then on the list let’s have a discussion of what you think of it. Rod has sketched out some ideas for recommendations. But I think that might be one of the sections we really need to concentrate on.

We've got this background. It delineates two areas one of which is basically people breaking into registrar accounts.

Another major component is cyber crime, people using stolen credit cards and such to sign up domain names very often for bad purposes.

So what I'd like to suggest then is an action item, read that, respond, especially please discuss the recommendations on the list so we can pick this up next week because we’re at the end of our meeting today.

So thanks again Rod and we’ll pick this up next time.

We have one more meeting in December which is next Monday the 21st then we break for the holidays. And then our meeting after that is Monday, January 4.

January 4 is the deadline to have all material basically written and drafted for all topics. And we’re pretty darn close to that right now. But if there is a topic that somebody hasn't written about yet, it’s due by then.

What’s going to happen is Marika and I are going to discuss off-line putting up our master draft together. Marika is really great I must say, at synthesizing material and slotting it in.

Our ultimate goal is to create initial report. That report’s going to get read by the GNSO Council and a lot of other people in the community.

It's therefore important for us to put it into a formatted and do some editing that accurately reflects what we want to say.

But it's also got to be focused and we have to be very careful about drawing attention to our recommendations because that's what we especially want people to pay attention to.

We basically have January to go through that document. That's going to be a time consuming process because we want to make sure it's accurate. We also have to measure our levels of consensus on certain areas and make it - make sure everything's complete and accurate.

So the next couple of weeks are really essential to writing up any material. We're going to have to spend most of January especially concentrating on the recommendations because that's what the council and everyone else is ultimately going to pay attention to.

We have to deliver the final initial report by February 14. That's basically the deadline for all - or I'm sorry, the 12th I think which is a Friday. That's basically the deadline for all kinds of groups to get their materials in so that they can be posted and discussed at the ICANN Kenya meeting. So that's a deadline that the GNSO Council kind of has for us and for all other similar groups.

So I'm going to continue to push I'm getting material written. We're going to have to do a lot of editing but we'll discuss the process a little bit more. And Marika and I will be telling you a little bit more about how we're going to work through that process.

Mikey, I see your hand raised. Do you have a question?

Mikey O'Connor: Yes Greg, this is Mikey. Just my recollection is that we were sort of churning our way through a long list of issues. Have we gotten all the way through that list or are there any of those?

Greg Aaron: We have a couple of issues we have not gotten to yet which is sale of counterfeit goods and false affiliation an unauthorized use of logos. So we have two to go.

Mikey O'Connor: Okay.

Greg Aaron: Those will be on the agenda for next week.

Mikey O'Connor: Okay.

Greg Aaron: Okay so we are at the end of the meeting. Any final thoughts? Any final questions?

Okay. We got through a lot of stuff today. Thanks again to Faisal and Martin, Mikey and Rod who provided our material for discussion today. Thanks again -- much appreciated. And we will reconvene next week for our final meeting of the year.

Mikey O'Connor: Thanks Greg.

Man: Yes, thank you everyone.

Greg Aaron: Thank you everyone.

Man: Thanks Greg. See you.

Greg Aaron: You have a great week. Take care.

Man: Thank you.

Greg Aaron: Bye-bye.

Man: Thank you.

END