

**Transcription ICANN Singapore
GNSO Privacy & Proxy Services Accreditation Issues (PPSAI) WG
Wednesday 11 February 2015**

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.

On page: <http://gns0.icann.org/en/calendar/#feb>

Don Blumenthal: Okay we've got the recording started for working group members who are here - just the usual reminder to update your statements of interest.

We do have some people here who are not on the working group. We rarely get to see each other, so I'd like to just start off with around the table who the working group members are and what brings you here. And also just for our information just if anybody in the audience wants to identify yourself, that would be nice too. Seems good to know who's interested in our process. If we could start with (James).

Woman: Don, we love to refer to privacy rights.

Don Blumenthal: Pardon? I heard the word privacy, which doesn't surprise me.

Woman: (Unintelligible) privacy?

Don Blumenthal: Certainly.

Woman: I'll employ my representative.

James Bladel: Do you want me to start Don?

Don Blumenthal: Yes.

James Bladel: Yes so James Bladel with GoDaddy.

Sara Bockey: Sara Bockey:, GoDaddy. Sara Bockey:, GoDaddy.

Rich Merdinger: Rich Merdinger, GoDaddy.

David Cake: David Cake, Electronic Frontiers Australia.

Holly Raiche: Holly Raiche, ALAC.

Christian Dawson: Christian Dawson, Internet Infrastructure Coalition.

Val Sherman: Val Sherman, Smith, Gambrell, & Russell, IPC.

Frédéric Guillemaut: (Unintelligible) registrars.

Lindsay Hamilton-Reid: Lindsay Hamilton-Reid, 11, registrar.

Ollie Hope: Ollie Hope, HEG, registrar.

Eleanor Bradley: Eleanor Bradley, (Dot UK) and Nominet Registrar Services.

Kathy Kleinman: Kathy Kleinman, Fletcher, Heald & Hildreth and non-commercial.

(Stephanie Coffing): (Stephanie Coffing), NCSG.

(Joan Kerr): (Joan Kerr), (MPOC) and full of curiosity and an open slate for learning.

Kirin Malancharuvil: Kirin Malancharuvil for MarkMonitor Thomson Reuters IPC.

Marika Konings: Marika Konings, ICANN staff.

Ben Butler: Ben Butler, FSAC and GoDaddy.

Don Blumenthal: Don Blumenthal, Chair, FSAC. Completely unaffiliated these days, just kind of hanging out.

Graeme Bunton: Graeme Bunton, registrar, Tucows, and co-vice chair of the working group.

Mary Wong: Mary Wong, ICANN staff.

Darcy Southwell: Darcy Southwell, registrars, domain.com and (Direct I).

Amr Elsadr: Amr Elsadr, non-commercial, (unintelligible), NCUC. And whether I'm a member of this working group is debatable.

Man: (Unintelligible) learning from your posts (unintelligible) center. Law enforcement, in case anyone has any.

Don Blumenthal: If folks in Adobe could identify yourselves while we're doing some logistical stuff.

Woman: We are from (unintelligible) gTLD. We would like to follow some information's from this session.

Man: (Unintelligible) registrar.

(Dominir Alab): I'm (Dominir Alab). I'm a settler from Sudan.

(Dani Andala): (Dani Andala), ICANN staff.

Jacob Williams: Jacob Williams, Interlink or registrar.

Laura Hutchison: Laura Hutchison, Nominet.uk and Nominet Registrar Services.

Sergey Gorbunov: Sergey Gorbunov from RU-Center.

Don Blumenthal: (Unintelligible) introducing invisible people behind the curtain there. Just to let people know, the other co-chair is Steve Metalitz with the Intellectual Property constituency, but he is - and I suspect some other members of the working group are tied up with some of the IANA related sessions.

And second I'll say Alex Deacon from the MPAA just came in, just so we've got a full roster, people know.

Very often we will do something of an open working group session. We're at something of a break point in our work, a logical break point. So I think what we're going to do - I know what we're going to do today - is go through our current progress to refresh ourselves.

Sometimes it's easy to lose sight of what happened before and also to inform the people who are here who are not part of the working group. We really urge say open discussion on anything as it comes up among the working group members but also people who are not members but who have thoughts.

We have from the beginning looked to make this as open a process as we could, in the sense of contributions from people who aren't the working group and contributions from people from different constituencies.

(Dick) joined us after much begging for the enemy to come in to play. But having been on his side of the fence for many, many years doing Internet investigations at least one of us looks at him fondly.

I am going to take a second and bring the slides up because I can't read.

((Crosstalk))

Don Blumenthal: Pardon? Can't read them. That's my problem. So let me bring them up on my
- yeah.

Graeme Bunton: Just while - this is Graeme for the transcript - just while Don's bringing up the
slides, there's a few people in the Adobe Connect that's probably worth
recognizing, putting their names in there. We've got (Susan Prosser) from
DomainTools. We've got (Michael R. Graham) from Expedia and the IPC,
(Kayu Kin), who is an observer, (Todd Williams) from internal broadcasting
and IPC.

I believe there is a dial-in line for those remote that would like to participate.
And if not, you can type questions or comments into the chat and we'll try and
make sure they get into the transcript.

Don Blumenthal: Yes I appreciate your picking up on monitoring the room there. Back to
basics, the whole issue of privacy proxy, what it does or doesn't mean and
how prevalent or not prevalent it is within the domain registration space goes
back a long time.

Issues of accuracy and accessibility and verification, validation have also
been out there a long time, but they've been focused on domain registrations,
the registrants directly.

Over time the pressures to put that kind of scrutiny, that kind of formal
recognition of privacy proxy that existed for registrars grew and just took a
long time. I remember discussions about this when I was still in government,
and I left at the end of 2006.

I was co-author of a letter from the U.S. Federal Trade Commission in 1998
about accuracy of the Whois system. So these issues are ever with us, and

we're still looking at them 17 years later, 16 years, given when we wrote the letter.

Finally, for lack of a better term - without a value judgment - the whole issue of affirmative accreditation of privacy proxy providers became part of the 2013 RAA negotiations. That field is full of issues. We've been at this work a year - a little over a year.

So - and that's just by way of saying if those negotiations had also taken on what we did, they wouldn't be done yet. It would be the RAA of 2015, maybe. So what that agreement did was set up an interim proxy privacy registration accreditation program. But it explicitly provided for the GNSO to set up a group like this, the proxy privacy services accreditation issues, policy development process working group. I actually got that right on the first try.

We have been at work for about - officially - about 15 months now, but I think it's fair to say we really only have been at work for 13 months. We set a very aggressive schedule. We're a little behind, but again we were aggressive, and I think we all are satisfied where we are.

The GNSOs established the working group and gave us a set of issues to look at. It was a massive set of issues - in the 30s I think. We had mid to upper 30s - 37?

So one of the first things we did is we reached out to the various SOs and ACs and constituencies and we broke these down into functional -- as best as we could establish them - categories so that we could tackle a bunch of issues in a somewhat coherent - ICANN and coherent - that's an interesting pair - coherent form.

We've been meeting weekly for that entire time. We've had say these face to face meetings and ICANN sessions and we also were the pilot and I think it

was a very successful pilot. There was a day-long face-to-face session in Los Angeles.

This is good. We can all meet, but it's only an hour and a quarter. And everybody who could make it in one place was very useful. Next slide please. I should probably get into it.

We completed our preliminary recommendations on most of our categories. We looked at mandatory minimum requirements for accreditation. And as you might expect, because many of the issues follow the same track -- same type of track -- we've used the registrar accreditation as a model for much of what we've done.

The core faces fundamentally I think the same sets of issues - proxy privacy provides some additional challenges, largely from an additional stage of separation between the registrant and the registrar.

We've recommended that any terms of service have to be published openly, not just in a -- if there are such things - paper contract. There have to be designated points of contact - an old term in the WhoIs debates for reporting abuse.

We've looked at relay of communications. Yes, there is a request for the underlying registration data. What are the rules if and when that information should be forwarded from proxy privacy provider to the - and I'm going to use the term beneficial registrant?

You know proxy privacy setup I think the proxy really is the registrant. But they're not the party of interest. So again my terminology is beneficial registrants and I'll ignore the legalities. I am a lawyer, but I haven't practiced in over 20 years, so I can ignore things.

One thing we did is the historical term that goes was (relay as reveal). Pass along the information but when do you take away the cloak? But in our discussions we realized "reveal" is really two different things. Are you telling the requester directly? That's kind of reveal. But the other kind is posting the registration information in the open.

So we chose to break reveal into disclose (unintelligible). Here's who the beneficial registrant is. (Unintelligible). Put the information out there. And we've also looked at the accreditation. What happens if and credited registrar -- proxy privacy provider, sorry - either breaks the rules or decides just we don't want to do this any more?

Next slide? We do - these are the, I think, broad areas that are of most interest in what we have come to some levels of agreement. We do have some issues where there isn't a consensus yet. You know, the appropriate standard for being able to contact a proxy privacy and what the rules are for responding to enquiries, an escalation process when relay requests are passed along but get some level of delivery failure.

We get a lot of discussions on formal e-mail server definitions and protocol responses. So it's (kind of) interesting. (Unintelligible) went back to my days as an e-mail systems administrator.

Issues of disclosure, how to deal with requests for disclosure from for example law enforcement or third parties. I think the most common example that people would think of is say intellectual property representatives because those are the ones that make the headlines.

But another example is private organizations do bring suit to stop botnets just the way law enforcement will bring enforcement actions to deal with botnets. Microsoft is one. (Unintelligible), but others have done that.

Next slide? We're looking at the different standards for - and this is just expanding on what I just talked about - different standards for maintaining the point of contact. And we have looked out to other ongoing ICANN processes to assist us, not just the registrar accreditation agreement.

The IRTP - what's the I stand for James? Inter, inter - inter-registrar, thank you. Transfer process - has informed us, but we haven't come to conclusions. How responsive should the provider be? Again we're looking to the RAA to inform us, the standard be for ensuring provider the ability to contact a provider.

You know, for example, publishing on the Web site which again is modeled after the RAA, but it still has some tweaking to do to address differences that may occur in a proxy provider space. You know other - well, I'll get to that later. Next slide?

We're looking at - again I mentioned relay requests and what happens when there is no response. Now we're very careful to say that there may not be a response because the beneficial registrants chooses not to.

There may not be a response for other reasons, but we wanted to really focus on where the - here's where we're getting back to some old Whois issues - where the information that the proxy privacy (unintelligible) has about the registrant may be inaccurate.

Where the beneficial registrant may have affirmatively chosen to duck (unintelligible) to be scarce, not to be contactable at all, as opposed to just looking and ignoring. And we really focused on looking at where we know or where the proxy privacy providers should know that something's wrong with the contact information, whether it's inadvertent, which is still going to be - you know, there's going to be a responsibility to keep it accurate.

And whether inadvertent or just somebody's gone offline but held on to the domain. So something we're still looking on and it's what is an affirmative failure to respond? What do you need, what does the provider need to see in the way of return traffic? Most of the system's e-mail notification.

To say okay there is a real problem here as opposed to the beneficial registrant just ignoring. You know, how much can the proxy privacy do about that as opposed to just knowing there's an affirmative problem?

And again this would suggest up here - you know, the trigger for escalation isn't failure itself, but the provider's awareness that there's a problem. And we were still looking at the minimum mandatory - too many M's - minimum mandatory requirements for escalation of relay where there's a persistent (unintelligible) distant delivery - non-delivery.

And I can go into examples of the messages you might see if the message bounces, but you've all seen them so I won't bother.

You know, these are examples of the language under consideration. I'm not going to read them but what does the provider - if e-mail fails, what other affirmative forms should the provider take? You know, print out a copy and send it? Go knock on a door if it's - you know, whatever. Is this e-mail the only measure that has to be taken?

Issues of must versus should. This is the kind of thing we're tweaking. Must a provider take additional action or is it an option? How much does the provider have the choice of how to forward a relay? And is there an ability to charge for it, charge the requester? And if so, who takes the burden of the cost?

And if there should be any limits on those costs? There should be limits on the number of requests by the same requester because sometimes it's just stuff - historically it's harassment - registrars over proxy privacy - and we're aware of that. The dividing lines are very difficult to come up with.

Next. This has been an issue that - for what it's worth - I expected to be much more contentious. And I'm not saying it's not, but we came up to some groupings fairly quickly that we don't have a consensus on. But I think it's fair to say the discussion focused on fundamentally whether proxy privacy registration should be available to all or should they be limited? And if so, who should be ineligible?

Now, over history it's been easy - well commercial, non-commercial. Well, try to define those. Kathy and others had the discussions for over ten years - not directly but I remember talking to her about them in context from law enforcement to consulting to PIR and beyond.

And one of the persisting questions was why does a registrant really need to be public? The easy thing was commercial and well - okay, what does commercial mean? But beyond that - contrary to I think a lot of perceptions - there are legitimate commercial reasons for proxy privacy.

The best example I think came to us through our IPC members who suggested that during product development there may be a domain out there to facilitate a new product's use, whether it's e-mail or a Web site or whatever. But before the product's released, the company doesn't want to know who's behind it.

So we kind of focused in on okay, it's only a company that's actually doing financial transactions online should be reachable directly and not through privacy proxy. We're still struggling on how to define that. We're still struggling on whether there should be this kind of distinction. But we focused on that type of distinction fairly quickly, so...

And now where we are I think is working out if we have a consensus on either and how to define one of our options. And I think we're focusing in on again transactional versus non-transactional. Pardon?

Woman: (Unintelligible)

Don Blumenthal: Generally, no. This is as it says on the slide, "Working Group Chair Suggestion," not accepted across the board by any means. Next?

And how to deal with third party requests? And this is where I said we're at a logical break point. The representatives in the registrar community and the intellectual property community have very - I think it's fair to say - distinct - Graeme's reaction there might suggest - there are distinct differences of opinion.

A couple of months ago some members of those two constituencies broke out on their own to focus because they've got the clearest view. And it was going to be - it's very involved. I think it's fair to say they are coming close to the point where the working group will be able to look at a document - and what form is unclear, not established.

But at least where the process will finish, and then the working group will focus on the work of that subgroup. I think once we have finished that we'll have our final draft. We'll have a complete draft.

The group will go back over and look at it, but I think the final steps are including that information, having the working group discuss it, doing a relatively short term review of the whole document and getting a draft out for public comment.

Man: I'm sorry - if I could just get a clarification. You said we'll be ready with our final draft. Do you mean our final draft of our initial report?

Don Blumenthal: I apologize. Sometimes people point out to me I get sloppy with terminology.

Man: Okay, thank you.

Don Blumenthal: Yes, we will be getting to the point we will be reviewing our final draft and then publishing an interim report. Okay, got to write that down. To me the - pardon?

Man: Which some day will then lead to our final draft of our final report.

Don Blumenthal: Some day.

Man: My process here. I'm just...

Don Blumenthal: Well I think I just jumped to the next - we hope to have our interim more published and be in a position to have completed the public comment period before we get to Buenos Aires, yes.

That said, I think I rambled a bit more than I wanted to, but people who know me know that's not uncommon. At this point - and I saw one reaction to something I said.

Woman: Yes?

Don Blumenthal: So I'm going to start - I saw one. There may have been other more subtle ones. I'd like to open it to the working group to make comments, general comments, on things as I represented them.

Man: Why don't we go back to the questions as we've got them in the slides.

Don Blumenthal: Just one by one?

Man: Yes.

Don Blumenthal: Okay, here?

Man: Yes.

Don Blumenthal: Here. Okay, here's the overall slide and where we're still working on or looking for working group consensus if at all possible.

And you know I think maybe I'd like to - because I'm kind of free form in my approach at times - I only saw reaction on one. So rather than go through and just get blank stares, like the ones that happen on phone calls sometimes, I'd like to do an - this is a reminder but I'd like to have people jump in where you think we need to talk more or I need to be corrected in what I said or whichever. I'll turn my red light off and let other people light theirs.

(Steven): This is (Steven) (Unintelligible). I have two questions about it.

Don Blumenthal: If you could identify yourself for the transcript please.

(Steven): Yeah I'm (Steven) (Unintelligible). Two questions about two of the cases, two of the outstanding questions you still have. One of them is the contactability issue. (Unintelligible) comfort in a new RAA where it says that the e-mail verification, if the registered name (holders) for the account holder is non-contactable we should start verification. And if it fails, suspend the domain name.

If the account holder in the end, the person has really paid for the (name) and he's behind the privacy proxy services...

Don Blumenthal: Okay I want to jump in quickly. Okay, no, let me let go.

Man: (Unintelligible), key systems. Yes, in many cases the account holder would be the one that also domain name. However, we are looking at cases also where privacy services may not be affiliated with the registrar directly, maybe provided by a reseller, by a completely unrelated third party.

In that case, the registrar would simply not know who is the underlying registrant and therefore the privacy proxy provider would have a corresponding obligation to verify his customer. The (guest) registrar would only be able to verify the privacy proxy service provider and not the underlying registrant.

(Steven): Okay clear. A second question about the transactional remains. Who should define which domain - whether a domain is transactional, yes or no? Is that the provider of service? Or is that the registrant himself?

Holly Raiche: We've had a lot of discussion about that one. I'm just a little bit surprised by the word transactional. I think the majority of us around the table in the committee realize distinguishing between commercial and non-commercial was just so difficult and indeed there are many legitimate reasons in the commercial sphere why someone would want a domain name.

It just became very difficult to - A, work out a different - and I'm not sure the transactional gets there anyway. But B, does it matter? And it was hard to figure out does it matter.

So we've had a lot of discussion. This is a recently new term, but I think it reflects the long discussions we've had - not only what's the definition of transactional/non-transactional -- or more familiar to us - commercial/non-commercial.

And then if you can actually agree on a definition, does it matter? I think the majority of us have said it doesn't matter, but it's still on this table I think.

Don Blumenthal: Kirin you came to mind when I heard the word majority, so I'll just pass it to you.

Kirin Malancharuvil: Thanks Don. This is Kirin from MarkMonitor. You are pressing it with your introduction of my comments. I do take offense to the term "majority," and I

think that that's something that we've also had long discussions about. So let's please be careful with terminology because there's been a lot of concern in the community this week about misrepresentation and I think that's probably something.

So let's put that on the record. The majority (unintelligible) have not said that. And the majority of stakeholder groups represented in this organization have not said that. It's an ongoing discussion. It's a complicated one.

I think the majority of people have acknowledged that it's a complicated question and that there's a lot more left to discuss about it. But let's not make any determined statements here about what we've determined one way or the other. Thanks.

Kathy Kleinman: But what we can say for certain is there's no consensus -- Kathy Kleinman, non-commercial - that there's no consensus. I'm moving towards a change on this. We're deep diving into what ultimately is content review, what's going on on that Web site?

We haven't - if we go down this path, the fights we will have over what is transactional, which is ambiguous - I don't think we've even begun (unintelligible) where we're going on this.

I run a non-profit, and you can give me money, but you're doing it through another organization. A lot of small businesses, medium-sized businesses, non-profits aren't taking the money themselves. They're going through third parties and other Web sites that may or not be apparent. We could spend another three years on this, guys.

I just wanted to share that (Stefan) - is it (Wetzel)? -- from Dot...

Man: (Dot DE).

Kathy Kleinman: (Dot DE) - got up and he was talking about this in I think the public forum but one of the big sessions where he said, you know, "Think carefully about transactional, guys. We have laws in my country," he said, "That require you to identify on your Web site if you're transactional if you're a certain type of commercial. You know, pass those laws in your countries. Leave the domain name system out of this." So I just share that because it was so relevant and it was just two days ago. Thank you.

Don Blumenthal: Which forum was this?

Woman: (Unintelligible).

Man: In your mic if you're going to talk.

Woman: Kathy, I think that was that "All Things Whols." I think so because (unintelligible) the segment.

Kathy Kleinman: Okay, thank you. All the big fish (unintelligible).

James Bladel: Also briefly - James Bladel speaking for the transcript - and that's something that (Volker) I think has informed us of many times. And I think that gets to some of the principled and practical problems associated - or complexities associated - with this issue - I mean determining whether or not domain name is being used or let's say domain name is associated with a Web site and then the Web site is associated with transactions.

So it's a couple of steps removed and then there are other intermediary mechanisms I think as Kathy and Holly were alluding to.

I think that it really boils down to is this even something possible to do? You know, if we want to set aside the principles and the theoretical and the hypotheticals and just say how do you know? Where's the bright line? And then what do you do?

And I think if you can't answer those questions - if we can't come together around some answers for those questions, then you know I think that it's pretty clear that this is a non-starter and we should be careful before we dive in.

We can spend three years on this. The temporary provision sunsets in 2017 - just a reminder - so we do have a ticking clock. We don't have three years, but it's something that we should say, you know, is this something that we want to break our pick on trying to solve? Thanks.

Kirin Malancharuvil: Thanks (Volker). Kirin Malancharuvil from Mark Monitor. I think that first of all since we started this in 2014 and this sunset is 2017, I think that's exactly (unintelligible). So I do think we have that time, and I think that if it's an important issue we should take that time.

What I really raised my hand to say though is that I think it's actually a fairly dishonest characterization to continue to say that we don't deal in content examination all the time in the policy-making process at ICANN and in the issues that we confront certainly as far as IP owners and registrars interact.

We look at content all the time. When you determine whether or not a domain name is abusive, you're not just looking at whether or not the trademark is being used in the domain name itself. But often you're looking at the content of the Web site itself to see if it's free speech, to see if it's protected, to see indeed if it's a commercial use, which would maybe be dispositive on something like whether or not it would be considered parody.

So I think we need to step back because it's a very compelling argument to say that we don't want to get into content examination and we don't want to get into what the Web site is actually going to be used to. But we've been doing it for years.

It's important and it's actually a dispositive examination and a lot of things that we look at when we are determining abuse online. So, you know, yes it is a complicated issue. Said that twice just this morning. And it will take us a long time to get to a conclusion on this that's fair and representative of all views.

But, you know, it's not as if we haven't done this before. And it's not as if it isn't an important issue. Thanks.

Man: Yes I would agree with Kirin that a lot of the problems that third parties and especially rights holders have are not with the domain name itself but with the content it leads to. However content is -- at least at last time I looked - not part of the (remit) of ICANN is hosting, that content is hosting.

Most domain registrars - some do, some don't - do not have even the hosting under them and the privacy proxy services most certainly don't. So I'm somewhat certain if in the end we will have firm policies for the privacy proxy services that will deal with what is essentially not part of ICANN's (remit) and may rely on best practice recommendations in this case instead of firm policy.

Christian Dawson: I wanted to dovetail on what James was...I'm sorry?

Woman: You have to identify.

Christian Dawson: Oh I'm sorry - Christian Dawson with the Internet Infrastructure Coalition - ISPCP. I wanted to dovetail on what James was saying because I think that we're talking about potentially building a big machine to address this. We would have to look into arbitration processes, how we're going to do what we're going to do, how we're going to monitor content.

And I come from the Web hosting arena. And one of the things that I really like about that space is you can start a Web hosting company in your basement. There are things that are really - innovation comes on the Internet

because there are lots of small businesses that are driving that innovation, that can do some exciting things. You don't need to be a huge company to get started.

And I'm always very - I ask the question whenever we get into a system where you're going to need to have layers and layers and layers of identification processes, make it so that it really requires a lot to get started. You can't start with a small organization and get going. I ask toward what end?

We have to take a look at what it is we are achieving, what it is we think we can achieve if we build this big machine. And I don't think we've answered that question either. Can we do it is one question. But if we take the process of ratcheting up the bar as to what it takes to be able to offer this service and do it that way, what are we achieving at the end of the day?

Don Blumenthal: Thank you Christian. I have James in the queue.

James Bladel: Yes so just quickly, I'm not really clear on who was being dishonest by saying that ICANN's remit does not include content. Content is hosting. There are no hosting constituencies. I mean ISPC's kind of close, Christian, but not exactly there. I think that we do review content as a matter of our overall portfolio of services.

And our terms of service give us actually broader latitude to deal with content issues than we would see under ICANN policy. So it's actually - we prefer it when we have a problem that's hosting because we can kill it. It's not always true when we're simply providing registration services for other content providers.

And, you know, and I think that this continual confusion of those two issues or blurring of that line is - you know, it's something that comes up quite a bit at ICANN. It was in our discussion earlier in the GAC session about the

sensitive strings and safeguards and how that might apply to content that might be used for some prospective TLD someday. And it comes up with a lot of misguided or misconstrued complaints filed under Section 3.18 of the RAA.

So, you know, content is something that I think - it's what we all came to talk about but unfortunately it's slightly outside of the tent of what ICANN can do. The service providers here I think have voluntarily waded into this area under their own terms of service, but it's not under the umbrella of consensus policy, not within the picket fence I think as our friend (Jeff Newman) might say.

Don Blumenthal: Thanks James. Do we have anyone else in the queue? David Cake. State your name.

David Cake: I said something similar to this in the opening Whols section. This is one of these things where ultimately we're asking the question of - a question that depends on us knowing the use of the Web site and the content at the time of registration or, you know, in a sense. And we can't ever actually do that, like know that reliably.

What we should instead be asking is there a way should transactional use change how we deal with reveal and things like that perhaps would be a better...

I don't think we will ever answer this question because we're asking the wrong question. We're saying - because we're depending on knowing the future essentially which (unintelligible) knowing what content is on the site at time of registration. And you can't.

Woman: Maybe let's back up and say if we agree - which clearly is still under discussion - to make a distinction between whether you call it corporate/non-corporate, transactional/non-transactional, what implication would that have on the way we operate?

And maybe the way through this is to say does this distinction flow through to everything else that has been decided or will be decided around the table?
And maybe that's an easier way to deal with this issue. Thanks.

Don Blumenthal: Stephanie.

Stephanie Perrin: Stephanie Perrin for the record. Excuse my ignorance if I'm not up to date on all the research that's been done on this issue because I'm finding it hard to navigate the new site and find things.

But I'm looking for research that demonstrates that the ISP route to take-down for crime - I mean, oddly enough I'm actually - as a privacy advocate - very much against crime you know. We're not trying to put anyone out of business here, except criminals.

Where's the proof that the ISP route doesn't work? I had this discussion with Don the other night, and he assured me that domain name information was useful, indeed mandatory, for investigating crime. But I'm not convinced that we need a distinction on commercial/non-commercial for these matters.

There's so much other avenues if you have a serious matter that you get at the ISP. Why does ICANN have to step into regulation of financial services or non-financial? I mean really, that is so deeply into content that we can't go back.

I mean, some of us argue that we're deeper already into content than we should be at ICANN. But I can at least understand the intellectual property trademark argument surrounding the use of words in domain names. I cannot the minute you start looking at what's happening on the Web site.

To me that's a pretty clear demarcation line. And the fact that we're having a problem with the bright line, I don't get it. So if you can show me the research I'm anxious to learn. Thanks.

Don Blumenthal: Okay I think we've got - oh, sorry about that, I think. I'm going to go slowly because we are trying to re-establish audio in Adobe. I just want to suggest one thing. What I said yesterday was not that domain names - was just that there have been some statements flying that law enforcement or the privacy community - private party community - does not use domain name information.

My suggestion was that that is not true. It's not always used. Frankly, when I was doing cases it was rarely used except as a research tool, not to bring a case. But it was more just clarifying some inaccurate statements that are very common out there about the use of domain registration information.

I'm going - I'd like to just finish the queue as it stands now and then at least take a break to see if...

((Laughter))

Don Blumenthal: Oh.

Man: We've got five down the middle.

Don Blumenthal: And Kirin yes, thanks. And then at least see if we want to talk about anything else, but this kind of helps explain there are some areas where we really need to take the time, and also just to guess that people are not in the working group don't hesitate to contribute. We talk every week.

Kirin Malancharuvil: I have a couple of comments. I had my hand up initially to respond to the gentleman - I'm sorry, I don't know your name.

Christian Dawson: Christian Dawson.

Kirin Malancharuvil: Christian, Mr. Dawson. So your comment about what we're trying to accomplish with this provision, I don't know how involved you were in the group when this issue first was presented, but the proponents of this provision actually submitted a white paper to this group in which we - I believe quite neatly outlined the goals of the proposal.

So if you want to examine what we're trying to accomplish it actually boils down quite simply to one thing, which is to achieve contactability of somebody engaging in transactional activities online similar to or at least along the same lines as that which is standard in most international jurisdictions in a brick and mortar world.

So for example you have to display a business license if you're selling goods and services. And you have to register your information with perhaps the Chamber of Commerce as one example. So I think it boils down to that, but there's a lot of actually really good information in that white paper.

Now whether or not you agree with that white paper - the conclusions of that white paper - and sign onto it is another issue entirely. But if you're asking the question what it is that we're trying to accomplish, I think the answer is contained therein.

Before you respond, I just would like to say - my other point which I'm in the queue for, and that is like Stephanie I'm really excited about the question that you're asking about why the ISP route is inadequate because MarkMonitor actually is sitting on just a mountain and a wealth of data about that issue.

We do - what - thousands probably of abuse complaints daily I think probably. How can it be that I'm too quiet? I'll get closer. So we're sitting on a wealth of information about that actually and I think that the numbers are really quite poor.

When we talk about the ISPs that are present here at ICANN or in the room, I think we probably have great compliance rates with those people, those that are super cooperative because they're here, they're participating, whatever.

But overall I think that when we go the ISP route for compliance with abuse complaints that are kind of all over the map, we've got something like a 20% compliance rate with ISPs - 20%. Something around that - no bigger than 30.

So I'm happy to actually pull that data and provide it from - you know, I would have to anonymize it, but the ISP route is completely inadequate. And flight from one ISP to another is a huge problem - registrant flight. And there are lots of sympathetic ISPs in countries in which they're just plain unreachable - lots of ISP safe harbors.

So I hope to be able to give you the numbers that support that argument, but rest assured we would love to have an ISP route to address these issues. And it's just, it's not happening for us or our clients, and we have a pretty large portfolio of data to support that. Thanks.

Christian Dawson: May I respond? Christian Dawson. Thank you. I appreciate it, and I will get out of queue then after I do. I don't need to give my comments, incorporate them. Kirin, I very much appreciate your comments. I actually was in the group when that came out and I do understand, have reviewed the white paper that was put together.

And when I was talking about to what end ultimately I was talking about the idea that - I understand that the goal is contactability. Coming from the ISP and hosting background, I am part of the system that (Susanne) was discussing wherein I am responding - my team is responding - on a constant basis to law enforcement (requests) for information, and we're part of the process.

Hopefully what you're identifying is the 20% good actors in that system in order to make sure that bad stuff doesn't happen online. I would love to see that data that you're talking about. That would be extremely useful in trying to figure out whether - the scope of the issue -- because sitting where I'm sitting, I'm seeing effective tools, good actors with a whole bunch of hosting and cloud providers with ISPs what are actively engaged and willing to solve problems.

And I don't see - for the most part - that the people that aren't doing that are staying in business for very long. Now there's certainly a black market but what I'm trying - or a whole bunch of bad actors in certain parts of the system and there always will be.

My question when I said "to what end" is can we create a system that's so ironclad that it can't be - that you're going to be able to avoid that - well, ultimately we're going to have somebody check a box. And a bad actor, are they going to check the right box? Can we guarantee?

So we're going to build this whole system and will it be any more effective to raise your numbers or will it just create levels of bureaucracy? I don't know the answer to that, but it's something that I think we need to consider as we move forward and try to add these layers. That's all.

Don Blumenthal: (Unintelligible) still get some other business in.

(Fulker Climont): (Fulker Climont) speaking for the record - just three small points. This is something that - the first one to something that Stephanie said. We had a very productive session with the registrars I must say. They had a very productive session with law enforcement earlier this week. Very helpful, very interesting to find out what their needs were.

However, one answer to a question that I posed was a bit disconcerting. When we asked them if they could provide any examples or data or statistics

or anything of how or if at all the changes in the RAA that they demanded originally that were intended to enable them to better go after crime on the Internet had any effect, they weren't able to provide anything, any example - not a single one. And I found that a bit disappointing.

And the other point - maybe we just do something - like Kirin said - maybe we just need an ICANN for hosting them, an organization that deals with hosting companies, just as ICANN deals with domain name registration companies. Maybe that would be a solution.

They have policies there that work all over the world. It may be a jurisdictional problem. There may be an enforcement problem, but maybe that's what it needs.

Kathy Kleinman: Kathy Kleinman, two quick points. One is if we're reopening this, please let me know so I can book my Tuesdays at 10:00 a.m. Eastern for the next three years. I didn't think we were going back down this. I really thought we were going into a final report.

And we had really talked about this for months and months. But one thing I'd like since we are here, we're hearing - there are a lot of people here who we haven't heard from. Love to know (unintelligible) public. Please come to the table. There are open mics.

Let us know what you're thinking because that's one of the reasons we're here. We know you're hearing voices and concerns and issues that we've been voicing now for months. So come to the table. Share with us what you're thinking. We'd appreciate it.

Don Blumenthal: Let's (unintelligible).

Woman: We need to...

Don Blumenthal: Anybody else who thought you were in the queue when I said we'll cut the queue - in the line that we talked about?

Man: I think Holly was.

Don Blumenthal: Okay. Are you still in the queue? Then you're not out of the queue. You're ready to talk.

Holly Raiche: A couple of things, Kirin. I think the real concern you have is contactability, and maybe that's where we should actually focus. And to Kathy, I don't really want to spend the next three years getting up at 2 o'clock in the morning.

Kathy Kleinman: We appreciate that you've done it so far. It's amazing.

Don Blumenthal: And there's a limit on how much we're going to change our meeting time to accommodate various times of our membership. But I appreciate you and David and other people who do suffer with - so it's a U.S. dominated time system.

David Cake: It's a little kinder for me on the other side of the country.

Don Blumenthal: Okay, I would like to move on a bit here. We've really focused on some issues very heavily. To be honest I think we did hear some new things here. And at least this issue of commercial/non-commercial, transactional/non-transactional we discussed a few months ago, but again I think we did hear some new things here so I'm glad we had the discussion even though it went a little bit long.

I'd like to throw it open to other issues that people want to discuss. And again as I said and Kathy said, if you're not part of this group formally, I assume that you're here for a reason. You have an interest, so we'd like to hear your thoughts on what we've talked about here or things we have not addressed. Please come up to the table. We have a - I guess - roving mic. That

(unintelligible) there, but we can get it again. Get involved in the discussion.
And identify yourself please.

(Lucy): Sure. My name is (Lucy). I'm from (Dot NZ). I think - and picking up on your point - and I guess it is going back a little bit - I came because I'm interested in just looking at privacy proxy.

And I partly come from the distinctive of having a few girlfriends who when GamerGate was going on last year was sort of really concerned that the contact data from the domain name registry was really the only one public registry that people could find out information about them and lead to them being docked or whatever else.

And they don't have Web sites. They just maintain a domain name that fits (unintelligible). And I think in that context we're a long way away from trade. And we're also dealing with private individuals and there's no sort of clear opt-out (regime) other than maybe finding some company or person that knows them to forward the information to them.

So I think when I was listening to this discussion I came from that job as thinking someone who doesn't have a Web site at all. And so you might not even be looking at content of those e-mails.

And looking at the commercial and non-commercial and transactional versus non-transactional, I think what was so - if you do either look to go further down that path you'll need to be very mindful of your local jurisdictional laws because the trades legislation in New Zealand, for example, a lot of the anti-trust laws all have definitions of what counts as in-trade for misleading and deceptive content. And it could be quite confusing from a compliance distinctive to (unintelligible) your definitions that don't align with those.

So I don't know if that's at all helpful but just from somebody who's not on the working group, those were some of my thoughts.

Don Blumenthal: I particularly appreciate your bringing that issue up of e-mail existence only. It's a point that's too often lost in Internet discussions. Internet does not equal worldwide Web. And I'm somebody who's only had an e-mail presence on the Internet for about four years now.

That's changing. Got to get my advertising out, but for the last four years again it's just been two e-mail addresses.

Terms get kicked around, so just to make sure everybody knows the background here, could you define GamerGate? Because it's one that's still not in general knowledge I don't think. I only figured it out about a week ago.

(Lucy): I don't know how to necessarily define it.

Man: I'd be happy to just take a stab at it if you'd rather.

(Lucy): You just jump in there.

Man: GamerGate was a large online controversy which while it was basically a culture war within computer game journalism essentially was how it started. But it basically ended up as a campaign of harassment against prominent women in the games development and games journalism spaces and has been associated with a lot of very significant incidents of harassment such as grotesque death threats and so on, bomb threats, and things like that.

So while it may seem a stupid issue in that it's about - you know, claims to be a video games journalism - the real thing is it's an example of an online controversy that has become a really significant issue - harassment issue.

And one of the things we do need to learn and inform our discussion is that, you know, obscure as, you know, Whols may be to many people, it absolutely is well known and understood by a lot of - essentially organized harassment

campaigns and such things like that. We can't underestimate the extent to which it will be used.

Don Blumenthal: Appreciate it.

Man: Is it okay for me to build on that one more second? Because I would like to describe also that one of the concepts that - it's a terminology that's been referred to as doxing.

Man: Yes, doxing is a thing that comes from outside the - it didn't originate with GamerGate though. They've certainly made a lot of use of it. And it's used by a lot of the sort of Anonymous campaigns.

Doxing is essentially destroying privacy as a political weapon, as a weapon. So it's the idea that to harass someone, you publicize all of their contact information, including physical addresses and home phone numbers.

And the joy of it is you don't even need to do anything. You can just go, "Oh, and this person, here's all their contact details. I'm not suggesting you should use it to ring up and harass them, but if you were, there it is."

So it is important to use that - destroying privacy is used as a deliberate or campaign of organized attacking on people as part of - I mean GamerGate is just one example. So...

Man: And the one thing that I'll say is that somebody who is running a transactional Web site can still be a target of...

Man: Oh absolutely. I mean a lot of the women in the GamerGate controversy - and it's not just women (unintelligible) but mostly - were people who were definitely running - you know, they were involved commercially in the space, but often on a relatively small scale. We're talking like donations and that sort of things.

We were not - donations of things like (petreon) or selling games for very little, that are essentially at a very small price. These are not - that gap between transactional and not could be, you know, small.

Ben Butler:

Ben Butler for the record. I wanted to - without regressing the meeting back to points that people wanted to leave behind - as a non-member of this party but a very interested party in the discussion, I wanted to give an example of exactly where this line between the domain name and the content is a dangerous argument to try and make because that is not the only two sides of this particular coin.

I was asked to consult on an abusive issue a few weeks ago. The domain name portfolio in question was several hundred domain names that were derivatives of legitimate online businesses. They were being used in e-mail only based phishing campaigns. They were all using privacy and proxy services.

The brand holders, the trademark holders if you want to call them that, had no idea how to contact who was responsible, other than the privacy and proxy service provider. And there is no content. This is not a situation where as a registrar we could say go talk to the hosting provider. You're going to have to figure out as a registrar and as a privacy and proxy provider how you're going to respond to those issues.

So don't just pigeon hole yourself into saying it's a content issue or it's not a content issue. The domain names can be used in all sorts of ways for abusive purposes that have nothing at all to do with the site content. And you're going to have law enforcement and IP holders coming to you wanting you to solve this problem.

Man:

Just another comment I'd like to make while we're on the subject. People who are involved in organized, you know, doxing and harassment campaigns

understand social engineering. So when we talk about things like reveal in reveal a copyright complaint or something like that, they will misrepresent themselves as copyright holders quite cheerfully. So we need to - those processes need to be strong.

Don Blumenthal: We've just got a couple of minutes. I'd like to see if there's any other issues people want to hit.

Woman: (Unintelligible)

Don Blumenthal: Okay.

Kirin Malancharuvil: You gave them lots of time (unintelligible).

Don Blumenthal: (Unintelligible).

Kirin Malancharuvil: Okay, please don't because it won't go anywhere. So the issue - nobody thinks that this issue is dispositive. For the entire contactability issue on privacy proxy, nobody says that putting this distinction in is going to allow us to get every criminal that's hiding behind a privacy proxy shield.

This is one issue of many, and yes there are lots of things to talk about. Whether or not donations should be included is one thing to talk about. But the presentation of the difficulties surrounding this issue is not enough of a - is not - it's not convincing enough to a large number of us to throw out the issue entirely.

All we're saying at this point is that there is more discussion that needs to be done, and the baby should not be thrown out with the bath water just because we've identified a number of issues that need to be solved. I have absolutely no idea what anyone was talking about with GamerGate. So if we want to take that to the list, I would appreciate somebody explaining to me how that has anything to do with the issue that we were talking about. Thank you.

Man: We're at 10:45.

Don Blumenthal: Yes, yes. Yes, let's take that to the list. Reserve comment. Stephanie, and that will be it for the meeting.

Stephanie Perrin: Yes and I'd be very happy - Stephanie Perrin for the record - just to contribute a recent report from the Council of Europe. I'll send it to the list. I'm not the lawyer. I'd really appreciate what you have to say about it. (Dewey Coff) - and I apologize for massacring the Dutch name - wrote it from the rule of law as applied.

And my only comment would be - and I've been sort of yelling about due process since I got here - and this paper examines it in some depth. The more we go into being a law enforcement facilitation mechanism at ICANN, the more we raise fundamental questions on how far we've strayed into private sector policing.

And that's where you get into these very fundamental human rights issues. I'm not here to defend crooks and GamerGate harassers. But you have to be clear about the mechanisms that we are employing to break these things. So I invite you to read the paper. And if it's a crumby one please tell me because it sure looks good to me.

Don Blumenthal: Thanks for your attendance and interest and time. The working group's going to take a break for the usual post-ICANN break for a week and we'll be back at it - whatever two weeks from Tuesday is. Thanks.

END