Transcription ICANN London
GNSO Privacy & Proxy Services Accreditation Issues Working Group
Wednesday 25 June 2014

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://gnso.icann.org/en/calendar/#jun
The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page

Don Blumenthal: Good morning. Let's get started. A little bit delayed because we had back to back meetings in here. I expect there'll be a few more people filtering in because they told me they would be late. They say this is not the easiest hotel, necessarily, to get from one room to another; just a little bit spread out.

Okay, we're going to just do introductions. Probably because some of the people in the room who are on the committee have not met each other but also so that people who are not involved in the back here will know who we are. Decide later if that's a good idea or not but hey, we took the job.

After that we'll kind of summarize where we are in the process, open it up for kind of focused discussion on some of the subject areas that we discussed already but then leave time for open topics either from the group here or I think most importantly from people who are not on the committee so we can get a chance to get questions in here or views because we really don't have a public forum time - a formal way to submit commits accept at the meetings once the process gets rolling.

So with all that out of the way why don't we start just going around the table, introduce yourselves, who you're with whether it's constituency, company, both and then we'll get into the substance - that's the word, substance. It's going to be a long day for me, I'm warning you.

Start over here.

Man: (Unintelligible) Power Internet Group, Registrar.

Chris Pelling: Chris Pelling, NetEarth One, Registrar.

Roy Balleste: Roy Balleste, St. Thomas University, NCUC.

Man: (Unintelligible) Registrar.

Tatyana Khramtsova: Tatyana Khramtsova from RU-Center. Registrar.

Christian Dawson: Christian Dawson, Internet Infrastructure Coalition, ISPCP.

Osvaldo Novoa: Osvaldo Novoa, ISPCP.

Mary Wong: Mary Wong, ICANN staff.

Phil Morano: Phil Morano, Katten Muchin Rosenman, IPC.

Steve Metalitz: There we go. Steve Metalitz representing the Coalition for Online Accountability, IPC.

Don Blumenthal: Don Blumenthal with the Public Interest Registry ostensibly representing the stakeholder group but that only means I'm the only person here from the group.

Graeme Bunton: Graeme Bunton, I'm from Tucows. We're a registrar. Also myself and Steve are the co vice chairs and Don beside me is the chair. And there's a couple more seats at the table if people standing in the back want to join us.

Benet Garcia: Benet Garcia, Hibu. Reseller.

Marika Konings: Marika Konings, ICANN staff.

James Bladel: James Bladel, Go Daddy.

Holly Raiche: Holly Raiche, ALAC.

Volker Greimann: Volker Greimann, Key Systems.

Darcy Southwell: Darcy Southwell, Domain.com.

Alex Deacon: Alex Deacon, Motion Picture Association.

Griffin Barnett: Griffin Barnett, Silverberg, Goldman & Bikoff, IPC.

Don Blumenthal: Members in the back. Okay if not - if people are interested if we could pass the mic around for introductions just so we get an idea of who's interested in what we're doing.

Lindsay Hamilton-Reid: Lindsay Hamilton-Reid, 1&1.

Man: (Unintelligible), NGO.

(Judy): (Judy) (unintelligible).

Man: (Unintelligible).

Woman: (Unintelligible), Nominet.

(Tony Bowman): (Tony Bowman), Nominet.

Man: (Unintelligible) University of South Hampton.

Man: (Unintelligible) German Civil Liberties Union.

(Guillomo): (Guillomo) (unintelligible) Interpol.

(Chris Parsons): (Chris Parsons) for (Pervetera).

(Tim McArthur): (Tim McArthur) for CIRA, dotCN registry.

(Kelly Saulter): (Kelly Saulter), (unintelligible) group, registrar.

(Jeff Wilson): (Jeff Wilson) (unintelligible) Group.

(Luke Edwards): (Luke Edwards), also (unintelligible) Group.

(Gary Potts): (Gary Potts), (unintelligible).

(Mark Noetz): (Mark Noetz), data provider.

Man: (Unintelligible).

(Thomas O'Toole): (Thomas O'Toole), Bloomberg (B&A).

Woman: (Unintelligible), ICANN.

Woman: (Unintelligible) Publisher's Association.

Man: (Unintelligible).

Fred Feldman: Fred Feldman, Thompson Reuters.

Don Blumenthal: Appreciate it. Nice crowd section. I made a pitch at a meeting the other day and was glad - good to see one person took me up on it about coming to the session.

Generally - is there any way we could blow that up? Good point, all I have to do is log into Adobe Connect. Well I'll give the intro I was going to do here.

Generally we are nicely - never mind, I'll just cover it. Oh, much better. Thank you.

We started work roughly back in October where we had our initial informal get together. Really started work in January. And six months in we are generally on track for our goal of having the report out - a draft report out early next year, January, February.

We divided the groups - the questions the GNSO gave us into groups. We're not going through them in order. That was largely - and this is mainly for people who haven't followed (unintelligible) obviously. We did that to make our discussions more coherent, more sensible.

As it is sometimes our groupings will require back and forth discussions. We'll come to a prelim conclusion and have to go back and look at it again after we discuss related issues later. But at least by grouping we cut down on that.

We broke into seven groups. We have gotten through four of them already. Obviously three more but again there will be some circling back. If I had to identify two areas that are going to be the most difficult I think we've covered one and we still have one to go.

Now generally we've reached preliminary conclusions on a number of charter questions but I think these are the highlights. One of our basic questions, we've got proxy and privacy service we're supposed to examine, or accreditation, we - I think we fairly quickly - nobody suggested there was a reason for us to examine privacy and proxy differently so we're proceeding as if the criteria for accreditation will be the same in groups.

Let me just suggest here whenever I say we came to an agreement or consensus or whatever these are all draft conclusions; we will be revisiting as we start drafting the final document.

We will recommend that ICANN will publish a list of accredited proxy privacy providers with contacts and contacts that are reachable, identifiable. We'll recommend that there be some way to label registry entries that are there - proxy privacy services, when they're used as registry entries.

You know, in some cases it's very easy to identify. But not always. There are a few ways to do that, I think we have some things in mind. But our job here is to recommend the - not standards, the policies, so a lot of things that we discuss we may come up with suggestions and thoughts but that's really going to be ICANN staff's role to come up with the specifics once our recommendations get through comment to the GNSO and the Board.

There'll have to be validation. I'm going to be real careful with that term, validation and verification. They have different meanings to different people. Some codification in contracts now but still if you're not familiar with those you may not focus into the formal definitions. But they'll have to be validated or verified per the specs - along the lines of the specs in the RAA - 2013 RAA.

Now that would seem like it's just easy enough given how many proxy privacy services, at least we know of, are connected to registrars but many aren't so the mechanics of that will be something we'll have to address.

Services will have to relay notices required by an RAA or consensus policy. This is one of the areas where I talked about jumping back and forth. We have a question that we suggest that where we had to address that basic point but later on we will get into specifics of reveal and relay involving proxy privacy.

Customer agreements with registrants will have to set out rights and responsibilities, have provisions concerning termination in cases of transfer. We'll have to look at issues concerning protection of the privacy element when a proxy registration transfers from one registrar to another, because there potentially is a hole there where the information can be public however briefly.

They'll have to be designated contacts; it's not just - along with just listing a contact - a contact on the Website, ICANN Website. And finally, we've decided there should be a list, malicious conduct, that's appropriate for reporting to privacy proxy conduct. And again that's something that will take developing either under later questions that we have to address or under, again, once it's moved out of the policy process and into specifics that we'll be - well there's the traditional ICANN policy versus implementation question.

Pardon? Oh, sorry, you're hiding behind your mic.

James Bladel: Technically it's Marika's mic. I'm just borrowing. So this is James from Go Daddy. And I don't mean to take the conversation into a detour here but I do want to point out that during some of the other sessions here in London we captured - as we're running through the issues that this group is addressing - we've uncovered something that I think may be a pretty sizeable omission from our charter and our mission which is what happens when a accredited privacy proxy service with - believe to be a base of customers, is de-accredited?

And that opens up another bunch of interesting avenues about whether or not they are also required to make data escrow deposits separate from any registry - oh I'm sorry, registrar data escrow deposits and how that might be allocated to a successor privacy proxy service in the event, you know, in a bulk fashion.

So, you know, I don't know if this the appropriate time to tack that onto our list but I think as a working group we may have missed that one; I don't think it was in our charter and I think it's only come up here in London in the last couple days.

Don Blumenthal: Well I was just going to ask Marika or Mary to talk about our ability to add questions so - and I see Marika has her hand up.

Marika Konings: Yeah this is Marika. But I think that's definitely something that, you know, staff would also take as part of, of course, the accreditation program like I think that process is in place for de-accreditation of registrars, what happens then.

So I would presume that is something that is already at least on our list in the framework of an accreditation program. I will definitely take this, as well, back to our colleagues and as said, presumably the model that is being used for the accreditation of registrars may serve as a model here noting that of course there are some particular items that would need to be considered.

So maybe we can take it back as an item to see where conversation internally stand on that. And we do have I think a section that talks about the accreditation and more, you know, what are the reasons for the accreditation. But I think under that we could possibly then as well review what the staff's thinking is for that part of the process and see if there are any specific concerns that the group has around those items.

Don Blumenthal: Yeah, I appreciate it. We do have the section on the process of the accreditation or the issue of de-accreditation. But what James is suggesting and Graeme was mentioning - add some issues that aren't explicitly in our questions.

Steve Metalitz: Yeah, this is Steve Metalitz for the transcript. I agree that's the course to follow with this. One question I would have is I'm wondering how big the problem is because as you pointed out at the outset we need to have an accreditation standard that deals both with affiliated proxy - privacy proxy services that are affiliated, really alter egos, of accredited registrars and those that are not.

Those that are I would think we - I'm not sure there would need to be any special treatment because there already are these procedures for if registrars become de-accredited. And they do have to make escrow deposits and so forth.

So that may be part of the answer but obviously because we were supposed to be setting up standards for - excuse me - unaffiliated accredited providers, that then clearly doesn't - isn't covered by whatever the provisions are for registrars. Thank you.

Don Blumenthal: James.

James Bladel: Thanks. And good point, Steve. We're trying to kind of build the general case for the future when there are independent - let's call them independent or unaffiliated privacy proxy services.

But I think even in the case where it is affiliated with the registrar we'll have to take a close look at when those names are resurrected in the new registrar; do they automatically inherit the privacy services of that registrar? Is that a criteria for selecting that successor registrar? Or do they come back to life in an exposed state? And I don't mean to make this more complicated but unfortunately at ICANN everything's more complicated than (unintelligible).

Don Blumenthal: Okay (unintelligible). Yeah, I mean, I think at this point it's on our list of issues that we'll have to - we've got some ground work to do, I'm sure we will address them - these new questions. We've just got to work out the way we can do it and procedural issues, substantive issues, whatever comes along.

Yeah, we've got some upcoming both current things that we discussed and not really come to any kind of agreement on and then some challenges that we foresee. The one area where we've had I think the most intention, I think is probably a good word, is the issue of whether all privacy - all registrants should be eligible for privacy and proxy services.

There are essentially three groups I think, maybe a fourth, but for the most the discussion is centered around the traditional - well three, one, yes, everybody should be eligible regardless of purpose or registrant identification or corporate structure, whatever, everybody should be eligible.

The dichotomy that's been in place since I've been involved in some of these battles, and I worked on my first Whois accuracy paper in 1998 or 1999 which is really kind of depressing, the traditional - our discussion has been between, well, not everybody should be eligible and there should be a distinction between commercial and noncommercial. You know, we'll leave definitions aside.

A proposal that's gotten a lot of discussion in the working group is a variation on that. Noncommercial and commercial organizations that do not use their domains to conduct transactions would be eligible for proxy privacy. One of the best examples, a commercial domain that would be eligible is a company that's doing new product development and wants an internet presence but doesn't want a premature release of their plans.

And then companies that do use their domains to conduct transactions, and again there's definitions to be developed, would not be eligible for privacy proxy registrations. I'm going to loop back to that as soon as I finish this slide.

We need to develop more specific guidelines and questions concerning what kind of malicious conduct would constitute abuse. And there's even been some thought, well, about whether there should become some kind of uniform reporting form. The MCA has been suggested. I pulled out an abuse reporting form from the anti-phishing working group so at least we would have some ideas to work from or to recommend that staff work from.

We need to look at the Expert Working Group privacy proxy recommendations to decide how to proceed with respect to them. Now I don't think there's much significantly different. I don't think there's anything significantly different, just it's only three pages out of 165 or 166 and really just gives some high level suggestions that I think we're working through.

Finally, we need to tackle reveal and relay issues which I think is going to be another difficult one. There's all sorts of nuances there.

I want to circle back to the start of this slide. Like I said, this was a contentious - our only really contentious discussion I think. And I wanted to give opportunities to people on the working group to - if nothing else question my description of the avenues we discussed and my characterization of them.

Wow, this was - oh, Steve, go ahead.

Steve Metalitz: Something - got to get something started here. Thank you, Don. This is Steve Metalitz. You know, I thought what might be most helpful just in terms of stimulating some discussion would be to look at these points, especially the first three - and I'm happy to give my perspective and in some cases this has been the provisional position of my constituency, on these and see - because I'd be very interested to hear from others off the working group as well with their views on it. However, it's now - it's disappeared so I...

((Crosstalk))

Steve Metalitz: No, that's okay, I was just going to work from those bullets. On - this commercial non commercial issue I think you've accurately characterized what the new position is that has been put forward. I don't think that that position has commanded a lot of support on the working group though it has its adherence.

And I think the reason is, at least from my perspective, it doesn't really solve the problem which is that it's very difficult to determine whether a registrant is commercial or non commercial and even whether a particular use is transactional or non transactional. There's a lot of gray areas. There's also going to be a lot of variations from country to country on how those points are defined.

And I think that the general idea that - and principle - anybody would be eligible to have a proxy or privacy registration is by far the simplest way to proceed and I think while in an ideal world there would be benefits to excluding certain types of registrants, I think it's just the practical difficulties are insurmountable even if it's at the level of transaction versus non transaction.

I think on the malicious conduct point, I wouldn't assume that we do necessarily need a detailed list. We do have lists now that are in the 2013 RAA and in the PIC specifications of the new gTLD Registry Agreements. They're not identical but very close.

And it may be that that's enough and that the entities that have to deal with those, registrars, registries, that accredited service providers can also deal with that list and be sufficiently open ended and flexible. And of course we don't want to - one downside of a definition is that it might exclude new forms of malicious conduct that we can't anticipate now. So I would just put out there that we may - may or may not need that list defined.

And on the third issue about the Expert Working Group proposal, it's important to remember that - I agree, there's a lot of overlap there but they're talking about a - how privacy and proxy services might be structured or accredited in a new - totally new environment starting - one that really is not like today's Whois environment and is a paradigm shift and which is now being, you know, we're starting now the debate on that.

And I know some of the other people in the room came earlier from the session with the EWG and there's going to be a lot of debate about that. Our job is look at accredited proxy and privacy registration - or what the accreditation standards should be in today's environment which, whether we like it or not, is kind of where we are and I think where we will be for some period of time to come.

So that is one difference that we need to bear in mind as we look at these - at the Expert Working Group recommendations. So, you know, I don't know how many people, when you go outside the front door of the hotel and you've seen that little stone pillar that is there? And it's a historical marker that tells you that this hotel is the sight where, starting in the 12th Century, public executions were carried out.

So I don't know - I'm not trying to revive that process but I did want to at least put some views out there. And I hope people will shoot at them to - and give their reactions on these issues because I think that would be useful for the working group.

Don Blumenthal: Oh, I've got to stop imagining. James.

James Bladel: Thanks. James speaking. And I want to work backwards from Steve's contribution and first off just be very grateful I think that participation - the trend that we've seen in increased participation at ICANN meetings would definitely decline if executions were part of the agenda because I know it would involve contracted parties for starters.

Don Blumenthal: Be more efficient.

James Bladel: Yeah, certainly it would be, you know, led by Compliance. I don't know, maybe attendance would actually increase actually now that I think about it. I do want to, you know, enthusiastically agree with what Steve was saying. And it kind of was percolating in the back of my mind when we noted on the list here about the EWG which is that this is kind of - in an embryonic state here of not being policy. It's more of just kind of a high level principle or even more of a vision statement, the EWG report.

And so while I think we should be mindful of what's coming out of that particularly as it relates to our work, I don't know that it's necessarily something that we have to navigate as part of our recommendations.

I wanted to address just real quickly the threshold question because I think we have spent a lot of time on this and I think as - what's starting to seem like a - and certainly speaking for registrars is always a challenge because they're so diverse.

But I think it's starting to seem like a - a position of at least most of the registrars that also operate privacy proxy services is that in addition to the practical concerns that Steve indicated, there are even more than just determining what is or is not a commercial use of a domain name.

I think for starters that a domain name itself is not a financial instrument, that the transaction is occurring somehow, either credit cards or PayPal or, you know, cash on the street, there's some other mechanism by which the financial transaction is occurring.

And the system may also have its own dispute mechanisms that the registrant may be providing a marketplace for individuals and businesses to exchange and transact with each other and therefore maybe uninvolved in any commercial involvement.

I'm struggling to think of why they would need privacy but I just want to say it could be possible that they are - they are unrelated. And then finally just that if, you know, it's a transaction that's gone wrong, it's a customer service issue if it's gone really wrong and it crosses that line into fraud then we need to - I think we are on our to do list highlighting what we do in the case of illegal activity. So I think it would already be covered under that relay and reveal process whatever, you know, whatever comes up there.

So I just - I believe - and then finally there was that issue about whether or not political or religious or other types of donations constitute commercial activities. So I think there's a lot of - as Steve was saying, there's a lot of practical concerns about how you monitor this, how you would define it, how you would enforce it and what the downstream consequences of that might be.

Don Blumenthal: Thanks. Christian.

Christian Dawson: So since we're dealing with questionnaire issues I wanted to - the ISPCP actually - we took the time to focus on our response specifically to this. And I figured it would be a good time to go ahead and actually read it, it's pretty short so.

"The Interest Service Providers and Connectivity Providers operate Internet backbone networks and/or provide access to Internet and related services to end users. We're key players on the Internet and have a central role in its stability and development. The ISPCP Constituencies seek to selectively respond to the GNSO PPSAI Working Group community questions for London."

"We focused comments only on Category C and seek to state unequivocally that we do not believe in a threshold for privacy and proxy services. We do not believe that it's appropriate for this group to address this nor do we believe it necessary or proactive for ICANN to require categorization of use of a domain for any contracted party."

"We therefore file the following official responses on behalf of our constituency. Category C, Question 1: No. Category C, Question 2: No."

Man: The ISPs stand behind...

Don Blumenthal: Yeah, I appreciate it. And just as a general note, any - all of our templates, the submissions to the committee, to the working group when we solicited them early on are on the - are on the working group wiki page for anybody who wants to follow up and take a look.

Christian Dawson: Appreciate it.

Man: Question from behind.

Don Blumenthal: Oh yeah, I can't turn. Please cover that one.

Man: (Unintelligible).

Man: (Unintelligible). So for the record (unintelligible). I just wanted to highlight that the - (unintelligible) on the issue of who would be eligible for privacy (registration) proxies but also the question how do define those (unintelligible) who would be eligible to access the data behind the privacy proxies and also define in a way all the work is the proxy at all because many companies at the moment (unintelligible) function as (unintelligible) proxies for (unintelligible) services even they are not accredited or seem to be as a proxy service.

So you could also define these (unintelligible) who are eligible to access or use the privacy proxy. Thank you.

Don Blumenthal: That's going to be part of the - a lot of that is going to be part of that reveal and relay discussion that we'll have later on. But it's definitely on our agenda.

Man: I just want to step back to the discussion a second ago by James about charitable organizations and not having to disclose information about, you know, their identity. That's one of the biggest factors of fraud actually.

And in a place in the world where, you know, perhaps one of the most stringent privacy requirements are invoked, Canada, the name of the charitable organization, the charitable purpose, the cost of fundraising, the address and the name and the phone number and contact person of the charity must be provided for a physical discussion about a durable donation. So why would that not be required online?

So I'm just curious quite you would have invoked that?

Don Blumenthal: James?

James Bladel: On the Website, absolutely.

Man: And why not in the registration?

James Bladel: Because it may be unrelated.

Man: That doesn't make sense to me.

Don Blumenthal: You want to - I could mention a number of instances where parent companies will, if nothing else, will register a domain. That's one example. The registrant may be possible to contact the registrant and the responsible party for the domain but it may not really provide adequate information in terms of contacting the entity behind the Website.

Man: And if there's fraudulent activity occurring?

Don Blumenthal: I don't.

James Bladel: Well we are discussing a mechanism for reporting illegal activity. And I think that that would certainly qualify as illegal activity. And then in that case that reveal and relaying - or the reveal process I think would kick in. So it's a question of NVIDIA reactive thing when fraudulent or illegal activity is actually determined to be occurring or are we doing that preemptively by just banning them access to the privacy service entirely?

Man: I think they should not be entitled to privacy service for that purpose. I mean, Stephanie has a comment and she's a privacy expert; I'd love to hear her comment on it.

Stephanie Perrin: Well, can I just - oh (unintelligible). Yeah, hi. Stephanie Perrin for the record. I realize you're talking about charities which are not eligible for protection under the data protection law, okay? But the conflation of information that's available as part of a charitable denomination, registration, whatever, and having this stuff available in an open Whois directory you can't do that.

Because you're talking about massive disclosure for unrelated purposes. If you have an illegitimate law enforcement allegation against the charity that they are doing something fraudulent then with or without the new recommendations of the EWG you should be able to come down, state your case and do a revealed on the charity.

The information or charitable designation is primarily there for tax purposes so that's the reason that that's available in the physical directory. And it may have to be available on the Website. But that's different than the directory.

So I guess I would like to, from a public policy perspective, and let's face it, ICANN is enough business, you have to maintain clear boundaries about what work we are doing. And we're not policing tax and we're actually not policing criminal activity; we're making information available under particular circumstances for those purposes.

Man: I have one important question to ask, is there a right of privacy for commercial enterprise?

((Crosstalk))

Don Blumenthal: In what country?

((Crosstalk))

Stephanie Perrin: Yes and it's - yes and it's complicated. And in Canada it goes province by province.

((Crosstalk))

Kathy Kleiman: Hi, sorry to be coming in late. Kathy Kleiman, Fletcher, Heald & Hildreth (unintelligible). Yeah, under the United States law that's a right of anonymous political speech and that includes both individuals and organizations. So if a few people come together for political purposes and put out a domain name and Website and lists and emails, yeah, they're supposed to be protected because the right of the speech and the marketplace of ideas - and even if they become an LLC, that doesn't change the nature of the communication which they are engaged, which is noncommercial.

((Crosstalk))

Man: I'm talking about commercial purpose.

Don Blumenthal: Okay...

Kathy Kleiman: Commercial entity versus commercial purpose. Oh my God.

Graeme Bunton: All right, we have a couple people waiting in the queue that we should maybe move on to.

Don Blumenthal: Yeah.

Graeme Bunton: (Laura) is first I think.

(Laura Steeds): (Laura Steeds) with (unintelligible) Script. I'd like to speak out. And one of the few people here I believe who does support - not allowing people to have privacy proxy who are using domain names for a commercial purpose.

First of all I'd like to address the point that was made about whether domain names can even be used for a commercial purpose or they're facilitating. I think that's a Website very clearly can facilitate commercial activity.

It would be a bit like saying, I don't actually buy anything, my money by something. Well, technically that might be true but without me the money doesn't actually purchase anything. Without the domain name, without the Website there's no storefront through which consumers can purchase goods so I feel that's a bit - I don't think that's a compelling argument.

The question of practicality that's come up several times, I don't think that's an issue either. I think the way this is handled is you asked people at the beginning when they're registering their domain name, "Are you using this for commercial activity?" If the answer is yes the privacy proxy service is not available. If they answer no then it is. Obviously people lie.

But in the event that that happens then people can file a complaint and the relay reveal process can commence from there. I don't think there needs to be massive enforcement or people checking. I think this is something that comes down to enforcement and complaints.

Of course the big question is whether this is even desirable. I'd argue that it is. I think there is a precedent for people who are - who have a commercial purpose - not commercial activities but somebody who is actually selling a product in nearly every country. There are a few exceptions (unintelligible) I know you've mentioned.

But, in nearly every country corporations have to register because that way if there's a dispute in a commercial transaction people can get back to the party responsible for this document activity and file a complaint.

I recognize the point about corporate speech. I don't think, and I believe this point was made by the gentlemen at the end, that corporate speech elections is the equivalent of somebody who's actively selling a product should not be able to hide their identity in the event that there's some kind of dispute. That needs to be out there. There is a clear precedent for that in the physical world. I don't think this is terribly different.

The question of whether there are exceptions, for example, charities that might need to hide their identity for political reasons, I think that's important. But these are the exceptions to the general rule.

We can put something into place for exceptions for political purposes but I don't think that we can define policy based on edge cases. Thank you.

Graeme Bunton: I've got Wendy in the queue next. And please state your name when you talk for the record.

Wendy Seltzer: Thanks. Wendy Seltzer. And I want to support the unequivocal anyone should be permitted to use privacy proxy services, no matter what the category of their current or planned domain name use or status.

And I think this discussion has helps to illustrate the reasons. There are different laws and regulations and requirements in different jurisdictions. There are different categorizations of the spectrum of activity. There are individuals who vary at the different times of their use of a domain whether it's for personal, commercial, political, religious purposes.

And I think our Whois and domain name registration system, and no matter how it evolves under the EWG or otherwise, will never have the level of detail necessary to capture all of that. The appropriate place to apply those laws and regulations is at the application layer, if you will, at the place where people are making the use.

If you want to regulate that a commercial Website should publish contact information, tell people to publish contact information on the Website itself and regulate it there. We shouldn't be backfilling these requirements into the Whois display or into who may or may not register with a privacy or proxy service. Thank you.

Graeme Bunton: Thank you, Wendy. I've got David then Volker then Benet. Anybody else?

David Cake: I just wanted to say that the difficulty we discussed about - yeah, this point about when - your commercial entities versus commercial activity and so on is quite complicated but essentially means that we - you can't make a decision on appropriateness - well and whether someone is acting commercially until after registration and so on, it's got to be - it can't be a - and basically this distinction becomes increasingly a complicated one and largely one that must be done on a case by case basis which means that of course you can have a proxy privacy registration because we can't make that decision until long after, you know, you can't make the determination of commerciality until long after you already have had to make the decision about whether they can use a privacy or proxy service so.

Graeme Bunton: Thank you. Volker.

Volker Greimann: Yes, two points. I can't believe I'm saying this but I'm actually agreeing with LegiScript on one point. We should not be making policy for edge cases. Edge cases being criminal use because the majority of domain names are used legitimately.

Second point I was trying - I am trying to make is that the domain owner does not need to be the user of the domain name. There are many cases out there where people are renting out the use of their domain name that they bought legitimately to a company that used the domain name.

Even I have been approached for my family domain name by a company that wanted to use it. I denied that because I wanted to use the Website as well. But if you only want to use, for example, the email functions of the domain name and want to - do not have a plan for using the domain name for hosting then you might as well rent that out to someone who does want that.

I still do not want to have my information in the Whois just because the user of the domain name has a commercial purpose.

Graeme Bunton: Thanks, Volker. Benet.

Benet Garcia: Benet Garcia for the record. So I had three points basically. One is that we seem to be discussing a particular kind of paradigm where there is a Website and there's somebody hiding behind it somewhere else, where at the SMB level and the Website is, I mean, like your pizza parlor, you know who they are, you know where they are. They're not hiding behind their Website or their registration. Your tanning salon, your consultant, that they are not hiding behind anything so your access to their malicious behavior is a personal thing but that kind of information they put in their RA is irrelevant to that particular (unintelligible).

The other thing is is that, you know, we're talking about the scales of the different problems. It's a much bigger problem for these people who are - and I don't say at the level of SMB the difference between individual - a person and commercial is so subtle when you're talking about how they use their websites and how they - what they do personally that you'd be making distinctions all day long to try to draw that line.

The other thing is it's a matter of scale, we talked about the, you know, malicious use as an edge case. But what's not an edge case is when I, as a reseller, when I put new Website out into the world and that information goes out there, people mine their emails and they spam.

Now if I were to just draw you a bar chart of how often that happens versus malicious behavior this is a much bigger problem I'm protecting someone for then the few times someone might maliciously do it. And we talked about ways about getting around that and actually getting access to what's behind the proxy but that - but just my point is that it's a matter of scale so there's that.

Graeme Bunton: Thanks, Benet. I've got (Laura).

(Laura): Thank you. And could I communicate I'm also flabbergasted (unintelligible) and LegitScript agree on something. However I would argue that - so although LegitScript's focus is obviously on criminality I don't think that this is just about criminality. That would be an extreme example of when you would want the information about a company revealed.

But let's say I didn't receive my product, let's say my product wasn't what I expected. I should be able to contact the company and be able to negotiate with them directly. That's a thing that happens in the real world, it's a thing that’s happened in the real world forever, I think that should happen on the Internet as well.

Wendy made an excellent point about how they should list their contact information on the Website. They should. The trouble with that is that we can't validate that. There is absolutely no way without getting into really serious freedom of speech concern that weekend ensure that the contact information listed on these websites is okay.

However, at the Whois level there is a mechanism to validate, there is a mechanism where they're not - even in our system where we don't actually check I don't believe they are legally supposed to put false information which makes, again, in the worst-case scenario make it possible to go after them. And in the best case scenario where it's a mix up, but I really need to contact them specifically I can.

To the point that you don't always know what you're going to do with a domain name, domain names can fluctuate back and forth between commercial purpose and not commercial purpose, I was under the impression that people can go back and forth on privacy proxy used as well.

And comment again, I agree that it's impossible to enforce this from the front and back I do think that a complaint filed against somebody using a domain name for a commercial purpose who is using a privacy proxy is fairly simple. Thank you.

Don Blumenthal: Volker and then we'll move on to the next topic.

Volker Greimann: Yeah, I have to think about it just move on.

Don Blumenthal: Stephanie and then we'll...

Stephanie Perrin: Stephanie Perrin for the record. Volker, you're making me feel guilty; I'm not going to think, I'm just going to go ahead and speak. I'm a stranger here myself, I've only been on this working group for a while. I'm not familiar with ICANN's (bring it) policies into detail I'd like to be. So can someone please point me to the document that indicates ICANN's scope for the regulation of electronic commerce?

I was involved, when in government, with regulation of electronic commerce in the early days and I didn't think it was ICANN's responsibility to govern anything but the domain name. So, yes, there's a problem with criminal use of online commerce but how is that ICANN's problem?

And just because we could have good data in the domain name system to solve this problem, does that mean we either have the responsibility or the right? Thanks. And if I'm wrong, please show me this because I just don't understand it.

Don Blumenthal: Okay. Have you collected - I mean, I want to move on here, do you want to...

((Crosstalk))

Don Blumenthal: Okay, we are going to make an exception because somebody from the community that we haven't heard from wants to speak.

((Crosstalk))

Man: So for the record (unintelligible) Interpol. Yeah, first I thought I'm not going to comment on anything but it seems I'm only law enforcement person here in this room. I feel that I have to say something.

Anyway, as it was said before, these services, they are mostly - they are legitimate. And the users they are legitimate. But there has to be also process to protect the legitimate use of these services. And this process means that there has to be ways of mechanisms for law enforcement to take actions - appropriate actions to a person's and services abusing this service - privacy and proxy services. So that's just my point.

((Crosstalk))

Woman: I don't think any of our conversation at any point has ever said that in fact (unintelligible) you should not have access to Whois. That really is not the debate. The debate is all about the extent to which, A, you can define a commercial purpose immediately, whatever; and, B, if that should make any difference to your access.

But nobody here thinks you guys shouldn't have - we just have to define what we mean by law enforcement, that's all.

Don Blumenthal: Another interesting issue. Next on our agenda is to go through some of the preliminary conclusions that we've reached in our deliberations. We are - we've kind of done that but I'd like to at least carve out at least a few minutes to go through the other ones we've addressed just to see if we can get some thoughts from - either additional thoughts from people at the table or thoughts from folks who haven't been involved all along.

I will trust staff to go through those and you can quickly summarize because I'm having real troubles seeing that or Graeme or Steve either.

Steve Metalitz: Okay, I'm supposed to summarize what our conclusions are? Okay. The first one that I see up there, which is A2, you know, privacy and proxy services - those are defined in terms and the staff can indicate what the source is but basically a proxy service is defined as one in which no information about the actual registrant is disclosed in Whois. And a privacy service - the name of the registrant is disclosed but no other information and there's forwarding information.

So the most recent data we had was that something like 95% of the services involved are proxy services and privacy services are extremely rare. But we were asked whether there should be a difference between how they are treated for purposes of accreditation or anything else.

And this is a good example of a question where we gave a provisional response but we may have to circle back. As we sat at the beginning of the process we couldn't think of any reason why they would be treated differently. But we did say we may come across one as we get into some specific questions. So that's the reason for this.

I don't know whether, you know, maybe if people have any comments on this question this would be the time to come forward with it especially people that are not members of the working group who may want to add something that we've missed in our deliberations on A2.

Don Blumenthal: We have a classic member of the working group to start. That's you James.

James Bladel: Oh. I'm like who are you talking about? So James for the transcript. And, you know, I've been thinking about this one a little bit more as well, Steve. And I actually think that we got it right, our initial reaction or our gut may have been on the mark.

And I say that because my understanding is that the distinctions between the two are not only, I want to see mostly irrelevant, but are also becoming more and more of a gray transition than a black-and-white line.

If we define proxy services as containing no information in Whois regarding the underlying customer I think even a number of those services are changing to at least indicate that they are acting on behalf of a unique customer by some sort of a customer ID number or some other unique identifier perhaps in the relay emails.

So I think that, you know, the distinction between the two is becoming very very blurry and therefore I think that it probably benefits the working group to treat them as interchangeable because I think that the industry's trend is that they are merging into one type of category and it's just semantics if we call them a privacy or proxy service at this point - or will be soon.

Don Blumenthal: Appreciate it. Any other - okay? Oh, no, we do.

Man: I just wanted to comment that (unintelligible) indication of usage of proxy - for a proxy (unintelligible) are those players, for example, some nation states or someone who want really to hide their registration data they are not using -

they wouldn't consider using any public (unintelligible) proxy registration. So in that case it would require that to be indicated publicly then you would need to involve also the case of those (unintelligible) proxy or hard proxy instances. Thank you.

Don Blumenthal: Okay.

((Crosstalk))

Don Blumenthal: I just can't read it.

Steve Metalitz: Turning it off. Okay the next question is B1. And if someone could scroll back up? Thank you. And this is, as we mentioned, the question is whether the entry in Whois should clearly show that the registration is made through a privacy proxy service. And a little background on this is that there have been a couple of studies that ICANN commissioned to try to measure the prevalence of privacy proxy services and for some other reasons.

And it wasn't always possible to determine this. Sometimes it was pretty clear that this was a proxy registration but other times it wasn't. So - and especially if we were going to have the standardization of reveal and relate you need to know if this is one where you need to try to, you know, if you're qualified to get a relay or reveal you need to know that this is a service that is subject to it.

And of course the registrar who would be under the obligation not to use an unaccredited proxy service provider would need to know. So the idea was that there should be some way that any coolies user could tell that a particular registration was a proxy registration.

And I think in general, we discussed a couple ways of doing this area in general we kind of left that as an implementation question as to how this should be done but that there should be some method whereby somebody who accesses a Whois record would be able to tell whether or not it was a privacy/proxy registration. So that was our preliminary conclusion.

Any comments on that?

Stephanie Perrin: Stephanie Perrin. Just to say that the EWG, for what it's worth, we recommended that be a mandatory field, I believe so that we would know.

Don Blumenthal: And that's one of the distinct differences between what we are working on and any new system. There may be more flexibility in a new system to add a field to Whois records. Right now it's not an easy process. We probably have to be looking at other mechanisms for identification.

Steve Metalitz: Okay no other questions or comments? Okay so the next question is on periodic checks to ensure the accuracy of customer contact information. Another way to phrase this is to say what verification or validation requirements would there be for this contact information?

And I think the significance of this is that, again, in a situation where someone is entitled to get that information revealed from the proxy or privacy service, it's important that we have some confidence that the information will be valid and verified and be able to contact the person.

So the debate really I think within our group mostly focused on whether they should have the same requirements as for verification and validation of a Whois - excuse me, of a domain name registration generally, in other words the requirement of registrars under the 2013 RAA - the extent to which they have to validate or verify or whether there should be additional requirements based on the fact that there will inevitably be a delay in accessing this information, again, any reveal situation and therefore the chances that it is actionable need to be even higher.

I think the tentative conclusion that was reached here was basically to parallel what's in the 2013 - or in a manner consistent with the 2013 RAA; you can't exactly parallel it because obviously there's some differences.

We address the situation in which the - the service as a captive affiliate of the registrar and may not - it's not - if the registrar has already validated and verified that information then there's no need for the service to do so.

And then we also recommended that an equivalent to the Whois data reminder policy be put in place whereby the proxy providers - the service providers would be required to tell their customers annually that they need to maintain accurate information and that - and that they should update it and then the rest of it again parallels - I don't know if it's exactly the same but it parallels the 2013 RAA provisions regarding re-verification when there's a change.

So basically our provisional conclusion, and again this is something that we are going to circle back on after we've had that discussion about relay and reveal, is that the verification of this data would be similar to what's required for registrars under the 2013 RAA.

Graeme Bunton: We've got James in the queue.

James Bladel: Thanks. James speaking. And just to add to that I think that, you know, as a registrar with an affiliated privacy proxy service we certainly like to reuse procedures and code wherever possible so mirroring what is already in the RAA and other policies is - just makes operational sense and doesn't require us to go out and reeducate the world again on a different procedure.

The only hesitation I have - and I don't think it's a big objection at this point, it's just a little bit of uneasiness - is, you know, currently the proxy service in some cases will - because it is the information that is in Whois will respond to the ICANN Whois reminder request but then its customers would have to respond to a different type of data contact reminder request. So when struggling with how that is all going to work. But otherwise, you know, I think it's sensible to parallel this around existing requirements.

Graeme Bunton: That's a good point, James. I also tend to agree, speaking as Graeme from Tucows. Wendy.

Wendy Seltzer: Thanks. And a question that I have that applies equally to the RAA requirement and these that would parallel them but perhaps more strongly here if we expect that any significant user of privacy and proxy services would be individual.

I'm concerned about the security and stability implications of the verification requirement and the ways that it could be gamed to cause someone to lose a domain name if the presumption were that they should be suspended if they failed to respond.

So to play that out just a bit further, The notification of bounced email you could imagine somebody - a domain being subject to a prolonged to denial of service attack such that they didn't get the initial email, didn't get follow-on emails, weren't available for contact through that means, being out of the country and being unable to respond to verify their information through the manual means, this could be used deliberately as a way to deprive someone of a domain name.

And particularly when we're talking about individuals in small operations, they're less likely to have someone back at home who can check in a different part of the business that everything is continuing to function normally.

Graeme Bunton: Thanks, Wendy. I don't think the gaming of that is something that we discussed in the working group. Someone can correct me if I'm wrong. James, you have a response too?

James Bladel: Oh just that, you know, if anyone is perhaps thinking that that sounds like an unusual or rare or exotic type of occurrence I can assure you that is a very common occurrence where people will see a high-value domain name that someone doesn't want to sell and they will find various ways to try and get it canceled so that they can pick it up in a deletion or a drop type service.

And unfortunately - we call that shaking the trees. You know, and it is very common unfortunately that they will attack a domain name that they want to cause to be deleted both through this policy and through invalid Whois reports, just continuously filing invalid Whois reports.

Steve Metalitz: I just want to say I hear what you're saying and what Wendy is suggesting. I'm not sure that this adds to that problem, in fact I think in general it would be - I'm not quite sure how this would be vulnerable even to that. But I understand it as far as domain name registration is concerned.

James Bladel: I mean, hypothetically, Steve, it's possible that this would just create a new vector of vulnerability to that same practice - that if someone had to respond to both and ICANN Whois data reminder and a privacy proxy Whois reminder that the proxy service was no longer able to respond on their behalf then that...

Steve Metalitz: But the person would not respond to the person - the individual would not respond to that - would not even get the Whois data reminder, the service would get it. So in fact there would be - I just don't see how this adds to the vulnerability.

James Bladel: Well it is, at a minimum, it's something we should probably introduce into our discussion when we circle back on this one.

Volker Greimann: Maybe we can just agree on ensuring that mandated communications are - do reach the registrant so there is no duplication of efforts. And if the privacy service, for example, like ours, is set up in a way that all messages are transmitted to the beneficial owner, even if it's sent by the registrar and the privacy service does not get that directly then no additional messages need to be sent out.

It's basically saying Whois data reminder policy need to reach the registrant with the data of the underlying beneficial owner and all other messages also need to reach the original registrant - the real registrant. So basically saying if the registrar is setting it up - that it reaches the registrant it's okay, you know, nothing additional needs to happen. If it isn't - if that isn't the case then an additional message would have to be sent to ensure that the registrant is reached.

((Crosstalk))

Don Blumenthal: Okay, could we bring up the slide that showed the very brief description of our conclusions? We're at 15 minutes here - 15 minutes left. And send it in the idea here was to have the public, onlookers, comment but most of the discussion has been from people at the table, what I'd like to do is bring up the over arching list or the summary list but then leave some time for open questions from the audience or issues we really should be may be addressing or changing our focus or whatever else and have 15 minutes for just throw things at us or ask us questions, whatever.

((Crosstalk))

Graeme Bunton: There we go.

Don Blumenthal: All right, a brave man.

(Kevin MacArthur): Yeah, (Kevin McArthur), (unintelligible). A lot of this seems like we're collecting information, at least through the Whois process as well, that might e useful for a policing purpose in the future. And from a Canadian perspective, generally speaking, you don't collect information in the hopes that it may someday be useful, you only collect information once there is a use for the purpose of that collection.

And so I'm curious in this, you know, differentiation of reveals and all this, we're actually creating a process by which we are collecting information that may not be useful to a business purpose.

Graeme Bunton: Thank you.

Don Blumenthal: I was just going to ask if anybody wants to respond?

Steve Metalitz: Yeah, I think that this gets back to the point we raised earlier that we are designing these standards for the current environment. We're not collecting any new additional information from registrants than is already required to be collected under the RAA.

The EWG was asked to take a clean slate approach to this and look at the purpose of the collection and so forth and some of the points that you're raising.

That's not really our remit. Our remit is to say, under the existing - in the existing world where - gTLD world - where these are the data elements that are collected and where there are privacy and proxy services that, at this point, are not subject to any standards what should be the accreditation standards including the circumstances under which the information that is collected but is not made public should be made public. So that's kind of the environment within which we are working.

We could get into the debates also about what the purpose of collection of this data is. I'm not sure that's a fruitful debate in this environment but I would just say that the purpose is basically the same as it was since before the

World Wide Web when Whois first began just to identify and enable contact with the party responsible for Internet resource.

Stephanie Perrin: Hi. In the sense that - Stephanie Perrin for the record. In the sense that I'm speaking on behalf of data protection, I'd like to align myself with being a law enforcement official here because data protection laws should be enforced. And I would suggest that when we actually do some kind of a compliance audit on those elements that we are collecting, it may be that we don't have adequate reason to collect it.

So just during that's out there. That could come from and ATRT report; did that come from a complaint that causes complaints to ICANN under data protection law and, you name it.

Don Blumenthal: If I can just flush out for people who haven't followed - or been enmeshed in this stuff since who knows when just to clarify something Steve said there. The contact points - or the reason for the contact way back when was - the purpose was to get a hold of the person who controls the domain strictly for technical reasons. If you went down you'd know how to get in touch with to try to remedy the situation and get back up.

That gradually morphed into more general purposes for contact and then it just exploded with the commercialization of the web and the advent of the first hyperlinks through the Mosaic browser and it's been an interesting process looking back at that initial step to what it is now or how it's used now.

Nobody wants to look at the summarized conclusions instead of - as opposed to the detail we went through? Okay I really expected more commentary, I'm not sure there's a point to going back to reading the template. It is up there. And again we are - while there aren't formal opportunities to provide comments, if you're not on the working group, except for those of us who have been sucked into NomComm and will go underground as soon as this one is - this meeting is over again.

We're in the halls. Our information is posted on the Website. And certainly - at least I and I assume a lot of other folks are open to listening in an informal way. We did specifically at the launch (unintelligible) program reached out to folks at that session Monday morning to come. And I'm glad I had a taker. We've reached out to LE to join the working group and somebody from the US FDA has and hopefully more will because we really are looking for the broadest representation on this working group and it's not too late to join.

I made a presentation at the Center, which is the European Association of ccTLDs, a few weeks ago and asked ccTLD registries to join us. We don't cover CCs but the European approach at least to proxy privacy has been much different from what we're talking about, independent services. But there are rules there.

And as more and more of the CC operators are getting into the G business because they're becoming backend operators of new gTLDs and DNic is supporting dotBerlin, for example, I think there are some valuable perspectives to come from that group and any others anybody can think of and I mean that.

This has been a dynamic group. We're six months in and we still have strong participation on our phone calls and on the mailing list, which is very unusual and highly appreciated.

And at that point why don't I just give folks 8 minutes back which I think would be particularly appreciated if there are people outside waiting to take this room over. Appreciate your time.

END