TORONTO – Privacy/Proxy Accreditation Program Development
Wednesday, October 17, 2012 – 13:30 to 14:45
ICANN - Toronto, Canada

MIKE ZUPKE: Welcome, thanks for coming. Good afternoon. Now can we begin recording, please? Thank you. Alright, thanks for coming. Today we're here to talk about the privacy and proxy accreditation program that was envisioned as part of the negotiations that are ongoing right now.

Related to our accreditation agreement, we've got a great panel of people here to talk about sort of their perspective and their opinions on the program and about proxies and privacy services, some of their experiences with those.

I'm going to introduce the panel in a minute. My name is Mike Zupke. I'm the director of registrar programs at ICANN staff. So I'm going to give you a little bit of back ground about how privacy and proxy services work, and then we'll get in to the real reason why you're here.

To hear the discussion about how the accreditation program should be developed. So I think probably most people in this room know a thing or two about domain names so I'll try not to get too elementary.

But the privacy and proxy services that we're talking about are WHOIS privacy and WHOIS proxy services and they were born out of the market place because there were people who felt they didn't want their contact details to be published in WHOIS.

And it's not necessarily just individuals it also could be corporations who are perhaps launching a product they don't want made public. But often times it was made for individuals who, basically privacy concerns. There are proxy services and there are privacy services, and sometimes people use the terms interchangeably.

But there is actually a difference and probably James of GO Daddy will correct me if I get this wrong. But generally the idea is a proxy is a registrant who licenses its use of the domain name to another person.

Who we call sometimes a licensee or the beneficial user or the beneficial registrant, or some people say the real registrant. It's not the registered name holder; the proxy is the registered name holder.

In a privacy service, the registered name holder is still there, so here's just a little bit of information about proxy services. The general idea is, if you as a consumer decide you want to use its main proxy services.

The general idea is if you as a consumer decide you want to use a domain proxy service, basically employ this third party usually a company to be your proxy.

And then when they get information or correspondence that comes to them because of their contact details in WHOIS, they would generally forward that to you.

Right now there's some inconsistency in the marketplace as to how that information gets forwarded. So we'll talk a little bit about that in a minute. When we talk about proxy it's easy to think about the registrar.

When you think about domain name or you want to register a domain name, the registrar offers you a proxy service but there are other kinds of proxy as well.

It could be a proxy service that's a company affiliated with the registrar. It could be a reseller, a Web host. It could be a stand-alone proxy business which I don't think is particularly common.

It could be an attorney who is registering a domain name for a client. It could be a broker, usually on a secondary market, who is purchasing a domain name for a client that oftentimes might be for business purposes where they wish to keep their business plan a secret until they launch.

There could also be family members if you have a parent or a child who is doing something on the Web but isn't quite ready to register the domain name or isn't quite tech savvy enough to manage that.

You can do that and then you're basically the proxy. We'll talk in a minute about what we're talking about in the accreditation program for proxies.

But I just want to point out now that when we talk about proxy accreditation we're not necessarily talking about everything on this list. We're not trying to regulate your children or your parents necessarily, unless they are pretty sophisticated and selling proxies to a lot of people.

Then as I mentioned there's the privacy service. In a privacy service, typically those are usually run by the registrar itself where in a proxy, the registrar cannot be the proxy because the registrar and the

registered name holder can't have a registration agreement between themselves because it's one person.

But in the case of a privacy service, the end customer can sign up for a domain name and still be the registrant or the official registered name holder but the WHOIS contact details are actually provided by the registrar or some information that's provided by whoever the privacy service is.

Then typically, like with a proxy, the correspondence should be forwarded to you when it comes from third parties. So I thought, before we get into this, I just want to kind of give you a little bit of a status of where we are and how we got there.

Whereas, I mention we're in the process of negotiating amendments to the registrar accreditation agreement which we also call RAA. And hopefully it won't be too confusing that we're talking about accreditation of proxy services when we also accredit registrars.

We'll try to be clear about that. But this is kind of a statement of what the current, what the 2009 version of the registrar accreditation agreement says about proxies. We have provision 3.7.7.3 which in some form has existed since 1999 but was amended for the 2009 agreement.

That basically says that registrars must include in their registration agreement a provision that tells that registered name holder that if it is licensing the use of its domain name to another party that there's a certain responsibility for the behavior or the actions that come with opening that domain name.

So in essence, the registered name holder is responsible unless when presented with reasonable evidence of actionable harm, it will disclose who the underlying customer is and their contact details. The other two provisions that are in the 2009 version of RAA are really concerned with the data escrow program.

Before we had these provisions, there was no obligation for a registrar to escrow registration data of the underlying customer. So in the even the registrar failed, you could conceivably have a file, the data escrow file, containing nothing but the proxy service.

That's not particularly helpful if the proxy service was also the registrar. So we want to encourage registrars to also escrow the underlying customer data and being cognizant that there might be reasons why a registrar might not want to do that.

Or why a registrant might not want to do that, it's basically offered as a requirement or a requirement for disclosure. So the registrar must either deposit the underlying customer data or disclose conspicuously to its customer that it's not doing so.

Then there's a similar requirement for resellers. The only real difference there is that resellers don't necessarily have to escrow the data. They can just give it to the registrar. So here's what we're talking about today.

We've got, I sort of tried to break out this into really basic components of the discussion we were having, the staff and registrars right now. I think this first bullet point we're generally in agreement on. What it says is that we'll put a provision in the accreditation agreement.

It's sort of like a placeholder. It says that when there is a proxy accreditation program, registrars will only knowingly accept proxy registrations from accredited proxies, and the same for privacy services.

The nuance is where we'll still kind of discussing. That's how do we get to this accreditation program? So what the ICANN draft of the agreement posted before Prague says it could be through a consensus process.

It could be through just contractual negotiation and hardwired into the accreditation agreement. Or it could be a program which is commercially reasonable that takes place in consultation with registrars.

From our perspective, we want to involve other stakeholders in that too. But that's for the registrar's sake that they would want consultation in there. We heard a lot of people today and earlier say there's a right way to do this process and there's other ways to do this process.

We've heard both sides of this. We've heard some people say this really should be done by a PDP. We have heard other people say hardwire this into the contract because that's the fastest way to get it done and that's how we want it.

The staff perspective on this is we don't really know how this is going to evolve. We want to see what's the substance of this program going to look like? Then we can make a decision about what's the best path forward.

I've talked to panelists about this and I've asked them to try to help us focus on substance because from my perspective and from the others of

us on staff, this is a listening experience for us. We want to hear what it is that the community expects will be included in this program.

That will also help inform the decision about how to go forward in terms of implementing it. So I'll stop there. Were there any questions and I hope I wasn't talking too fast. I tend to do that. Okay, excellent well educated crowd.

So, let me just introduce our panelists here. We have a really great diverse group. I'll start here on the end. We've got Bobby Flaim who comes to us from the FBI.

We've got Wendy Seltzer who is a member of NCUC and also a founder of the Chilling Effects Clearinghouse, very interesting stuff there. We've got Steve Metalitz who comes from IPC and is also an intellectual property attorney.

And we've got Susan Kawaguchi and she comes to us from Facebook. She also was a member of the WHOIS review team. So we asked her if she could sort of maybe put two hats on and tell us a little bit about her experience at Facebook and also a little bit about what she experienced as part of the review team.

Finally, we've got James Bladel who comes to us from GoDaddy and he also was a member of the WHOIS review team so hopefully he'll be able to sort of add some color from that experience too.

So to sort of kick this off I thought you know why don't we just sort of start with the why. Why are we doing this? Maybe Bobby you can kind of give us some idea about what is it that the law enforcement community hopes will come from this?

BOBBY FLAIM: Thank you. I think what we're hoping comes from this is part of the recommendations that we had put forth about three years ago was all about due diligence transparency in the WHOIS.

Part of the recommendations concerning the proxy and privacy registrations and making sure they were credited was making sure that they fall within the ICANN system of the due diligence accreditation ensuring that they are legitimate organizations.

They are falling within the RAA and kind of falling within the whole framework of ICANN to make sure that if law enforcement needs to get information through legal process, we know exactly where to go and who we're dealing with.

A lot of the proxy and privacy registrations are being offered now by the registrars and that has worked out well. So we want to extend that over to ensure that the whole landscape is on an equal and level playing field so that when there is a privacy or proxy registration we know exactly who to go to.

We know exactly who to serve our legal process to and we know exactly who the players are. So that's kind of the thought process behind that and why we had put that in our recommendations. So is that?

MIKE ZUPKE: Yeah, for sure. So maybe you could sort of tell us how exactly you see that playing out when in the day to day interaction that you'll have with

registrants or licensees, how do you see this benefiting you specifically, or benefiting people in your community fairly specifically?

BOBBY FLAIM: The benefit is we know who the actors are. Like I said already, we know who some of them are but again it's to have established criteria on who's offering these services and to make sure that ICANN knows who they are and they're within the ecosystem.

So for us the benefit would be legal process, who are we dealing with? Are they vetted out? Are they legitimate agencies? Does ICANN know who they are? Do they have a license? Do they have a business license? Are they semi "accredited"?

So who are they and where will ICANN's reach be if they are not complying with ICANN's rules and regulations such as the registrars are right now.

Because that is a very big portion of the domain name industry and how registrants register domain names, again we just want to make sure there is the due diligence and the transparency and accountability.

MIKE ZUPKE: So I should say I would like to encourage the panelists to talk amongst themselves. You don't have to wait for me to ask questions. I see Steve is ready to jump in so please go ahead.

STEVE METALITZ: Thank you Mike. I think it's worth putting just a little bit more context here. I think you gave a very good introduction and the distinction between privacy and proxy services.

But the study that ICANN commissioned from the National, from NORC, about four or five years ago really is one of our best pieces of data on this and it showed that about 20%, about 18-20% of all registrations in gTLDs are proxy or privacy registrations, mostly proxy.

That's 20% of a very large number. At that time it was 100 million. It's a lot more now. If .proxy were a TLD, it would be the second largest gTLD in the world.

So we have this vast universe of registrations where the goal of WHOIS is to, among other things, allow people to know who they're dealing with online. And enable contact with the operators of online resources is failing in those areas because that information is not accessible to the public in WHOIS.

And then the provisions, you mentioned 3.7.7.3, which is intended to provide a path to finding out that information when the registration is being misused is not working. It works sometimes. It varies from provider to provider, but there really aren't any kind of clear path that Bobby's talking about really doesn't exist.

So our view, just to make it clear, we support the use of proxy services. Although it's interesting, there are some ccTLDs that don't allow them and that might be worth exploring too. But the vast majorities of proxy registrants I'm confident are using, are perfectly legitimate and are using registrations in a perfectly legitimate way.

But we also have evidence, and I think common sense would tell us, that people who are up to bad things, including but not limited to theft of intellectual property, are just proportionately likely to use proxy registration because it allows them to hide who they are and to frustrate the accountability and transparency that WHOIS provides.

That's the status quo and that's why we're glad to see motion toward trying to resolve that status quo and put some, you know it's a Wild West situation there in the proxy universe in .proxy.

And we are really eager to see some rules of the road put into place that would benefit law enforcement, that would benefit intellectual property owners, would benefit the public which is also really ultimately the beneficiary of public access of WHOIS.

So I just wanted to add that additional context because it's not a small isolated problem. This is a huge part of the gTLD universe.

MIKE ZUPKE: Thanks Steve. It looks like Wendy is dying to jump in here.

WENDY SELTZER: Thanks and given past discussions we've had on the subject will likely not surprise anyone that I disagree. Basically from the start the notion that we should be accrediting proxy and privacy providers and the purpose of the WHOIS and the rationale for ICANN to do that, I think this proposal is a dramatic extension of ICANN's contractual Web to include oversight of another class of parties well beyond the registries and registrars to a potentially large number of providers.

Now when you said you didn't plan to accredit the parents and the attorneys, or at least not the parents, if you don't demand that all of them be accredited where do we draw the line?

And if there's a line we know that the bad actors will find their way to the other side of the line. So it's not clear to me how this solves the problem that we have.

And I think we have to seriously consider the costs of adding yet another accreditation program to ICANN's mandate, the costs both in dollars of developing, administering, and overseeing the compliance.

More important perhaps the cost of dilution of attention for the organization as it has to expand its staffing and its mission to cover oversight of yet another piece of the Internet content landscape which is really getting pretty far from the registration and the database of a domain name.

Lots of the complaints that would be made against privacy and proxy services won't be ones that can be determined, does a zone file validate.

So I think that's a huge cost that ultimately falls on the registering, domain registering public because that's where most of the money comes into the system from.

And that means it's harder for individuals and non-profit associations to register and use domain names as pointers to their online speech.

MIKE ZUPKE: Thanks Wendy. One of the things that I think has sort of driven this concept or this potential accreditation program is really it's the interest of law enforcement.

It's the interest of people who are enforcing intellectual property rights. But one of the things that I think could also be an outcome of this is enhanced consumer protections. And I'm wondering how would you balance that equation?

WENDY SELTZER: I hear intellectual property posited as a consumer protection often in practice I think that there's more of a gap. I don't think consumer protection is a mandate of the DNS. There are plenty of other places to protect consumers.

When studies have asked consumers do they even know about the WHOIS as a place to find information, most of them don't. The WHOIS is poorly suited as a business lookup database.

If you're asking should I do business with a website, there are better ways for you to determine that information. And if you're trying to protect consumers against bad actors using the Internet, there are better ways to get at them than through WHOIS information.

MIKE ZUPKE: So I appreciate that. I probably didn't word my question very clearly. I was thinking more about the actual users of the privacy or proxy services who are maybe experiencing inconsistent treatment across registrars.

For example, one registrar might be particularly agreeable to demands that come in to reveal the identity of the underlying user where others might be a little bit more challenging at those sorts of requests.

So there is a potential in doing this program to at least have some consistency or have some strengthening or aligning consumer expectations with practices that go on.

WENDY SELTZER: I would suggest that consumers are more benefitted by the availability of a variety of different programs with different offers and different contours that some of the services offered for free may be worth as much as people pay for them.

Others of them may be ones that come with guarantees of we will only reveal your information response to a court order. I think that then there are third parties, Electronic Frontier Foundation and other rights organizations who can help to aggregate information about where the best and less good places to get privacy and proxy services might be. I don't think that's ICANN's role.

MIKE ZUPKE: Okay, hey James. I was just going to ask you a question. Thanks. But go ahead please.

JAMES BLADEL: You were going to ask me a question?

MIKE ZUPKE: I was.

JAMES BLADEL: Okay, go ahead.

MIKE ZUPKE: Well I was going to ask you…

JAMES BLADEL: I might cover it here but…

MIKE ZUPKE: As a representative of a registrar, you're probably in a really good position to see how consumers' expectations align with the actual service and whether there are areas where that could be improved or enhanced, or how you see it in the marketplace.

JAMES BLADEL: So certainly from a consumer's perspective that paid for a privacy service, every reveal is a failure of customer service on their part. Any time that we actually send them information or even relay a contact that they were not expecting or asking for in some respects could be considered a diminishment of the value that they believe they paid for which is to get some protections against those types of things.

So I just wanted to kind of touch back and circle back. I'm wearing three hats today, obviously with GoDaddy which is a registrar and we have an

affiliated proxy service provider which is a domain by proxy. I don't think we've been secret about that.

It's a very popular service. Also a member, former member, alumni, what are we calling ourselves? The artists formerly known as the WHOIS Review Team, just circling back to the beginning as Steve mentioned these are very popular services.

Ours in particular, we're very proud of this service. I think what that tells you is that this is meeting a need. This is solving a problem that is perceived in the marketplace.

That someone's willing to step up and open their wallet for an optional service like this at the level that we're seeing indicates that there're a general concern about exposing personal data onto public databases which have no access controls or restrictions on use.

So we are participating in this program for a couple of reasons. One I like to think that we are a good actor in this space. I think that my friends from the IPC would probably back up at least part of that statement.

That we have put in some rules of the road, it may only apply to us at this time. But we're willing to share those practices and disseminate them throughout the community and throughout this industry.

I think it raises an interesting point. You asked me not to go there, but where's the authority coming from to do this? I think that's an interesting point. I think ICANN is not a government.

It can't go out and bring somebody under its umbrella. Everybody that comes to ICANN submits to it willingly for the perceived benefit. So we want to make sure there're benefits to privacy and proxy providers to becoming accredited, that it's opening up new markets for them.

That it's putting them in touch with customers or products or providers that they wouldn't otherwise have access to. My fear, and again same thing we say as a registrar, we're trying to put more daylight between us and the bad actors that Bobby's talking about.

I hear this every ICANN meeting, registrars, and proxy servers, not you guys. You guys are good guys. But yet we're painted with the same brush whenever we kind of go after the bad guys.

My concern is that this will be more of the same. That the good guys will step up, will implement accreditation, will apply for accreditation, and then will follow whatever prescriptions come out of the accreditation program, and will pass those along to their customers.

And the bad guys will say, "You know, it's not for me. I'm a bad guy proxy service. I'm not going to bother with accreditation." And we will kind of add some structure or some concrete to the status quo. That's my concern.

But again, we're willing to participate. We're coming here to say we have, I think, the answer to what a good proxy service looks like. We have the blueprint to an accreditation program and we want to share it. We're not guarding this. We're not treating this as a secret sauce. We're not selling this. We want to give this away.

MIKE ZUPKE: I certainly appreciate that. And I was hoping maybe Susan you could talk about your experience with the good and the bad as sort of a reverse user of proxy services.

SUSAN KAWAGUCHI: So I agree with James and GoDaddy. They have a well-defined process. I know what to expect. I know where I can use my trademark registrations and receive information.

I try not to make requests that they can't fulfill, to put them in a position where they have to say no to me. I do an evaluation, look at the site, and look at the domain registration.

If Facebook is not in the domain name but there's Facebook content and unauthorized use of Trademarks on the site, then I don't go the, and it is a domains by proxy registration.

I do not look to them to provide information to me. I think they have set up a very well standardized process. What isn't happening across the board in all proxy providers is the definitions that you laid out here on proxy and privacy.

No one is really adhering to those definitions. They're not clear cut. So you'll have a privacy service that looks very much like a proxy service and vice versa.

So the definitions have to be very well laid out in the expectations for those two services because I do think they are two very distinct services. I also think we need to step back a little bit and think about why people

and when people should be able to use, or entities should be able to use a proxy service.

There are many legitimate reasons. Free Speech, we don't all have the same rights in each country. I believe in that that you should be able to have a proxy registration and not have your details divulged.

What I do not agree with is there's any sort of ecommerce, any sort of collection of money, an ad if it's a site making any sort of money, at least in the US if you go downtown and you go into a store there's either you're talking to a person, a representative of that company.

And you're also seeing a business license on the wall. You know who to contact if you have a problem. But to me, there is no legitimate use of a proxy for a business online. They should just not be allowed.

To me it's a bright line, a distinct line, and it shouldn't be crossed. I think we need to start out with some very basic elements and decide as a community the standards for this.

MIKE ZUPKE: So I'm wondering Steve as an intellectual property attorney if you sort of had a different thought on that?

STEVE METALITZ: Well, yeah, I think I just want to comment on one thing James said which was about the possible unintended consequences of this in setting the current situation in concrete. It's a little hard to get my mind around that image of this chaos becoming concrete.

But I think the idea you put forward was if there were an accreditation program, then registrars if they wanted to be accredited could only deal with those proxy services and not deal with unaccredited proxy and privacy services.

And I agree with you. I'm not concerned with if the bad guys end up having their children be the registrants there's probably very little that can be done about that.

That's a different problem but we're really talking about these major commercial services for the most part. It strikes me that there are costs to an accreditation program which Wendy pointed out and of course you could achieve the same objective.

And probably more quickly, if you simply embodied the standards that you wanted these services to use in the contract, the RAA, and said, "Registrars have to limit the sale of proxy registrations to entities that meet those standards."

Accreditation is really just kind of shorthand for that. And it also gives the registrars some confidence that they can rely if it's an accredited service they can rely on that and they'll have a safe harbor in a way.

But you could do it the other way which could be a lot more efficient in terms of getting us to that point. We probably should talk more about this whole question of who can, who should be able to use a proxy service or a privacy service.

And I'll just mention that there was a session here just a couple hours ago where the preliminary results of another study by NORC

commissioned by ICANN were disclosed. I thought it was kind of interesting.

They were trying to figure out what can we tell about the characteristics of registrants in the domain name system? Two points stood out for me. One is that there seems to be no statistically significant difference in the level of use of proxy services between legal persons and natural persons.

In other words, companies or legal persons are just as likely to use proxy services as natural persons. I was a little surprised to hear. And the other data point was that they looked at sites associated with these domain names.

I don't know all the methodology that they were using but their conclusion was that the rate of potentially commercial uses of the domain name was actually higher for registrants that were using privacy and proxy services rather than those who did not.

So it's kind of the opposite of what Susan was saying as far as the bright line. This was a statistically significant difference. So that's our status quo. Anybody can use these. They can do it for anything.

I appreciate the value of trying to address that. But I would say it's probably simpler to, I think we should focus perhaps less on entry into the proxy system and more on exit from the proxy system.

Entry into the proxy system, are you allowed to do a proxy registration? That depends on your status and who you are and so forth. That's sometimes very difficult to ascertain. It could put a big burden on the service to ascertain that.

Exit is when are you kicked out of the program at least to the extent that your contact information is revealed to someone who has come in and shown that you're using the domain name in a harmful way. That depends on behavior, not status.

It should be easier to determine that rather than at the front end saying, "Gee, is this an individual? Is it a legal person? Are they going to do something commercial?" it's hard to answer those questions.

But on the other end, what have they done or what has happened? How has the domain name been used? That should be easier to determine.

MIKE ZUPKE: I'm seeing people to your right who look like they want to add something.

WENDY SELTZER: So I would disagree with the notion that ICANN should limit who can use privacy and proxy services. I don't believe that we can draw the line at an iota of commercial activity. There are numerous individual and non-profit sites that support themselves using advertisements.

There are lots of, and again as a consumer protection matter it's up to the consumer to determine does he want to do business with someone who identifies or is he comfortable doing business on a basis that doesn't have that connection.

I don't think ICANN is in a position to make that determination for all consumers. It's certainly not in a position to make that determination

for all would be speakers online. I'll stop there and come back to other questions since I see Bobby also interested in responding.

BOBBY FLAIM: Thank you. To go on one of your earlier points, I really do think it is ICANN's role. ICANN is this is your contract; you're on the final arbiters. You're going to hear many people from many different industries and I think the bottom line of ICANN is the safety and the security of the Internet.

And I think it's going to be, I think it is your role to make that distinction and make sure all the players are who they say they are and that everyone is complying with the same rules and regulations and contract and everything else that goes along with it.

It shouldn't be that just GoDaddy has to do what they need to do and no one else does what they need to do. There has to be a level playing field. I would agree with Facebook and Steve Metalitz in so far there should be, not everyone should have the anonymity.

You can't walk down the street and have the right not to be noticed. If you're a business and you're engaging in legitimate business activities, why would you need to hide who you are?

You have to file certificates of incorporation. These are things that you need to do so why would you need to hide who you are on the Internet and hide your domain names? So I think that is one thing that should be considered.

The other thing is criminals do use proxy services. We've done surveys in the FBI. We've had child exploitation cases, national security cases, consumer fraud, credit card fraud, botnet fraud, in which they have used proxy registration. So criminals will pay and they will gain the system if there are not the proper mechanisms in place.

MIKE ZUPKE: So one of the things that I've heard that I think might be helpful, Steve called it the exit from being a user of a proxy service. I think what we're really talking about is when does the underlying customer's name and contact information get revealed, right? So I'm wondering if any of you would like to sort of offer when you think that should be and maybe? Okay, James, great.

JAMES BLADEL: No, I actually agree on that. I think it's much easier, much cleaner to establish the terms and conditions under which you have abused your use of a proxy service and to kick them out and to perhaps standardize some of those practices.

I think determining eligibility at the front end is not just problematic. It's just something I'm not comfortable with because it strips to divide folks into classes or based on use and intention. Of course people change their minds.

They don't have ads up today or a PayPal donation up today. But they put one up tomorrow or they take it down when they think someone is looking or something like that. I think that what we have determined is, and I think this does frustrate.

I'll be on the level. I think this does frustrate the folks who would like to see more structure in this area is that as the provider of the service, we establish the terms and conditions under which we will kick someone out of our service, of the use of our service.

I think that it's probably safe to say that law enforcement and intellectual property folks might want a greater say in those scenarios and to put some more clear-cut rules in there. But I think that ultimately it comes down to some standardization, some consistency.

But with the understanding that ultimately there needs to be discretion and judgment on the part of the service provider to say, "No, I think that this is not a legitimate request to expose the personal information of someone. I understand you believe you have a claim and you believe that very strongly. But that doesn't translate into an obligation on me necessarily."

Or "No, I do believe this is a law enforcement overreach in this particular scenario." I think this is something that should be reserved in sort of a judgment area of the service provider. But ultimately as businesses, we're going to want to limit and minimize our exposure.

So if we believe that someone has a clear cut case, they're gone. And by gone what it means is we just cancel the proxy service and reinsert, well we don't want to call it their original, their contact data into the WHOIS database. That has the Net effect of essentially kicking them out from the umbrella and putting them into public service.

MIKE ZUPKE: Go ahead Susan.

SUSAN KAWAGUCHI: So I just would like to address sort of the standardization because if I go to GoDaddy I know what to expect. I know pretty much when I'm going to get what I need from them. And they have a certain process for specifying the information I need to provide.

But that is not at all consistent across all the proxy and privacy providers. Just within our own enforcement program, I've identified 24 different proxy providers. I'm not sure how many there really are out there. I just know those I've identified.

So when I go to company x and say, "This is Trademark infringement. They're using Facebook in the domain name and it's unauthorized use. It's confusing. Here are our Trademark registrations."

I'll get pushbacks that are unbelievable. Well, a lot of times, A. I get no response. You can fill out the form all day long but it's not going anywhere.

B. I get a response, bring me a court order. Okay, a court order to get this site that is obviously infringing and most likely doing something criminal, just to get the contact information?

That doesn't fly. It's just not scalable. Then there's sort of a step down from that, the subpoena. I have used the 3.7.7.3 hundreds of times in these requests to push back.

Sometimes that does give, I get a response then. But having to figure out everybody's process to reveal information is just painful and

extremely time consuming. In the meantime, they're taking money and people think they are doing business with Facebook.

MIKE ZUPKE: When did you…? Was there something you wanted to add?

WENDY SELTZER: Yeah.

JAMES BLADEL: I got a lot of folks that are trying to get in on this and I don't know how long you wanted us to just talk amongst ourselves because. I know this is more of an open ended format and I just wanted to mention the panelists, I'm willing to stand down and let folks start chiming in from the…

MIKE ZUPKE: So the idea was we'd have about fifteen minutes at the end for comments and questions. But if things are sort of relevant to our discussion, maybe one of our staff members could walk around with a microphone and allow that?

WENDY SELTZER: While staff is walking around, we're not walking into uncharted territory in asking about the standards for reveal. US courts have had to encounter this when asked for the identities of anonymous speakers in context online and off.

They've raised a pretty high bar that speakers are entitled to protections of their identities because the shielding of identity is a value in itself that shouldn't be taken away without due process.

So in the online defamation context, John Doe suits brought against individuals posting to online message boards, the courts have said, "You have to show that you have a prima fascia case that you can show all of the elements of harm before you get the identity of the poster."

And plenty of those suits have then been thrown out because somebody was trying to make a political case, was trying to unmask a political opponent, or somebody who was not engaged in unlawful activity.

So I think users need those kinds of safeguards and those kinds of safeguards that can come only from the independent and objective oversight of a court, not the service provider subject to all sorts of pressures, including how much is it going to cost me to stand up on behalf of a user.

MIKE ZUPKE: So if I could just sort of push back a little bit, it sounds like what you're saying though is that they, the consumers, have choices in a marketplace that would maintain that standard of requiring a court order or subpoena and that's how they would protect themselves if they wanted that greater sense of privacy. Is that right?

WENDY SELTZER: I'm saying consumers should have that choice and privacy and proxy programs that forced them into a lesser degree of protection by accrediting only proxies who would reveal on anything less than a court order isn't giving consumers the full range of choices they're entitled to.

MIKE ZUPKE: Gotcha, thank you. Why don't we go ahead with the questions out here?

CHANDRA WATSON: Yeah, I just had a couple of comments on some of the earlier comments that were made during the discussion. The first is I guess the comments I think that Wendy made saying that consumer protection is not a mandate of the DNS and we should protect consumers somewhere else.

I'm a little uncomfortable with that statement obviously in our discussions we're discussing the privacy implications of the policies that are developed here and also ICANN under its Affirmation of Commitment is obliged to consider consumer protect with respect to expansion of New gTLDs.

So I just wouldn't want to summarily dismiss the consumer protection component of the policies that we develop here. So I just wanted to say that.

Then secondly I think also there was a statement that WHOIS is poorly suited to be a business lookup directory and that's because the system is not properly administered and there is inaccurate data.

If properly administered, it would actually be ideally suited for a lookup as a consumer. If I was on a website and they don't have their information there and I was about to buy something, if I am educated about the existence of WHOIS and I go to it and I see they're really registered in India or somewhere else then I can make that determination as a consumer whether I want to proceed.

But I think it actually is quite useful to a consumer who is knowledgeable about its existence and how the system operates. I also think that, I think there was a discussion about whether or not ICANN should even be pursuing this program.

I think these proxy provisions are in the Registrar Accreditation Agreement. There are provisions about WHOIS in the agreement. There are provisions about the registration data. So to me it is a non-issue.

It clearly falls within the framework that ICANN has created in terms of administering its contracts and the type of scope of those contracts. I just also wanted to support along the lines of can this be used for consumers to empower themselves online.

I would support the comments that Susan made from Facebook which was that these commercial actors, these businesses, should not necessarily be allowed to hide their data.

So I think that we certainly recognize that there is value in the proxy and privacy services to do just that protect people's property. But if you're online and you're a business,

I think that's a situation where if you're talking about the entry point to who should be eligible for these services, that is a bright line that perhaps we could draw.

MIKE ZUPKE: I'm sorry. I should have asked you to identify yourself for the record. Would you mind doing that?

CHANDRA WATSON: Hi. My name is Chandra Watson.

MIKE ZUPKE: Thank you.

CHANDRA WATSON: I work for the US Federal Trade Commission but all of my comments are my own. They are not on behalf of any Commissioner or the Commission.

MIKE ZUPKE: Thank you Chandra.

MARC TRACHTENBERG: I'm Marc Trachtenberg with Winston and Strawn. I'm part of the IPC. I would like to agree with Chandra's very personal comments that do not reflect the position of the FTC. I guess two comments for things that Wendy said.

One, when you talk about the high standards the courts have for revealing the identity of people, that's kind of what we're talking about here. We're talking about reasonable evidence of actionable harm.

Things like Trademark infringement, if you can reasonably show that there is harm courts will reveal the identity. Then the Trademark owner or even people in the public who want to know shouldn't have the high burden of going to file a case in court and getting a subpoena.

Additionally you mentioned earlier that WHOIS is poorly suited to protect consumers and there're plenty of other options they can use. I would like to know what these other options are because I haven't seen any of them.

And there's nothing better than WHOIS, even in the poor shape that WHOIS is in right now. So if you could tell me what those other great options are in the marketplace for consumers to find out more information about a website I would love to know because then we could use them in my firm.

WENDY SELTZER: Sure. Websites that self-identify and go through accreditation or display address information on the site, offer consumers those options. It's not ICANN's business to run the Better Business Bureau. It's not ICANN's business to run the corporate registries.

There are other places that those things are done. There are certificate authorities who do identification and charge lots of money. Some of them do it well; some of them do it poorly.

But all of those offer opportunities to authenticate the identity of those with whom you're doing business when it's worth it to a consumer to find that authentication. When it's not, because they just want to see something on a website, they should have those lower cost options.

MARC TRACHTENBERG: We're not talking about businesses that want to be accredited. We're talking about opposite people. That's the point you're missing. We're talking about people that specifically don't want any information about themselves.

This isn't about businesses getting accredited, going to the (inaudible) or going somewhere else. But that's not who we're talking about. We're talking about everybody else, all the bad actors who basically are putting up a store front or putting up a fake Facebook site or putting up anything else.

And those people have the opposite goal of not being identified. So there's got to be some way in order for consumers to protect themselves and for businesses to protect themselves to identify who is behind that website.

WENDY SELTZER: And the opportunity is consumer education to look for marks of verified identity before doing business. it's not everybody should identify yourselves because you might want to do business. it's rather…

MARC TRACHTENBERG: I didn't think about that. We should just educate all the consumers, okay.

WENDY SELTZER: Yep.

MARC TRACHTENBERG: That's a great solution.

MARGIE MILAM: Who's the next? Sorry.

JAMES BLADEL: Can I just respond real quickly. You mentioned something. Because we did find a parallel which was that you could create anonymous Facebook pages. I'm not picking on Facebook. I'm actually defending Facebook.

So our proxy service providers, they're private companies and they can set up their own terms of service under which they will decide who they do business with and under what terms they will cancel that service. I think it's very similar in that regard.

SUSAN KAWAGUCHI: Because, yes, I am sure there is a way to circumvent everything, right? That's what people just sit out there trying to do that all day long. But you report that anonymous page to me and it's going to be gone. You report it to the company, it is gone.

So if I report a proxy registration that's doing business without the appropriate Trademark use, it sits there. It might just have just enough of our Trademarks to think oh yes, this must be affiliated with Facebook. But I can't do anything.

JAMES BLADEL: What I'm getting at is you, Facebook, makes a determination when I as a third party contact Facebook and say, "I don't like this Facebook page. I want to know who's behind it." You make the determination of whether my request is legitimate or not. You don't presume I have a right to know who is behind that Facebook page.

SUSAN KAWAGUCHI: No, I do not. But if you report the page then we review it. We do take those same standards that you, an evaluation process. I'm not…

JAMES BLADEL: I was defending us both.

SUSAN KAWAGUCHI: Yeah, it didn't seem that way.

JAMES BLADEL: It was a Kumbaya moment. But I was drawing an analogy I think to…

MIKE ZUPKE: I think this is a good discussion and I think when we look to what's going to be the make-up of an accreditation program, what we really want to know is, how do we set the standards for revealing?

Also I think another big question is what's the due process involved? And that's sort of the theme that I'm hearing from everyone in one way or another is let's say the proxy program denies the reveal.

Should there be some kind of an appear right? Or let's say somebody has their privacy subject to being revealed, should they have some sort of a right to stop that?

I'd be interested to hear if the people on the panel or if there are others in the room who might have thoughts about where should the bar be set. When we look at it as ICANN we're saying there's going to be some minimum threshold saying a proxy must at least do this.

It doesn't necessarily mean we're going to make every proxy exactly conform to the same practice. It's going to be some minimum bar.

So I'm wondering if you guys have any insight into where should the minimum bar be where we say in this circumstance, every proxy should reveal. Go ahead Steve.

STEVE METALITZ: I think that's going to take some discussion about the different types of abuses we're talking about because it's going to be different. And we've had some of this actually and we've made some proposals in the past looking at the different types of abuses that are prevalent.

I think one thing that needs to be made very clear is to address the problem that Susan mentioned which is proxy services that now say only if you present us with a court order will we reveal this.

I think that needs to be spelled out in the, I think it should be spelled out in the RAA. But it certainly should be spelled out in any accreditation standards which then registrars would be obliged to only use services that meet those standards.

And it should spell out that you don't require legal process for revealing. Again the point that Susan was making is this is not a takedown of a site. This is not pursuing someone. This is simply finding out who it is that has registered that site.

Providing the information that basically the normal expectation would be in the WHOIS database anyway, I think that's the important aspect there. Also there's another part of this.

I understand from James Bladel you're kicked out of the program entirely in that circumstance which means everybody sees your data. And I know some providers will not do that.

But just reveal it to the requesting party which means that if you violated party x's rights, then party x is going to be able to find out who you are. But party y and party z don't really have a beef against you would not.

Okay, so I mean that's maybe a bit of a nuance. But the other thing that's important here as an accreditation standard is when we get that information, we want to have at least a higher assurance than we have today that the information is accurate.

So we've talked about WHOIS verification requirements for all registrations. That's obviously a bone of contention in RAA negotiations.

But it strikes me that at least for those that are in a proxy or privacy service, where someone is paying for it anyway, and you can build this into the cost structure, there should be a verification requirement for that data.

So once it's ultimately revealed, in a circumstance where it is revealed, you have a higher level of confidence that it will be valid. I think some of the concerns that arise from a blanket requirement if you will of WHOIS data verification are much less so in the proxy and privacy area because it's already a value added service.

MIKE ZUPKE: Wendy?

WENDY SELTZER: Yeah, we're conducting this entire conversation as if the only bad actors are on the side of those hiding behind using privacy and proxy services. Unfortunately there are bad actors trying to pierce the veil of anonymity that legitimate speakers are benefiting from.

If only all trademark claimants were solid in the assertion of their rights and asserted them only against infringers. If only all the claimants of defamations or other harms were absolutely right.

But since that's not the case, that's where we need courts as independent verification and validation of those claims. It's only by

going through a court that we the public get the assurance that in fact there is a valid claim.

Within ICANN we often forget that. We often look only at the bad actors on one side. Unfortunately there are people who will abuse the process to get identities as well.

MIKE ZUPKE: Thanks Wendy. We're now to that point where we're going to take questions officially. So Marge if you'd like to go around.

STEFAN LEGNER: My name is Stefan Legner. I'm with InterNetX PSI Use A. PSI Use A is our accredited registrar. Internet X is a registrar in Europe. I want to make the following point.

Mike, you presented in the beginning showing what is privacy and proxy service and who offers privacy and proxy service. What has not been presented explicitly are all the legitimate reasons why anybody would use a privacy or a proxy service.

We all know that there are actors on the market who operate on the gray or on the black side of law. They want to intend to do illegal things. However, there are a lot of very good reasons to use such a service.

I would like to see written down all these legitimate reasons why to do so. And if ever there is any measure proposed or even decided to do, there should be clearly seen what legitimate reasons are killed by this measurement.

And Bobby, to you, why should a company, an official company not want to have a domain name seen with its name? I look at future marks, names of cars, names of products.

A company has its marketing department. They want to register this name but they don't want to have this name seen as some of their property because this reveals their plans.

So there might be very, very legitimate reasons to do so and this should not be killed, definitely not.

MIKE ZUPKE: Yeah, of course.

SUSAN KAWAGUCHI: So I don't think, I think there are very, and I said that earlier. There are legitimate reasons. I haven't outlined them but yes Facebook is a company.

There are times when we're going to launch something, usually somebody figures out before they tell me. But I will register domain names with a proxy.

What I will never do as the domain manager for Facebook and when I was at eBay and PayPal is allow the site to go live with the proxy registration.

If the site's going live, once it's live, then I flip it over. So what I'm saying is yes, there's legitimate use. But if you are doing business, I should be able to know who you are. And you should know who I am.

I mean the EU, there's all kinds of requirements that we do not have in the US to have information on your site. But I can show you a bunch of websites that are based in the EU that have no contact information but my own, but Facebook Inc.'s.

It's like no, that's not Facebook. I can attest to that. Nobody else is going to know that.

MIKE ZUPKE: Thanks Susan. I just want to note I think it's kind of a process consideration. I think that was a really good suggestion that we look at how every potential use that we're aware of would be affected. We'll definitely take that back. Thanks.

STEVE LEVY: Hi. My name is, oh wait. I think I'd rather submit my comment under privacy and I'm going to hide my badge here. My name is Steve Levy. I'm with FairWinds Partners. Specifically directed to Wendy again, you talked about consumers educating themselves.

You also talked about that the courts should be the arbiters of what should and should not be revealed. It sounds like you're spouting a very free market sort of concept.

I guess one of my questions is do you feel, for example, in the US the Deceptive Trade Practices Act should be repealed? Do you feel the Truth in Lending Act should be repealed?

And simply allow consumers to be on their own and sort of try to navigate their own way? Or do you feel these acts perhaps validly, in the

interest of protecting consumers, validly take certain matters out of the courts and make protections more automatic rather than requiring people to avail themselves for protection each time?

MIKE ZUPKE: So I mean you're free to answer. I think we could also take it as more of a rhetorical question. I don't think anybody disputes that there are valid reasons for consumer protections. But your point is taken.

MALE: Thank you, a couple of quick points. As a trade marketer what always upsets me is to see privacy and proxy services that do not respond. So I'd rather have a responsive service than in recluse where I cannot reach anybody.

I think we need to make this responsiveness work. Nonetheless, I do think that there are good reasons to have privacy and proxy services.

I've seen numerous cases where let's say a domain name was owned by the owner of the business but that person didn't want to have his private address go public.

This might be a specialty for the European market but as you said, and I'm thankful for the remark, we have quite detailed information duties in our distance selling provisions. And talking about consumer trust, these are much better than looking at WHOIS.

So as a European, I doubt whether WHOIS is the solution. I sometimes look at forums where people discuss ecommerce sites and the first

question that people ask is, "Do they have a proper imprint on the site?"

So people don't use WHOIS but they look at the website whether the business is disclosing their information. I think that's the way that would be advisable to go rather than trying to make WHOIS work, which I think will fail ultimately.

Because I think the bad guys will get ways around it. If I were a bad actor, you would only find perfectly valid WHOIS information, only the person that's in there doesn't know about it.

MIKE ZUPKE: Thanks, next question or comment?

MARC TRACHTENBERG: I would just say that…

MARGIE MILAM: Name?

MARC TRACHTENBERG: Oh, Marc Trachtenberg. I would just say that I definitely agree that there are numerous reasons why people would want to hide their identity. A number of them are legitimate so I don't have a problem with that.

I'm not suggesting that those things be killed at all. Definitely, with any system there needs to be protections. Now obviously, some good or

bad actors on both the trademark side and the infringer side are going to abuse the system.

There's no system that is totally immune from abuse. That's just the world we live in and what we have to deal with. That doesn't mean there shouldn't be a system.

The other point I would make is even with regard to relying on courts, a problem that we're seeing more and more is that these proxy services are going overseas.

So they're offshore and they're not responding to requests. Some require that you just send an email only, but they don't accept postal mail.

Others require you to send postal mail only but no email. So even if you were to go to court and you had obvious actionable harm, you had obvious trademark abuse, obvious spam or fraud or malware or whatever it is, the court has no power to order this proxy provider who is overseas to do anything to reveal the identity.

So the only choice you have now is to file possibly UDRP this trademark in the domain name. But then you have to wait for the UDRP.

Or now you can file an ACPA if the trademark's in the domain name. But now you have to go through the expense of filing a lawsuit in Federal court, get your default judgment,

it still takes a lot of time. If there's no trademark in the domain name, well then again your option is to file a suit in Federal court. That's not really a great system. There needs to be some protection built in.

I think accreditation is one way to do it so that these proxy services have to be accredited. They have to be responsive to complaints of harm. If they're not, they lose their accreditation. No one can use that service anymore.

MIKE ZUPKE: Yeah, go ahead.

JAMES BLADEL: I think those are good points and I would just put out, one of the things that Susan and I discussed on the WHOIS Review Team was that maybe it's time for you guys to start taking some scalps.

If you're having that much difficulty reaching a proxy service provider, then I don't know what the distinction is. The bad actor, the proxy, versus the registrant, I think they're one in the same at a certain point if you're having that much difficulty just getting responsiveness from them.

I think it's the same situation where if I purchased something online and they took my money, charged my credit card, and didn't deliver anything.

I start to care less about who that person is. They're just a bad actor at that point. I think that you can kind of paint the proxy and registrant with the same brush.

Because a legitimate service provider, I believe, won't engage in that kind of stuff. Just my thoughts and I thought maybe start taking some

heads. Certainly we'll drive the good guys to my business, which is what I want.

[DC BURLEY]: Hi my name is [DC Burley]. I come from India. I represent a company, Net for India, which is a registrar as well as an ISP in India. I just want to, given the discussion, my observation and interpretation is looking like most of the discussions are based on US and European Union laws.

But there are laws that are beyond these regions which need to be considered when such policies are drafted. One of the incidents which recently happened in India was that there was a government order to ISPs to block a website.

As for the agreement which is signed by the service providers with the government, we are supposed to block that website. However, BSNL, the largest ISP in India was penalized by the court for blocking that particular website without any instruction from the court.

Because the IT Act says that the judgment of a site doing anything wrong is to be decided by the court. Until then, the site provider is just an accused.

When it comes to the proxy example, the problem that we face in India and that region is, as for the IT Act which was modified recently, there is a clause which defines intermediaries.

It defines who all constitutes the members of the intermediaries which include the registrars, which includes ISPs, which includes quantum providers, etc.

In such an environment, if we are not able to provide the rightful information which is sought by the law enforcement authorities or by the court, then the intermediaries is considered to be in alliance with the bad people.

So in our opinion, there should be a default inner description on what is privacy, what is private registrations by ICANN and there should be a definite policy on when to disclose, how to disclose, and who to disclose the information.

The bigger concern that we have is for instance 85% of the traffic from India goes out of India. So if information sought is lying outside India, still I'm being considered as an intermediary being in access of his port in India.

So but I do not have any access or information of those websites. I can't block because the court has to decide. Nobody's ready to go to the court because the site is completely outside of India.

But we're having trouble because the liaise will be forcing us to take actions or the government will ask us to give more information on that. So when we are defining these policies, how do we define the policies on disclosing information of the private registration between geographies?

That's not understood in the discussion. So if a registrar…? Can I ask under the registrar currently, even if I ask nobody will disclose them?

So if ICANN can put a condition in the RAA which will clearly define when the registrar needs to disclose this information, especially if it is between different regions and different geographies. Thank you.

MIKE ZUPKE: I think you've raised a couple of really good points there and I think we do need to be really sensitive to this sort of when we're crossing jurisdictional lines developing the program. Tim did you want to add this question?

TIM COLE: Yeah, we have a question from online and I think we're going to have to make this the last one because we're out of time.

MIKE ZUPKE: Well, Alan is in the queue next.

TIM COLE: Okay. Caroline Chicoine asks a question, poses a question for Wendy. And I know you briefly answered it online but I think for the benefit of everyone here.

She says, "Do you envision there can be a proposal other than the status quo that can address the legitimate interests on both sides of the fence which necessarily would require compromise on both sides.

If so, what would that look like?" So I don't know if Wendy wants, it was a question for Wendy.

WENDY SELTZER: Okay, I'm sorry I didn't know whether you really wanted to finish the queue first and then come back to us. What I said online, I think best

practices among self-developed among the providers not compliance creep from ICANN.

MIKE ZUPKE: So in the interest of getting our last few questions, I'm going to not have a wrap up. I'm going to just let us get our last few questions in. so here's Alan.

ALAN GREENBERG: It's not really a question. It's a statement. My crystal ball tells me ICANN is likely to do something as a result of all this, if only because of the recommendation from the review team. Could you go back to the slide just before discussions and questions?

I'd like to call your attention to what I hope is an embarrassing typo. The last option of doing something is ICANN created program in consultation with registrars. I hope in a multi stakeholder model the consultation will be with maybe a few other parties also.

MIKE ZUPKE: Thanks Alan. And that was actually something I did mention when I was describing the slide, from staff's perspective we definitely want to get all stakeholder's input in this. But from the contract perspective, what registrars want is to make sure that they're consulted. That's a provision in the contract.

ALAN GREENBERG: Words on slides live for a long time. What you've said there is not acceptable to some of us other stakeholders.

MALE: That phrase is used in a couple other places already in the RAA, Alan.

MIKE ZUPKE: Thanks, Alan, point taken.

MALE: My point is probably a little smaller than everyone else's but it has to do specifically with phishing and malware issues. It's a little bit more towards the people that are actually using the privacy protect services for the legitimate services that do pass on the EMLs to these people and are getting in contact with them, with other people trying to contact them it's great.

But for websites that don't have commercial value and don't have contact information are personal websites for people. They have their websites hacked and used for phishing or malware purposes.

And now legitimate companies trying to get that information cannot get in contact with them because these non-accredited privacy protect companies are not passing on the information.

So now they are now being compliant with these phishing people without even realizing it. it is becoming a really big issue because these companies are not passing on the issues.

Eventually the ISP may become involved and may take down the site for them or may get in contact with them through other ways. But that can take days that can take months, as opposed to directly contacting the domain owner and having the content removed immediately.

MALE: I think that's a very important point. Sometimes the registrants aren't the bad guy. The registrants are the victims. And this does stand in the way of redress.

MIKE ZUPKE: So thank you for that and I want to say thank you to all of our panelists and all of the people who are here who contributed to this discussion. I promised I wasn't going to wrap up.

But I do want to say this is the beginning, not the end of this dialog. I really appreciate everything that's been contributed so far and we plan to come back to you for more, the entire community that is. Thank you.

TIM COLE: We can stop the recording. Stop the recording.

[End of Transcript]