SINGAPORE – At-Large Discussion - Registration Directory Services: Now and the Future
Monday, March 24th 2014 – 15:00 to 16:30
ICANN – Singapore, Singapore

SUSIE JOHNSON: Good afternoon to all our participants here in Singapore, and good morning, good afternoon and good evening to all our remote participants. My name is Susie Johnson. Welcome to the At-Large Roundtable on Registration Directory Services – Now and the Future Session, on Monday, 24th of March at 15:00 Local Singapore Time. Please remember to state your name when speaking for transcript purposes.

We have live interpretation in French, Spanish and Chinese, so please state your name when speaking in order to identify you on the various language channels, as well as for transcript purposes. Please also speak at a reasonable speed in order to allow for accurate interpretation. Over to you, Holly.

HOLLY RAICHE: Thank you Susie. We're going to be a combined session because our time has been a bit collapsed. It's registration data. It was originally one session first of all on the privacy specification, which was introduced as part of the 2013 RAA, and the Working Group that has been formed under that has been to put some flesh on that Specification. When Carlton and I talked though, what we realized is that many of the issues that arise from that Specification will be carried over to the EWG, looking at the future of WHOIS data.

It probably won't be called WHOIS data. They'll be looking at who collects it, who verifies it, who gets to see it and under what circumstances. Those are many of the same issues that are being talked about in the context of the Working Group on Privacy Proxy Servers. So we're sort of going to combine this session. We're going to at least start with the three speakers that were talking about the Privacy Proxy Specification Working Group and its tasks, but then go straight into the others.

For the first three speakers – and we're just going to have a bit of a discussion – James Bladel, who is GoDaddy… Do you want me to give you a correct title of will that do?

JAMES BLADEL: James from GoDaddy is probably sufficient.

HOLLY RAICHE: That's good. Kathy Kleiman, who is Data Protection Expert, lawyer. You can always trust a lawyer.

KATHY KLEIMAN: And co-founder of the Non-Commercial Users Constituency. I've been doing WHOIS since the beginning of time, which is way too long.

HOLLY RAICHE: That really predates how long I've been doing WHOIS, which is only since 2009. Sitting to my left is somebody who should have been Steve, but we've got a much nicer version of Steve, maybe, in Paul. He wants to be called Steve. Carlton, are your panelists here yet? Do you want to introduce them now? Okay, we'll wait. We'll start with the discussion that was really relating to the Specification as part of the 2013 RAA. In relation to that, we actually said that… All right.

Where are the questions? The questions that we asked in relation to the Specification, under the RAA privacy proxy services must be accredited. One of the first questions that's been asked of the Working Group is what do we mean by accreditation, who's going to do it, what should be required, and should the requirements under the 2013 RAA be different for privacy proxy services?

As part of that question, what would be the requirements, and then under what circumstances, if any, are the contact details of the registrant revealed either to a particular group, and how are they identified, or more generally? At that point that's when Carlton and I thought that many of those questions arise. The other question that's been pretty alive in the Working Group has been what do we mean by verification?

It has a particular meaning under the 2013 RAA with its own specification. Some of that discussion is, does that process actually apply to verification in relation to privacy proxy services, and who does it. I'm going to start with my friend James.

JAMES BLADEL: Thanks Holly. You're correct. The 2013 RAA does require registrars to abide by the temporary specification on privacy and proxy services, and use accredited services when such a program is actually launched. I'm going to pick on staff here. During the process of negotiation, one of the draft documents was put on the table that, "Here is that accreditation process and here's what it is." I think registrars, correctly, at that time said, "This is really not appropriate for registrars and ICANN staff to go off in a room and hammer out the details of an accreditation program."

This really needs a community involvement. There are other folks that are not inside this room that probably need to weigh in here. I have the dubious honor and/or shame of, having been the author of this temporary specification, which I think lays out some very basic foundational requirements and obligations for what I would consider, and I think a lot of folks would consider, to be a responsible operator in this space.

That's that you have a formal agreement, that you disclose the terms of service of the privacy and proxy service, that you have a point of contact for various types of abuse, including law enforcement, and that you have not necessarily a standardized process, but at least a disclosed process for how you will address domain names or registrants that violate those terms of service. Whether you're going to just cancel the name, the registration, or cancel the service that has the net effect of reinserting the proxy service customer's name into the public WHOIS.

Whether that's a bilateral disclosure with just the reporting party, whether that's a public exposure publication. These are excellent questions that are fodder for the Working Group to nail down. I think in the interim this is a good foundational requirement to establish some basic parameters for operators. I would point out a couple of things. It sounds like they're technicalities but I think they are important. One is that this temporary specification does expire, and that was done on purpose to ensure the temporary does not become the permanent.

You know how things are at ICANN – they get some inertia and moss grows around their feet, then suddenly it's 2030 and we're still using the temporary specification. That's just a cultural thing. The second thing is that this specifically refers to affiliated privacy proxy services at this point in time, and it's possible that – depending on how the accreditation program shakes out – unaffiliated, unaccredited services would use a registrar service without the registrar's awareness.

So it's certainly one of those catch 22s, where you can't make someone contractually obligated to be responsible for things that they don't know are happening outside of their sphere of control. So I think that's a baseline of where we are, how we got here a little bit. Kathy and I are veterans from the ASO WHOIS Review Team from a few years back, and I think this was one of the robust recommendations to come out of that Review Team; that ICANN should accredit these services and bring it under the umbrella – bring them into the fold.

As a responsible operator in this space, we certainluy welcome that, and we want to see the bar raised in this area, or we want to see these folks, if they're not able to meet these requirements, let's be honest, we'd like to see them exit this space. There we go.

HOLLY RAICHE: Thank you very much. I'm going to call on Kathy, who's also been a very active discussant in this space.

KATHY KLEIMAN: I agree with James. We have the battle scars of the WHOIS Review Team. Like James I want to add a little background to the discussion first, if I might. I want to also thank you and Carlton for setting up this discussion. It's an important discussion. Thank you. I've been representing registrants for 18 years. I hate to admit that it's been that long. I work on the WHOIS issues because of the registrant perspective. I've represented human rights groups. Many of you here know – individuals, human rights groups, groups fighting for political freedom, religious freedom, minorities… So the WHOIS data has very special purpose for them because they're mostly engaged in sharing ideas online and if you reveal their name and/or location, you may be exposing them to certain types of harassment, intimidation or worse.

The WHOIS data has been of great concern to me, because at least in the United States we have certain privacy rights associated with free speech. You don't. it's gone up to the US Supreme Court several times; whether you have to put your name and address when you're engaged in political speech, and the answer's no. So three principles that the Non-Commercial Stakeholder Group has talked about. I want to mention them briefly.

For the accreditation process the first principle's access. We think that privacy and proxy services should be available to all categories of registrants – individuals, non-commercial organizations, even businesses. Many small businesses and large businesses too tend to use proxy privacy services while they're preparing the launch of a new product or service. It can be a number of months between when they get the domain name and when they're ready to launch, but they may not want the market, stock exchange or their competitors to know what they're engaged in.

So access is one of our principles. The second principle is due process. How does a proxy privacy service disclose a registrant, whether it's revealing to a party requesting the data, or a publication, which is putting the data out to the whole world. There's an interesting problem, because what's illegal in one country is not necessarily illegal in another. In some countries it's illegal to have comparative advertising; we actually name the inferior product. In the US that's legal and in other countries it's not. So requesting the data of a company to reveal that, if it's not illegal…

The more striking examples would be if Chinese law enforcement wants to find out who's running a felon gun group or pro-democracy group, and that group is operating out of the US or out of the EU where they'd be protected. The third principle is creative options for remedies. We would hate to see this accreditation process have quick and easy solutions. We'd like to see proxy privacy service providers have the option to have creative solutions.

One of the ones we've been talking about in the Working Group is the ability to take down the domain name, rather than reveal the identity of the domain name registrant. This might be something registrants would ask for ahead of time, or something that might be asked as part of a due process – why is this being requested, and would you prefer to take it down rather than reveal? There may be legal reasons not to do that, but in many cases, in general, it might be interesting. I have to credit Wendy Seltzer for this concept.

So those are my three principles that the NCSG has been introducing – access, due process, and creative solutions and remedies. Thanks for letting me provide that background.

HOLLY RAICHE: Thank you Kathy. Standing in for Steve, Paul McGrady, and then I'm going to stand in for Richard [Glenn? 00:18:06].

PAUL MCGRADY: Thank you very much. I really appreciate you having us here today. This Working Group has been a fiery one, in the sense that we have people with strong points of view, but it's also been a very collegial one in the sense that we have a lot of respect for each other and know where each other are coming from. There are a lot of general principles that we all agree on. I have been representing brand owners for not quite 18 years but long enough to be weary sometimes.

The purpose of the brand ultimately is to protect consumers. I think that's one of the reasons why trademark lawyers love their jobs, because it's a loophole in life, where we have good paying clients, but we ultimately are protecting the consumer, which is the point of trademarks in the first place; not necessarily to own intellectual property in the way that patents are owned in the same sense. There are some very basic things we think in order for this process to result in accreditation and a program that makes sense and ultimately protects consumers.

Some of these have already been mentioned. Terms and conditions for participation that are published, that include obligations and provide consequences for violations. For customers that fail to provide accurate and current contact information. Also an obligation to refrain from any use of the domain name for illegal activity, including piracy, trademark or copyright infringements, cyber squatting and counterfeiting. Procedures including time limits for relaying queries from third parties to service customers – the relay we've mentioned before.

Procedures including time limits for disclosing to third parties contact information provided by the customer to the service – we call that reveal –, and procedures including time limits for publishing customer contact information in the WHOIS. Procedures for collecting and verifying contact data from customers; that's reveal or… Publication obviously won't have any meaning if the underlying data is junk. Of course, periodic reporting to ICANN on metrics, such as number of relay and review requests received actions taken, and things of that nature.

So again, many of these concepts have already been shared. I think that the discussion right now, at least from what I'm hearing, is how do we get there in a balanced way. There are concerns. Kathy's raised some very legitimate concerns, so we have to keep those things in mind, on the registrar side but also, on the privacy proxy services side, there's also the reality of implementation issues, where at the end of the day it has to be implementable in order to function. So that's from the ICP point of view where we are, and I'm looking forward to continuing the discussion.

HOLLY RAICHE: Thanks Paul. The one person who couldn't be here because his minister wanted to talk to him, this is Richard [Leaming? 00:21:43], who is basically a high-level cop involved in cyber security. He got a phone call last night, that basically his minister wants briefing, which basically says the governments are starting to get interested in things like IANA. His point started off to be the test for verification should be higher than the 2013 RAA, because simply somebody is not out there in the public.

What he was also starting to talk about though was if you're not going to talk about a higher level of verification, talk about getting rid of the person altogether, as a way of if you don't want to do one thing, what is another way out of that. I'm sorry he's not here, and he's also sorry. Is he back there? No? Okay. Anyway, I just want to put on the table that there's a very strong law enforcement interest in this issue. Do we want to have a brief discussion about this, or go straight into…? James?

JAMES BLADEL: To echo some of the points that have been made on the list as well, I think that the case needs to be made why these particular registrations are subject to a higher standard. Because someone has requested or shown an interest in what is essentially an unlisted telephone number on the Internet, does that warrant additional scrutiny? Who are we trying to catch? That would be my biggest question.

As a separate aside thing, we've got about three months now on this verification thing, and I can tell you, let's not be in a hurry to hitch our wagons or even exceed what we're seeing. This thing is kind of a mess. We've got our famous [Taz? 00:23:47] glitch. If you're familiar with the US there was a healthcare glitch. We're trying to prevent this from being an RAA glitch, but there are some high profile false positives happening.

So I think from a registrar perspective we get very nervous when folks say, "Let's take that thing that isn't working and amplify it and expand on it." I think that a dose of caution and maybe some conservative hesitation is warranted in that regard as well. So those two things. Let's make sure this thing works before we decide we need to eclipse it, and then let's really understand why we believe that these are inherently suspicious names.

HOLLY RAICHE: Thanks James. I think we'll introduce Carlton's speakers, and then we'll just have an all-in discussion, because I can see some people in seats are getting a little bit tense.

CARLTON SAMUELS: And time is going. Thank you Holly. Good afternoon everybody. My name is Carlton Samuels. I'm a member of the EWG looking at the next generation of registration data services. We're struggling with this issue. We've been working very amicably together for almost 18 months looking at what we might propose for policy development, with respect to registration data services, and at the same time try to grapple with some of the issues that exist today. When we started this we figured we might as well look at both groups and have some perspectives from the EWG about what we are seeing in the group.

So it's with great pleasure I introduce to you some of the members of the group. It's a small subset of the group here. Michele Neylon, most of you know him very well. He's probably At-Large's favorite registrar. I'll tell you why he is, because he shows up and he interacts when we ask him to, so that makes him a good guy for us. Stephanie Perrin. Stephanie is a privacy expert and she's Canadian. Rod Rasmussen is around here. Rod is in security, and he has a business on the west coast of the United States providing online security services.

We have Fabricio Vayra. Fab just arrived. Welcome Fab, come and take a seat. Fab is a lawyer, mostly dealing with IP issues. In the group he's the guy who always say, "So let me see if I understand this," which means he's going to start an argument.

MICHELE NEYLON: Carlton, in fairness, we don't argue, we debate and discuss vigorously.

CARLTON SAMUELS: I stand corrected, Michele. We debate and we discuss vigorously. So the question for us, that we thought would be interesting to address with this group, was you hear the questions Holly asked at the beginning about the privacy proxy services, and this is one of the core issues in the EWG. We thought we'd ask my colleagues to come here and give their perspectives on what is happening in the EWG with the entire registration data services; the major issues that we're contending with, and especially with the privacy proxy issue.

So, without more to say, can I ask Stephanie to give us her impressions and perspectives on registration data? Stephanie, you have the floor.

STEPHANIE PERRIN: Thank you very much Carlton. I must say it was Michele who talked me into joining the Privacy Proxy Services Accreditation Working Group. I'm sure I've got that in the wrong order. So Michele is to blame for the fact that I've been engaged in some vigorous discussion there. I must say, coming into ICANN as someone who's been working in data protection at the nitty-gritty level for 30 years, I'm struck by a number of things. In the absence of comprehensive risk management, it does seem like the mitigation to all problems is more data.

People don't seem to have a heightened appreciation that that's personal data in many cases, and it's competitive data in some cases. I've even tried to get the topic of Competition Policy onto the PPSI Working Group because it seems to me it's perfectly legitimate for a small business to want to use privacy proxy services and to have their data protected. That's one of their risk mitigations. So I find a lot of the calls for disclosure anti-competitive, as well as many other things, besides being anti-privacy.

Did you want to me to run over the three mian things we've done in the EWG, Carlton? Okay. I think there are three basic major blocks that of privacy improvements that we're seeking in the new WHOIS. One is that the access would be based on purpose, and that's a fundamental in data protection regimes, that people don't get access to data unless they have a legitimate purpose. So that means you have to accredit the person coming in and verify their purpose.

So it's not a country club license, where you get in the door if you're in this or that group. Even if you're law enforcement you still have to have a legitimate purpose for each one of these things. Obviously there will be complications when we're talking about some of the services that involve data analysis and large sets of data, but that's something we're probably going to have to work on.

We're looking for controls at the other end, such as audit controls that will also help keep an eye on who's coming in, and whether they're in fact living up to the terms and conditions to how they were granted access. I think I'm speaking too quickly for the translators, am I? I'll slow down a wee bit. The second… They're all major moves forward, but the second one would be we are proposing an enhanced secure credentials using cryptographic credentials to basically allow anonymous domain name registration.

This is for the kind of groups that Kathy was alluding to in her remarks; folks who have a genuine and proven need, not just to have the kind of anonymous registration that a privacy proxy service can give them, but the kind of security to know that even if their pursuers – be they an ex-spouse, a government that won the election when they didn't or whatever – when they show up at the door of the registrar threatening to take the servers, that can't happen.

That requires quite a bit of leg-work in terms of setting up the procedures, processes and accreditation regime, but it would solve a fundamental human rights problem and free-speech problem that's been around for many, many years. I serve on another advisory board for one of the European post-prime projects, where they're testing the credentials. It's not the technology that's the problem here. The technology's been proven. It's how do you implement the procedures, which are quite complicated and nobody's really done them.

So I think this is a great initiative for ICANN to move on. Now, what was our third one? Oh yes, how could I be repressing this concept? That is, because of the jurisdictional issues around the world where ICANN is operating, we are proposing – if you've had the opportunity to read the report that came out just before Buenos Aires – a variant, some form of binding corporate rules. Those companies that have already signed onto safe harbor will understand the concept. ICANN is not eligible for safe harbor because it's a not-for-profit. They don't really quite fit the mold of binding corporate rules either.

That's basically where an organization that's active internationally, and wishes to transfer data internationally, sets a policy, gets it vetted, gets it approved as meeting a level of data protection law, that's normally resident in the European community, and gets it blessed. They then do not have to go through further procedures for the data transfer globally within the corporation. Now, we would have to tweak that to fit the ICANN model, but in any case, the starting blocks for this – and I see this as quite a long process, because you're starting from zero – would be a privacy policy, which most companies are quite familiar with, because at least most American companies have developed privacy policies by now.

So ICANN doesn't have one. Michele and I argue over whether in fact, under the European regime, ICANN is a data processor or a data controller. I'm right. They're a data controller. [laughter] Meeting adjourned, that's right. Basically because – if you doubt me I'll send you the links to the European community's explanatory documents…

MICHELE NEYLON: Stephanie, you did convince me, it's fine.

STEPHANIE PERRIN: Oh good. Put that in the minutes. The data controller sets policy, and even though ICANN doesn't have the personal data the registrars do, and the proxy service providers do, we set the policy, so that makes us data controllers. So they're the three basic blocks, and I'd be happy to answer any questions.

CARLTON SAMUELS: Thank you Steph. Michele, Sir, tell me what you're thinking.

MICHELE NEYLON: [laughs] Michele Neylon, CEO and founder of Blacknight, currently Chair of the Registrar Stakeholder Group, Chair of the .eu Registrar Advisory Board, member of the EWG and various other things. I'm probably speaking in my own capacity because nobody else would support me. I suppose in many respects, when I first started getting involved in the circus that is ICANN, it was in some respects via... As a European I've always had issues with how ICANN handles privacy and how ICANN handles WHOIS.

Most country codes have resolved this. It's not something that causes headaches in the country code space, it's just done and dealt with. Huge amounts of personal data aren't just published to the world. Law enforcement doesn't seem to be having conniptions over this. I don't see any country code managers going into the ccNSO to whinge and whine about how trademark attorneys are getting very upset with them. So it's not like there's some massive problem if you have a regime that protects privacy.

So why on earth is ICANN being special about this? This is just my general view. Within the EWG we've been looking at a whole range of different aspects of domain registration data. Just to give you all a bit of background, for those of you who aren't Kathy Kleimans, who read every single report ever written on WHOIS and send us copious notes pointing out all our errors… Yes Kathy, we did ask you for comments. One of the things… When you talk about WHOIS within the ICANN spaces, everybody ducks under the tables, has nasty flashbacks to previous WHOIS-related efforts, and it's this massive thing that you can't really talk about.

With EWG we tried to work on the basis that everything that had come before should be put to one side, almost, and just to start from scratch; answering the questions that people had stopped asking. What is the point behind this? Why are we doing this? Why do you need this? What does each day's element do? So at the simplest level, in order for a domain name to resolve on the Internet, what data elements do you need? Don't all rush at the same time to answer that. You all seem to know the answer.

Building up from that, what are the other elements that you might need? What are the other elements that could be expected? Then when you're looking at different things like… This goes back to purpose. It frames the entire discussion very firmly within a framework that's compatible with privacy law in Europe and elsewhere, where you take purpose into consideration at every single step. That doesn't mean that the trademark attorney that wants to reach the infringer that their purpose isn't ignored. It is considered.

It doesn't mean that we wouldn’t consider the purpose being to blatantly infringe a trademark. We consider that to be a bad purpose, but we did look at it. Coming from that side of things, we’ll put together something that hopefully will be finalized for the London meeting. You’ll all probably hate it and rip it to shreds, but it will be quite robust and it should have some clear recommendations, which hopefully will lead to an improvement of the overall system.

But just to back up, Stephanie, ICANN does really need to address privacy. It needs to do something about it now. It needs to do something clear and consistent. It needs to put in place a regime where the burden of dealing with privacy doesn’t fall on the registrars or registries; that the corporate body is not trying to force legislation via contract.

CARLTON SAMUELS: Thank you Michele. Before we go to Fab, I’m going to give Holly a minute here to say something.

HOLLY RAICHE: For the one and a half persons in the room who don’t know, the RAA in Section 3.7.73 requires a range of WHOIS data, which includes things like names, contact details, for the registrant, to be public. That was probably put in there a long time ago for reasons unknown, but it’s caused a range of expectations for the people who would like to access that information to be very happy, and it’s caused a range of difficulties who don’t want it to. So we’re dealing with something that’s been there for a long time, that's caused both great pain and great glee. We're trying to figure out if we can do it better.

CARLTON SAMUELS: This has been a real problem. I'd like to recognize our colleague Rod Rasmussen, who's here. Rod is down at the end of the table. Rod, we'll come to you right after we have Fab.

FABRICIO VAYRA: You know better than to just leave it open-ended. Is there anything specifically you want me to speak about, or just my thoughts?

CARLTON SAMUELS: Let's start with your perspective of what the work of the EWG is, the specific things that you think are important.

FABRICIO VAYRA: I'm Fabricio Vayra. As Carlton pointed out, I'm an attorney, which seems to be the moniker I carry around ICANN. To help all those who would like to stop calling me an attorney, I'm also a dad, a sailor, a musician and occasionally I like to drive racecars, but that's another thing. So any time anyone would like to pick up one of those monikers and attach it to me, aside from "attorney", which I wear proudly, feel free. My perspective on all this, look, I think everyone came into this with the promise that we would be done in three months.

Here we are a year and a half later. If you see what the dates were of what we were originally do… I think it's a real testament to the group that we didn't really rush to meet that three months. I think that Stephanie has done a fantastic job as well as, as you heard Michele, as well as everyone else in the group to bring in their expertize and really highlight and table all of the issues. I think that everybody within our group should be, if they're not, very proud of the fact that they've taken this extra time.

In the movie industry we do credits a lot of times, and we know things like, especially in the animation, they always put how many babies were born during the production, because it takes so long. I feel like we might have to do that here, because we've had babies, we've had family deaths, we've had a lot of things, and the team keeps going. We do so so that we constantly make sure that we, if nothing else, appreciate what it is that everyone's bringing to the table. I actually think people go beyond appreciation. They actually go to try to understand.

That doesn't mean we don't bicker. It doesn't mean that we don't disagree at times, but we've really produced, up until now, something that I think if you look at it shows a real honest and earnest attempt, as Holly put, to get it right and do something better. We really are trying to do something better. No one's coming wearing the badge or shield they associate with. They're coming in and bring in an expertize to try and do something better. The reason we weren't done last year was because I think we looked at this report and continued to say, "We can still do something better."

The reason we know that is because you are, as a community, not just those in this room but those outside this room, took the time to tell us what they thought we could do better. We took that honestly and genuinely and decided, “We’ll devote another six months of our lives to this.” We could have just easily thrown in the flag, and everyone would have said, “It’s what we expected,” or, “What we didn’t,” etcetera. We keep trying to do something better.

I think the community at this point really wants something from us, so we’ve set a hard date by which we’re going to deliver something. I know that something will be better than what we would have delivered, back in November. I definitely know it’s going to be a system that’s going to be much better than you have today. I mean that from everyone’s perspective. I agree with Michele that people are going to be upset, but I think that’s a sign of true compromise and better.

Because from my perspective I’m sure there’s plenty of things that my IP colleagues are going to wonder, “How did that happen? Why did I have to do XYZ to get data?” But there’s a balance, and I think we can look at things as an 80/20 rule. You’re going to hopefully gain 80% for the 20% that you’re upset about, and I plead to everybody here that when you see the report, remember it’s the true, honest attempt by a lot of knowledgeable people who’ve struggled with each other for a year and a half to do better.

In so doing, please focus on the 80% that you’re gaining, and not on the 20%, 15% or 10% that you might be giving up, because that’s really nominal and you shouldn’t look at it that way. This system really should be better, and for the topics I believe you’re all interested in that you’ve heard Stephanie and Michele talk about, I think it’s massive leaps forward, and for good reason. It’s something that’s needed. Hopefully we do come through and get close to right.

Those are my thoughts and at the end of the day I have to say despite what anyone says, I'm very proud of this group for working as hard as it has, and truly trying to understand each other to do better. Holly, we really are trying to get it right and do better.

CARLTON SAMUELS: Thank you Fab. Rod, you have the floor, Sir.

ROD RASMUSSEN: Just general thoughts and observations about the EWG, or…? Actually, coming into it, I echo what my colleagues have said about trying to do better. I believe wholeheartedly the initial assessment that kicked off the EWG, which was that the WHOIS is fundamentally broken, and this will work for anybody. Everybody is unhappy with it as it currently exists. We know from other examples in the world that we can do a better job, but there are competing interests. How do we do things, and how do we do them in scale?

At the end of the day, the reason I was like, "Okay, I'm going to do this," is really not about representing security or law enforcement or that aspect of things, which is the hat I wear coming in, so to speak. It's not really what I wear when I'm there, but I have that expertize. It's really about how do we make the Internet actually scale and work on a long-term basis, so that people trust it? If people are going to do commerce, if people are going to communicate and do all these things about it, part of that is actually getting this right when it comes to the allocation of these resources and the responsibility, accountability, etcetera.

All those things that ICANN has as its AOC, how do we scale that to everybody who's using the Internet as well? I look at it as not just being an AOC for ICANN – that represents a community that represents all of us – we're using it; both publishing things in it and bringing things out of it. So knowing that we were going to tackle that problem, I've seen what I would consider a downward spiral in the trust and how the domain name system is being allocated. We've been patching it. From the security side we've been covering over things to protect users from things that are happening out there.

So how do we address that? My observation of the group itself is that it's been a tremendous learning experience, for everybody on the group. I think we've all learned a great deal from each other, and know far more now about privacy law, about registry operations, about everything there is that everybody has brought to the table. I think everybody else has taken that as well. I brought to the table my expertize and how people are abusing the Internet and how people are abusing the registration system in order to perpetuate things that people may not have been aware of, or when you start thinking about it's like, "I want to protect privacy."

Well, one of the worst things for privacy protection is identity theft that's being done by botnets. So there's this whole balance of things. I think we've all learnt from each other and really done a pretty good job at saying, "Okay, I get that. Here's what we need to do to take care of these aspects and interests and concerns." How do we do that, and then do it in a way that's fair, equitable, scalable, and at the end of the day can be put into automation. This whole thing is a system. It has to be supported by computer servers and then around that, a supporting bunch of people that are making the processes happen.

Around that is a whole framework of laws, contracts and policies that all get intermixed. You have to balance those things. I don't know how many man months of our own person months we've sat through, learning, I'd love that the rest of the community could learn what we've learnt as a result. They'd have a much better appreciation for all of the angles and challenges they all face. Then it becomes much easier to say, "Okay, we need to do something and here are various ways we can do it." That's my overall thinking on it.

CARLTON SAMUELS: Thank you Rod. We're looking at bridging this. We have folks here who've been actively involved in the PPSAI Working Group and we're keen to understand how the work that's been done, and the conversations, and the PPSAI might bridge and flow into the EWG. I wondered, James, if you had any ideas about that?

JAMES BLADEL: My idea would be – and I hate to put here on the spot, but I'm hoping that Stephanie can keep us sane and on track in that regard. I don't have a lot of visibility into what's going on in the EWG. I wish I had. One question about the EWG proposal that I hope they're taking a look at is the idea that a search on the directory is a two-way search. The analogy I use is I have a Facebook account. I don't know who's looking at my Facebook page.

I have a LinkedIn account and LinkedIn sends me an email account every week with, "Here are the people who've looked at your LinkedIn account," and I wonder if that's something that's a consideration in the EWG.

STEPHANIE PERRIN: We certainly want audit trails on who is getting into the RDS central to access things. Obviously we're going to have a discussion with law enforcement because when they're doing investigations the very idea of an audit trail is an [inaudible 00:53:39] to them. So those are going to be difficult discussions, but it's possible to build disappearing trails too. Being a non-techie I have tremendous faith in technology being able to solve these problems, possibly at great cost but that's the idea.

MICHELE NEYLON: Basically what Stephanie's saying is if the ICANN budget is inflated by about 40% next year it's all her fault.

CARLTON SAMUELS: Okay. Michele?

MICHELE NEYLON: I think Stephanie did cover it, in fairness. There's one thing that I think nobody did mention but I think is key to mention – that we are making recommendations that are completely non-binding to go to the ICANN Board. They get fed back into a policy process, or probably multiple policy processes, you all get to be involved with. Don't, for God's sake, think that any of our output is going to be *the* answer. It should be a very well-educated suggestion, but it's not an ultimatum.

JAMES BLADEL: But to answer your direct question, Carlton, I guess from what I'm hearing there is there's a pretty huge gulf between the work of the EWG and the PPSAI. They're up here in the penthouse looking at principles, and we are focused, I believe, on a specific subset of those principles. If they're re-engineering the entire data system, we're looking at, within the context of the existing data structure, an existing commercial service. So I think we're looking at that issue a little bit through a pinhole camera. I hope we're aligned with their principles.

HOLLY RAICHE: James, I think that was my next question, which is hopefully those are the discussions in the PPWG, because some of those discussions are about access, about what you do about people who don't want to be accessed, and what do you mean about "legitimate reasons" and "legitimate requests for access"? Some OF those, to me, are higher-level questions as well as immediate questions. But Kathy was next, I think.

KATHY KLEIMAN: Thank you. It's interesting – we had this issue with the WHOIS Review Team as well, that we were studying a system that was moving while we were trying to study it. Unlike the EWG we were supposed to study the WHOIS system as it is, not think about it anew. I'm somewhat jealous of the blank-slate approach. Yet there were Working Groups going on at the same time and it was hard.

Here I think we have to be very careful as the EWG results come back in, that we don't block out what the PPSAI Working Group is doing, but we find some way at the end of the day maybe to merge or meld or figure out the best parts of each, and bring them together to the gNSO, for the next steps and PDPs that will follow. That's my thought – that we don't block out anything but take the best elements. Thank you.

CARLTON SAMUELS: We only have about 25 minutes left, and I wondered whether or not we could have some questions from other members in the room. Alan, then Evan.

ALAN GREENBERG: Thank you very much. Three questions or comments all related to privacy proxy. It strikes me as I listen to people here on what's going on in the EWG, is depending on what comes out of that process, the need for privacy proxy services may be far lessened, and to the extent that they're still needed, the details may be very different. So I'm almost worried that we're going to build a complex privacy proxy accreditation process, which a year later won't be needed in that form. I do have two more questions, as long as you come back to me.

CARLTON SAMUELS: Jump in?

[KATHY KLEIMAN]:

[00:58:32] We actually had a little discussion on that on the list, with a small subset of the list. I actually think the need and appetite for privacy proxy services is going to go up, because even if you applied data protection law in a systematic way, which I would suggest we don't, and even if you got the secure credentials for the people who are at risk, that's a pretty small subset. You still have small business, you still have the hugely expanding number of…

Well, we saw the award this morning in the opening ceremony for the women who were working from home. They would want privacy proxy services, I would suggest, and they're running a business so they're selling. So there's aspect of it. The other thing is that the privacy proxy service, I'm learning as I go along, offers a buffer as well as protection. You have a lot of people who might want to contact you that you might not want to be bothered with. I put up my hand for that.

I have a small business, and I don't want to be bothered. I keep telling Michele I'm going to register it in Ireland so that I can get out of this. But all kidding aside, that's a valuable service, and the privacy proxy services can fill that gap.

ALAN GREENBERG:

I wasn't making a strong statement, I was just observing that the need may differ. The second one is – and it's been mentioned earlier – there are an awful lot of lawyers in the world who, on behalf of their clients, register domains and are effectively acting as a proxy service. Do we really expect each of them to be accredited by ICANN before they offer that service on behalf of their clients? Is that a realistic expectation?

[JAMES BLADEL]: [01:00:30] That's an excellent question. It is something that has come up, Alan, particularly when you consider from the registrar perspective that we cannot knowingly accept registrations from an unaffiliated or unaccredited proxy service. If, for example, we contact a registrant and say, "We have a problem with this domain name, there's a court order," and the law firm say, "I'll contact my client." Well, we have to take a look at that entire account really. Under the RAA, it's not a question of we don't have a lot of discretion there.

It says essentially that here's someone who's acting on behalf of third parties, who are not known to us and who have executed our registration agreement. I think it's an interesting question. I don't know what the expectation is, but I know that the expectation is on registrars that we would not accept registrations from those firms if they were acting as a proxy service.

ALAN GREENBERG: Certainly if a lawyer registers a company in their own name, they take responsibility for what that company is doing. I would have thought that an unaccredited lawyer who's registering something is simply doing it in their name and they take full responsibility for whatever happens as a result of it. Therefore it's not an arms-length proxy, it's just doing it. My last question is something that struck me as curious. I may have the facts wrong but I've been assured by a number of people that I don't.

If you file a UDRP and the proxy service reveals who you are, that gets published in the result, even if the UDRP is found for the registrant, and even if it's a completely frivolous URDP. Therefore, if you want to find out who someone is just file a UDRP. If you can afford that then you've gotten it revealed, and the UDRP providers are required to file a report. So unless the privacy proxy service says, "It's me, I'm taking full responsibility for any action," then it gets revealed. I've never heard anyone worrying about that or complaining about it.

CARLTON SAMUELS: I am not sure I know of that. That is what exists today. We've had some discussions in the EWG about purpose… The discussion we had yesterday had something to do with UDRP revelations. Do you remember?

[KATHY KLEIMAN?]: [01:03:12]. No, I don't think we went to UDRP. That seems to me that's something that ought to be settled in the privacy proxy services accreditation.

CARLTON SAMUELS: Were we talking about accreditation?

ALAN GREENBERG: Currently that is part of the UDRP rules, which are due to be reviewed some time in the future.

JAMES BLADEL: One of the reasons why that can get slippery, Alan, is that not all UDRP providers have exactly the same processes for that, in their supplemental rules. It's not just UDRP issue or a privacy proxy issue, it's also a bit of a provider rules issue as well.

ALAN GREENBERG: It's one of the issues that came up on the [lock-in? 01:03:53] PDP, and I'm reasonably sure this is consistent among them, but I may be wrong.

CARLTON SAMUELS: The requirement that publishes is consistent. That's how we know it came up. Kathy and then we'll come back to Rod.

KATHY KLEIMAN: I just wanted to comment, Alan, that you're pointing out something that's a really good point. When we drafted the UDRP it was long before the evolution of proxy privacy service providers, so this is one that I'm looking forward to returning to, because the issue of frivolous or harassing reveals is one that attorneys who work in defense of registrants see all the time. So we've got to plug that hole up. Thank you.

CARLTON SAMUELS: Rod?

ROD RASMUSSEN: In general, to take this up a level with EWG versus any other of the policy groups that are working on various things, there's a lot of things, a list of four or five, at least, open policy groups around things that touch WHOIS right now. We're trying very hard to create a framework and offer good suggestions for going forward in the overall space – some very specific model things, and the things you'll see in the final report. Some of them will hopefully address this issue.

But in general, the PDPs are going on all that other policy work that's very specific and focused. We're trying to build the framework knowing that those are going on, so that we can provide a way that that will evolve into whatever we're coming out with, as an overall framework, for the most part. I would say, with particularly the PDP one, keep working on that. We don't want to provide a prescriptive way of how that's going to work.

We are very well aware that that needs to be addressed, and we're having some of those discussions within the group, but at the end of the day we're going to end up with a framework within which, whatever the policy recommendations, for the most part, that come out of that group will fit into that. So I think that's important to keep in mind. We're not trying to solve all the problems that all the other PDPs are looking at right now. There's a bunch of other ones right now – too many to list.

I think though, there are some concepts that we're just discussing, that I think will help very much in this particular arena around making legal contact with a domain. I'm not saying a domain owner, but the actual idea of a domain and the entity around being able to provide purpose-driven ways that people can solve those kinds of issues without necessarily revealing the registrant or some other, un-affiliated, not needed for the purpose, type of contact.

CARLTON SAMUELS: Thank you. Can I have Evan next?

EVAN LEIBOVITCH: Thanks. This is Evan Leibovitch, a member of ALAC. My question, I guess, to the members of the Working Group is in the form of a "are you satisfied that?" and there are two specific cases. One is a general form of, "Are you satisfied that as this is all implemented, that the issue of incorrect contact information is going to go away?" That is, this is one of the things that at least from the point of view of At-Large, or people I've spoken to, ends up becoming a real problem that privacy was implemented by giving wrong information.

Hopefully, now that you're putting in these privacy proxy services, this is going to make it easier for somebody to have a level of anonymity while providing correct contact information. Does that mean that at the end of this that what remains, that those will continue to have incorrect WHOIS information will be breaches that can be acted up on by law enforcement or whoever? That incorrect WHOIS information will no longer be something that will be tolerated.

The other "are you satisfied?" question is that something that I thought was going to be a theoretical question, but turns out is not, and touches on both the brand protection and the consumer speech protection. That is, in the case of TLDs such as .sucks and .wtf and so on – which a couple of years ago in Brussels I thought was going to be a joke, but it turns out both of these are legitimate applications…

Now, you can have, conceivably, registrations under domains like these, that could be shake-down attempts on brand owners. But they could just as easily be protected speech from consumers or trade unions or whoever. Does the services as you're anticipating allow for properly being able to go after those that are doing it as a shakedown, while at the same time providing the protection to those that legitimately need it? Thanks.

HOLLY RAICHE: That's scary. I'm not even going to go there, because James is actually going to put his hand up to answer the first part of it, the first part of that. Actually, one of the discussions, Evan – and I'm still thinking about this – is a choice between do you reveal the information, which will have been verified under a process, but then at the end of the day, what happens when the next day somebody changes something? You're not going to know about it until you try to contact them. You don't contact them.

That could be a [while down? 01:09:36], but are we saying you check every name every day, so there's always going to be an opportunity? Yes, people will pass the test. They'll pass all the verification tests, then they change something. Now, I don't know how you deal with that because honestly that's difficult. The next part that you take a deep breath, if you are put on notice that there's a problem, and you go through the verification and it really is a problem, is it okay to say:

"Okay, this is incorrect. I'm not going to reveal the information but I'm just going to shut this down completely"? We're still thinking about it. That's a viable… You've said to somebody, "We're not going to reveal your information that protects, in many cases, somebody that wants protecting," perhaps unduly protects somebody that doesn't deserve it, but at the same time you've just taken them off the net. That's honestly a question rather than an answer. You want to say something?

JAMES BLADEL: I'd love to respond to the first part of your question Evan. I think in some respects we can de-couple the problem of invalid or incomplete WHOIS data from the privacy proxy issue. It really applies just generally to WHOIS. I'd love to see the EWG's position on some of these issues. In my mind you can drop these into buckets. There's invalid WHOIS because of an error, typo, or somebody left something off. There's invalid WHOIS, let's call it benign:

"Oh, you're going to put my phone number on the Internet? Well then it's 1234 567. Wow, it took it. I'll make it up or I'll give them the phone number for the phone booth down the street because I don't want my phone number on the Internet." Then maybe there are more malicious uses, where someone is actually trying to evade because their intentions are to do bad things. I'm sure the EWG has looked at this issue, and I know that we've referenced some interesting studies coming out of country codes.

If you can demonstrate that the information is trusted and protected, that the benign invalid WHOIS, the people were just doing it because they don't want to be hassled, bothered or spammed, probably can be cut down over time. The bad people… I'm sure Rod and some of the folks who work in security can understand that they're operating much faster than ICANN policy. Most things are, except for geological processes. But they are going to stay one step ahead of whatever filters we put in front of them.

We need to keep making it a hostile environment to that practice. I believe that over time this will diverge into… The benign stuff will start to come into the fold and become more accurate and become more valid. The truly malicious bit will start to trend towards legitimate stolen data. We'll see data that passes every test and data that fits every data. It's just not their data, it's someone else's. It's someone's stolen credit card or address.

But I think that we can say to a great extent that this is not always on the critical path for this Working Group. It's more just a general trend. I think the 2013 RAA and subsequent work in this area will probably improve that more than the PPSAI.

SPEAKER: [01:13:47] Just to address Evan's query, I think one of the things that we've been looking at within the EWG is the concept of accountability. Accountability, responsibility that somebody has to be accountable or responsible – depending on which way you want to look at it – for everything. So if you register a domain name, maybe you aren't that technical, but someone who might do work for you probably is. The idea of getting somebody as a contact… The thing is this:

You're looking for somebody who will respond, probably, more than anything else. I can send you junk mail, Evan, using carrier pigeons if I wish, and there's absolutely no way on this earth that I can oblige you to respond. There's no way I could do that. One of the issues we've all seen on our side in industry is people assuming a lack of response equals an issue, when it doesn't. What the Specification in the 2013 RAA has, and what I'd assume the PPSAI comes out with, and what is definitely within the EWG's initial recommendations, is this:

The provider of a proxy or privacy or whatever, that provider would be obliged to respond. For example, in the example of a trademark-type issue – let's say you're talking about the shakedown concept – sure, maybe they could put themselves behind some privacy proxy servers, but that isn't going to mean that he can't go after them if he wants to. It's this accountability type thing. The other thing as well is, I would caution you all to please stop treating WHOIS as a proxy for remedying all the world's problems.

How many of you in here have moved house at some point in the last ten years? How many of you in here have traveled…? Here's a nice tangible example for you: how many of you here go to ICANN meetings and pick up local SIM cards? The reality is that contact details update and change. If you take an overly prescriptive, overly binary, everything's black and white type approach to it, then I think it's the wrong approach.

Now, if you want to have a look at something that's a much more interesting approach, have a look at the securedomain.org. It's a Canadian thing that was officially launched this morning. There are those of us in industry who share the same concerns, we just approach things slightly differently. Thanks.

CARLTON SAMUELS: Thank you. Maria, you have the floor.

MARIA FARRELL: Thank you. My name is Maria Farrell. I'm a gNSO Councilor for the NCSG. I'm also an Internet user, and I'd like to express a point of view that I don't often actually hear coming out of the At-Large, and that is as an Internet user, who does not want to have my personal data published in the WHOIS? As a result going forward, I'm pretty much only going to register in cc's. I'm one of Michele's customers but I'm dropping my .com, I don't use it.

MICHELE NEYLON: Thank you Maria, I appreciate your money.

MARIA FARRELL: Money well spent. But here's the deal – I write on a relatively high traffic blog. It's a group blog. We get about 25,000 unique readers every day, and I can tell you right now, if I write a post this evening or tomorrow morning about feminism or about a topical issue in US politics, I will probably have about half a dozen rape threats by the end of the week. That's not unusual. Why is that?

There's a whole larger issue about women on the Internet that is coming out, and our users won't see that on our website because when I write one of those posts, typically what we do is that we moderate the comments so that first time users – it's usually a first time reader who makes this sort of threat – we put them into auto-moderation and the guys who write on the blog will go and monitor the comments for a few days and I won't. I don't see that, because they can be pretty graphic and they can be pretty specific.

Why do I not want to register and put my name, address, telephone number and email on the internet? That's why. That's not unusual. I don't have a particular reason for wanting to pre-register as having a special… I'm not running a women's shelter, I'm not an NGO in some oppressive regime – although those are definitely good reasons. I'm basically a woman who has a domain name, a laptop and an opinion. [applause]

Anyway, there you go. Anyway, I just wanted to get that there because there's also an argument that I often hear, which is that a domain name is a privilege and if you don't want to have a domain name, if you're not prepared to give up your personal data you shouldn't be able to have a domain name. I think there's a lot of assumed privilege that goes behind that argument, and that does not imagine that the world would be so different if you're just a woman writing crap on the Internet.

So we have .com's and those kind of names, because we want to host our own names and make sure that they work, and we don't want a proprietary platform that's going to pack up all our data if we want to move. That's just what I want to say as an Internet user. I really do feel quite strongly about this issue, and I'm not exceptional in my situation.

CARLTON SAMUELS: Thank you. We'll come to that gentleman down there, and then Fab will have a last word. We have five more minutes folks. Please keep it brief, thank you.

[KT HANG?]: Thank you very much Mr. Chairman. My name is [KT Hang? 01:19:52]. I'm from IFPI and I'm here also representing the RIAA. I think we understand that some points that have been made, especially as the private user who wants to keep privacy of information goes, as far as our industry is concerned, our main point is to have validation of the information. As you know, when we finally can track it down, and these people are hiding behind all these addresses, we cannot get to the people who are doing very bad things online.

I just came from another meeting at the Ministry of Law. The industry in Singapore is basically decimated, there is no industry left. It's less than S$20 million left. That's the size of the industry. We cannot get to the people who are putting all our works available for free online. We understand your concern. We understand the point you make, but I think we're just asking that in this process, if you could take that into consideration, for us to have some valid information.

If the information is changed for whatever reason… It's just changing my address. Nobody's going to come up to me. But if I'm using it in order to hide and do illegal activities, I think it's imperative that the system must allow us to get around that, or at least to validate, to shut it down, as has been said, so that our interests are also better attended to. Thank you.

CARLTON SAMUELS: Thank you very much. Fab, I think you'll have the last word.

FABRICIO VAYRA: Thank you Carlton. I'm so happy that you two both went back to back. Maria, thank you in particular for telling the story you just did, and recounting what you go through. I obviously, as an IP attorney by trade, live your life. But as an IP attorney by trade, I've often worked with women who've had to pull their bios down from the firm websites, because in response to ceasing the [sis? 01:22:00] letters to stop people from doing bad things, you'd be surprised how people come out of the woodwork and start sending very graphic, threatening emails, like the ones you described.

All for something that you would think it pretty benign and shouldn't illicit that response. It's baffled me for years, but I think that both of you sitting side by side and bringing up what you bring up… A great example; something I've lived through and highlights why we're fighting so hard to hopefully satisfy both of those needs… Evan, to your point, are we satisfied with certain results? I can't say because of what Rod and Michele pointed out, that we're giving recommendations.

So I can't really spite the football and claim a touchdown and say that I'm going to be satisfied with the end result, because I don't know where that's going to end up. The community still has its final say. But I am satisfied that we, within our group, have brought these experiences to the table, and we are definitely trying to create an atmosphere that resolves both of these. An atmosphere where people actually feel comfortable that by being on the Internet, and using a domain name, and expressing an opinion, you can feel safe.

Without some sort of accountability, responsibility and vetting, your personal information is not just out there. That I can be very satisfied in saying today that we are trying very hard. Once that person is vetted and once that person's purpose is revealed, etcetera, and there is real accountability to the requestor, like the RIAA, that they then can feel, because of the atmosphere that we've built, genuinely honest and free to put in their real information. They can do legitimate investigations.

So we really are trying to balance it. Both of these issues have actually been brought up in the past three days of our deliberation, so thank you guys for what you've said, because I think you reaffirm what we're trying so hard to set up. Thank you.

HOLLY RAICHE: I'm going to just cut the discussion right now, because the EWG has a meeting coming up. I'd like to thank everybody for a really interesting discussion. Obviously the issues are very live, and they are unresolved, or they're on their way to resolution. But it's been a very interesting discussion. I'd like to say for those who'd like to hang around, we're having a session at 17:00 on TOR, but you can leave EWG and come back!

But thank you everyone. It's been a terrific session, and thank you particularly to the… Thank you Steve, James, Stephanie, Kathy, Ron, Michele, Fabricio. I think that's everybody. I will see some of you in the Working Group.

SPEAKER: Excuse me, Holly, there's a question on the…

HOLLY RAICHE: Sorry. Everybody just hang on one minute. It might be the real Steve. Thank you everybody. Thank you interpreters as well.

[END OF TRANSCRIPTION]