LONDON – At-Large Policy Roundtable - Registrant Data; Existing Rules, Future Rules
Monday, June 23, 2014 – 10:30 to 11:30
ICANN – London, England

HOLLY RAICHE: First of all, thank you everyone for attending. This is the At-Large Policy Roundtable Registrant Data Existing Rules and Future Rules, on Monday, 23rd June from 10:30 until 12:30… It says 12:30, but then the other schedule doesn't say that, so we'll just keep going and hope nobody stops us. As soon as possible we will get the PowerPoints up so you can have a listen.

The issue is essentially about – and this is what I've explained in the PowerPoint… If you want to participate in this group, this is about both the privacy proxy server issue and the EWG Final Report. That's ICANN speak, unfortunately, and I apologize for that.

I'm going to do a very quick run down and background to bring everyone up to speed on what the issues are. We're very fortunate to have a number of people and a number of perspectives on this issue. James is looking very puzzled, but when he smiles he's going to give you some views on privacy proxy. Michele is not going to be able to help himself. Graham Bunton next, from the contracted parties side.

On my right I have Stephanie Perrin, who is also a part of our Working Group on EWG. Kathy seems to have left, but she'll be back. She's part of the group that's working on this issue. For those of you who have not followed this issue, pay attention to the presentation, which should be on the Adobe Connect. It's certainly before you.

The Agenda – we're actually starting off with the whole privacy proxy WHOIS issue, and then talking about the EWG – the Expert Working Group. For those who don't know what this is about, I thought that if they're going to join in the argument, they need to know what we're arguing about. If Ariel can't find these slides, we will. I'll find mine. I'm going to talk without slides, and hopefully they'll magically appear.

The issue of privacy proxy servers really starts probably several years ago, in terms of many years ago, when the Internet was populated by geeks, to find out who they were talking to there was an RFC as standard, that required that people had to identify themselves.

That was essentially built into the requirements that are now in the Registrars Accreditation Agreement, in terms of the information about the registrant must be made available, and publicly available, which makes sense when you've just got geeks on the line. It increasingly doesn't make sense when in fact we're talking about a much larger group of people, many of whom may not want their details made public.

They have a right not to have their information made public. We have a requirement within the RAA about publicly available information. It's called "WHOIS information". That will be made publicly available. In competition we have some fundamental rules on privacy, particularly in Europe, but certainly in the US, and a number of jurisdictions that say people have a right to privacy.

The discussions took place, resulting in the 2013 amendments to the RAA. Starting in 2013 the law enforcement agencies were very strong on their need to have access to WHOIS information. That is personal

information, contact details about the particular registrant. As a result of what they required, amendments were made to the 2013 RAA.

Also what happened in context was there was a WHOIS Policy Review Team. In its report it made several points. First of all that there are quite legitimate uses of the privacy proxy services, by individuals for their own personal reasons. By organizations such as religious, political, ethnic minority groups, companies who are working on upcoming merges and so forth.

The idea that people wanting to use privacy proxy services to shield from the public view data about the actual registrant, particularly contact data, the first thing that the Policy Review Team said in 2012 is that there are actually quite legitimate reasons why people use privacy proxy servers.

As they said, there are also some problematic uses of privacy proxy servers, some of whom are people who are criminals or are involved in some kind of misuse of the Internet in some way. There should be some information or some ability as to how to contact those people. The requirement in the 2013 RAA essentially – this is one of the bits of background – registrars must agree to comply with any ICANN-adopted specification.

What we as a Working Group – and there are Working Group Members here – were charged with doing was coming up with a Specification, which formed part of the changes in the 2013 RAA, that will set out rules for privacy proxy services, until such time the proxy accreditation program is established. I really noticed I don't understand why that's only for proxies. We're not going to worry about that.

Next slide. You don't want to read this, but as part of the Specification, just in case any of you are interested, there are definitions as to what is a privacy service, what is a proxy service, and since I want to hear from everybody else around the table I'm not going to go any further. I'll say these are defined terms. The privacy proxy provider or service provider is the provider of such services.

Now, this is the Specification that is part of the RAA, which will be binding as part of the 2013 RAA. It's pretty much a skeleton document as it is now, with some really basic requirements. The first is that registrars have to comply with the Specification that the actual terms of service must be published. There must be what's called an "abuse point of contact" and that's defined as a way to contact somebody with the ability to provide necessary information 24/7.

I won't go any further, but there has to be an abuse point of contact for third parties wanting to report abuse or infringement. Finally, in the Specification, a description of the process that has to be available on how abuse reports, etcetera, will be handled. That's what we've got now.

What the gNSO did in 2013 was establish a Working Group to develop the more detailed rules on what the Specification for privacy proxy services would be, starting with… I'm not going to go through all of the Terms of Reference, because there are about 20+ questions, but the Working Group has identified categories of issues arising out of developing some kind of Specification.

We have a thing called main issues. We have, under the next heading, the maintenance of privacy proxy services. What does that mean? How

are they registered? Should they be registered? What's meant by "contact points"? There's a section on the relay of complaints to the privacy proxy sectors. There's another whole section on the actual revealing of data about the registrant.

Then what happens in the case of an accredited privacy proxy service, if something goes wrong? That "if something goes wrong", we haven't defined that. We haven't defined a lot of issues. Now, the Working Group, in April 2014, released a paper for comment. Can I have the slide before that? I think I put out what the issues were. I didn't. Next slide.

In 2014 there was a paper that was put out by the Working Group, asking for comment. The At-Large Advisory Committee made comments. A summary of what the ALAC felt was that the requirements of privacy proxy services should apply to all providers. There was an issue about verification of the details of the registrants, who were using privacy proxy services, and what those verification requirements would be.

ALAC felt they should at least be the same as those requirements for verification of registrant details that are included in the 2013 RAA. We also said there needs to be a balance about legitimate rights of individuals and organizations to privacy, as well as the legitimate rights of the law enforcement agencies, and others, to contact information. Although, the way in which law enforcement agencies and others may get that information will be different.

The Working Group has actually spent a lot of time on a lot of working through the details as to what's going to be in the Specification. We've reached some provisional agreement, and I do say provisional

agreement, because we still have to, as a Working Group, reach final agreement. We have provisional agreement about, for accreditation purposes, we'd be treating privacy and proxy providers in the same way.

In domain name registrations involving… I can't read the whole sentence. I'll tell you what. What I want to do, instead of looking at… Go down. There are a couple of points that we have reached agreement on. I will say provisional and I would say majority. There are some difficulties with that, but most of us agreed that privacy and proxy providers should be open to both commercial and non-commercial entities on the same basis.

We've reached provisional agreement that ICANN should publish and maintain a publicly accessible list of all accredited privacy proxy providers; that registrars should provide a web link to the privacy proxy services that they run, that the verification of registrant details that is required under the 2013 RAA should be pretty much the same as that required under the Specification.

There are a lot of outstanding issues. Some of the major ones – and I'm sure that the people around the table will have other issues – but for some of them we have to work through what we mean by "accreditation". Presumably it will be ICANN. What tests will be used? What compliance arrangements need to be put in place? A lot of issues around accreditation. The responsiveness requirements.

What I mean by that is if there is a request for information about registrants, to a privacy or proxy provider, what do they have to do and in what timeframe? Again, that may be different as between law enforcement agencies and others. Then, in terms of the preservation of

anonymity in a transfer process, we have still to work through how that works, because we've got some issues about that. Can we go to some of the people who are involved in the Working Group?

Do I have another slide? Time's up. I'm not going to go through that. I'm going to say that in the Working Group there are people who are here to provide their own perspective, but also to have all of us listen to what questions all of you have in terms of what considerations and issues you have with privacy proxy services. The people who are Members of the Working Group… Steve Metalitz, put your hand up, from the IP community. James Bladel is here.

Michele's not going to talk until we get to the EWG. Michele will talk… [Laughter] Graham Bunton, who's also in the Working Group. Now, Stephanie isn't but he'd like to be? She is? Okay. Kathy also. I think I'm going to start with ladies first. If you want to highlight what your concerns are, we're going to quickly run around the table. We don't have a lot of time, although I notice there's this huge block of empty space after this group, where there's nothing scheduled, so we can run over.

Just a little bit of a "where you come from" perspective, Kathy and Stephanie, and then Graham and Michele and James and Steve. We'll probably have two minutes, because otherwise Carlton will beat me up. Kathy?

KATHY KLEIMAN: I wanted to thank Holly and Carlton for setting this up and inviting us, and also ALAC for inviting us to an ongoing discussion. It was very

valuable in Singapore. Thank you for the continuation. Holly, thank you for the introduction. That was very well organized. A lot of people know me here. I come from the Non-Commercial Users' Constituency. I'm an attorney that specializes in domain names, free speech, fair use trademark and privacy.

When I was with you in Singapore, we talked about starting points for the Proxy Privacy Accreditation Working Group, and I just wanted to quickly review the starting points, from a non-commercial users' perspective. That's that the Internet now has hundreds of millions of domain name registrants and many of them are speakers, using their domain names for personal views, political views, social views, and running the discussion for their communities and their countries.

This speech is incredible. This is one of the great things that the Internet has facilitated; these amazing international and local discussions, but finding people who share your views, finding people to debate them. From a proxy privacy perspective, as I look at it, we have to find a system that values these speakers and also recognizes that people want to find them. First that values the speakers and that traditionally we've valued speech more than the speaker.

There are certainly laws in the United States, rulings of the US Supreme Court, that talk about the value of anonymous speech, or even pseudonymous speech, so that the speaker doesn't have to put themselves out there, if they're doing something that's unpopular in their neighborhood or in their country. We think of Mark Twain and [Jord Sarnd 00:26:00]. Even Play Doh may have been a pseudonym.

This is interesting. There are a lot of places in the world that would prosecute and persecute people for their speech. Secondly, we talked about the disclosure of identity should require some due process. If you're going to disclose the speaker, have they done something illegal? This is something the PPAWG has made some good strides on, that proxy privacy services belong to everybody, because we feel that there are lots of legitimate uses. This seems to be something we're embracing and moving towards as consensus.

Then the third that we talked about last time was some room for creative remedies. Do you have to reveal the person, or can you take down their speech, rather than revealing them? Is there room for lots of different remedies? I have to say that I think the PPG is doing a great job. We meet every Tuesday. We spend a lot of time and effort. We go through each issue.

We're working through every issue, and I think that we're taking into account the principles that I raised in the last discussion. I appreciate that. I appreciate the efforts of everyone around the table in the Working Group. Thank you Holly.

HOLLY RAICHE: Thank you Kathy. Stephanie Perrin, who's also a Member of our Team?

STEPHANIE PERRIN: Yes, and I basically joined this because Michele talked me into it. Michele is my fellow traveler on the EWG, and it's been extremely instructive in terms of trying to figure out how policy actually gets implemented at the ground level, and has informed some of my

thoughts about the EWG. Since I'm going to talk about the EWG later, I think I'll leave it at that and say it's a fascinating experience.

I'll note that a lot of the future WHOIS replacement work depends on the widespread, cheap, or free availability of privacy/proxy services to ensure privacy. It's really important that the PPWG reach the appropriate conclusions on some of these key questions. Thanks.

HOLLY RAICHE: Thanks Stephanie. Graham Bunton?

GRAHAM BUNTON: Good morning. Thank you Holly. I'm Graham. I work for Tucows. We're a large registrar and we operate a relatively large privacy and proxy service as well. Myself and Steve Metalitz over there are Vice Co-Chairs of this PPWG. We were having a brief discussion last night about how the Working Group is going, and we've put out a document for the session that we'll be having here. You've got it? Great. Have we published it? Is it available online? Okay.

It is something I'd encourage everyone here to read, because what it does show is that we've had, so far, a reasonably contentious Working Group with a variety of ups and downs. We are moving forward pretty well and we're making some really good progress. This is going to be a fun opportunity here, this morning, to hear what people think about privacy and proxy, and some of the other views that we haven't been seeing within the Working Group.

I look forward to that. Again, a thank you to the people here from the Working Group to help us move forward, because it's been great.

HOLLY RAICHE: Thank you Graham. Michele?

MICHELE NEYLON: In common with a couple of other people at the table, I'm involved at some level with this Privacy Proxy Working Group as well as being on the EWG, where we've been trying to resolve a very longstanding issue within the ICANN context. Rather than all of us spending a lot of time talking about things, I'd prefer to hand over and let other people who are in the room talk and give them more time. I'm going to shut up.

HOLLY RAICHE: Don't be silenced by Michele. James?

JAMES BLADEL: Thanks Holly. Thank you to the ALAC for this invitation and opportunity to hear feedback on this issue, and the work so far. I work for GoDaddy. We also have an affiliated privacy proxy service, like Tucows it's quite large. I have a joke that I say at ICANN meetings. Maybe it's more of a punch line or a quip, but it's you can always tell when somebody's a newcomer to ICANN because they have a great idea on how to fix WHOIS.

I was guilty of this myself, probably, a number of years ago. It's since been beaten out of my by the recognition of how complex the issues

are, surrounding this topic. I think that extends into privacy proxy services, by default. I was with Kathy on the WHOIS Review Team, where we examined this issue. We had some very contentious discussions as well, for a year and a half, two years, resulting in the final report.

As a milestone, we acknowledged that these services exist, that they are valued. Within ICANN perhaps there's a perspective that they're only for trouble-makers, because that's what we fix, but the tens of millions of customers that use services like my affiliated company, and Graham's, and Vulkar's and others, from most of them it's as controversial as having an unlisted phone number or PO Box.

There's a number of reasons and motivations why someone would want that. I was also heavily involved in the RAA negotiations, that ended with the temporary Specification. I wrote quite a bit of that Specification personally, so please throw rocks in this direction if you hate it. The thinking behind that was – and not to pick on staff.

They did a fantastic job, but they came to those negotiations with a reasonably fully-baked accreditation program. It was the registrars who said, "Time out. This needs to be done through the proper channels, through a PDP." So every Tuesday, when we meet to discuss these issues, keep in mind that this could have been just a box to be checked in a contract.

We dragged this issue out into the open, out into the transparent community, to have these discussions at the Working Group level. I think that's the right place for these types of issues to be resolved and addressed. As a provider that has invested in people and procedures, to

not only provide a service but be responsive to problems, I think that we welcome the opportunity to raise the bar for the entire industry.

For those providers that just aren't up to snuff, we certainly welcome the opportunity to show them the exits. That's it. It has been a great Working Group. I think it was all over the map initially, but it has settled down here in the past few weeks, and I think it's making good progress towards its goals. Thank you.

HOLLY RAICHE: Thank you James. I have to say, when he first stood up and said, "This is the Working Group," and he said, "Now listen, we have to have something in place by 2017," I thought he was joking. I thought, "2017? That's miles away!" I have to say, having sat on the Working Group, I now think that's really close.

JAMES BLADEL: That was intentional, because as we know, the temporary has a way of becoming the permanent within ICANN. We wanted to specifically add an expiration date, "Best if used by January 2017," to that Specification, to guard against exactly that.

HOLLY RAICHE: Thanks. A final Member of the group who's here is Steve Metalitz.

STEVE METALITZ: Thank you Holly. I'm active in the Intellectual Property Constituency. I'm a lawyer representing the music, movie, software, games industries.

Industries that do most of their business online today, and are also very dependent on WHOIS as a key element of accountability and transparency online. I want to thank ALAC for three things: first, for inviting me, of course; second, for the introduction that Holly provided, which I think really helps to put this in context; and third, for the fact you have a sustained interest and engagement on this issue.

One thing we know for sure is that this is not a sport for the short-winded, and I think it's the fifth or sixth time that I've met with you and with this group, so I really appreciate the fact that you guys are sticking with these issues and how much you've contributed to the discussion so far.

I think your introduction really helped put in context that we have this system currently, and certainly even before the temporary Specification, in which, although ostensibly WHOIS was there to provide the accountability and transparency that's needed, so that people know who they're dealing with online – and we can have respect for the rule of law and other important values online – in fact, 20-25% of all gTLD registrations are almost all proxy registrations.

We have a problem there, because there are no rules or common understandings about what the circumstances are under which those perfectly legitimate proxy registrants, what are the circumstances under which people can reach them and under which people can contact them. That's the problem that we're set to face.

I think James if right. With his efforts we now have a temporary Specification in place to provide some disclosure about the rules that those people that are in that business now are applying, which is very

helpful. The idea would be let's see if we can get everybody to a similar set of rules and set it at a good level. That's the purpose of the accreditation process.

I agree that I think we're making pretty good progress in the Working Group. Some of the toughest questions lie ahead, but I think so far, so good, is how I would say it. I appreciate the engagement of all the people that have already spoken before me on the Working Group. They're making that possible. Thank you.

HOLLY RAICHE: Thanks Steve. There was one thing. I was just going to let the Working Group know I had a chat with Dave Piscitello yesterday, who said, "For law enforcement, access to WHOIS doesn't matter. It's not important. It's about the eighth or ninth most important thing." So I think our Working Group really has to concentrate on access to other information, because LEAs actually have access to the information they need.

Now, I'm seeking confirmation of that, but I just thought I'd let you know that that was something I'd never heard before. Somebody like Dave Piscitello saying that to me makes me think maybe we could have him to the Working Group so we could say, "Is that true?" and in which case that closes of a debate. After that, I'd like everybody in the audience to start thinking about the sort of issues that I've got up there.

It's things like, what do you mean about accreditation? Who accredits? How often? What are you talking about when you're talking about verification? These are the issues all of us, and the Working Group, are

facing, and we need to hear from you. Michele, first you get the floor, and then everybody else does.

MICHELE NEYLON: Thanks Holly. Very briefly, this thing about whether law enforcement use WHOIS or not, during the work we were doing prior to the 2013 RAA negotiations, law enforcement did engage at some level. We were able to have dialogue with them, with respect to clarifying exactly what they were asking for. They're here in the building this week. There's a bunch of them here.

There's lots of TLAs. There's FBIs and other things, and European equivalents. EUROPOL is here and INTERPOL is here. If people want to talk to them, they're there. They do have access to quite a lot of information. They can easily come to us. Irish law enforcement can come to us and we will give them certain things, under certain conditions. I can't give them things I don't have, and I wish they'd stop asking me for things I don't have.

There's no reason why they can't turn up for a call and actually go through some of those things with us, and I think it would be a good idea to formally invite them to do so. Thanks.

HOLLY RAICHE: Thanks Michele. Our first responder, Stephanie?

STEPHANIE PERRIN: This will give listeners some idea of what the debate is like in the PPWG. At a risk of being a pain in the neck – and I'm regularly a pain in the neck,

Michele will testify – law enforcement also includes enforcement of data protection law. The law enforcement folks that aren't here at ICANN on a regular basis, are the data protection commissioners, who enforce data protection law.

So I have had no success in getting those guys wedged into the bracket of "law enforcement" but they should be represented.

HOLLY RAICHE: Steve? Actually, if the rest of you around the table, and sitting in the audience, have questions… Garth, you're after that.

STEVE METALITZ: One thing I've noticed about ICANN, and 3,333 other people managed to get here, and for the registration fee, and jumped through the hoops to get through the door, it's very easy to participate. I just wonder why the data protection authorities, if they haven't participated, why they haven't participated, especially since many of them are in Europe, and we're meeting in Europe today. I think it would be great to have their participation.

HOLLY RAICHE: Garth?

GARTH BRUEN: Garth Bruen. Chair of NARALO. Holly, you know that I love you, but I do have to correct you. I'm not correcting you just for the sake of correction. This is actually a very important detail about some of the

history of WHOIS. It's this misunderstanding that actually ends up getting some of the arguments and discussions off on the wrong foot. People didn't have to identify themselves, even on the earliest network.

The actual explicit requirement was that someone placing a host that passes traffic, passes content, on what was then the ARPANET, had to identify themselves. If you were part of a local network, if you were a Harvard, MIT, BU, UCLA, Xerox, [Rand, Raytheon 00:43:33], whatever, that was up to the local network administrator, whether or not you were identified. If you were using the host, it was the host that was identified. It was the host that had to have contact information, and accurate contact information. That was the requirement.

This idea that people using the Internet have to identify themselves is completely incorrect. It's exclusively someone that has a host that has to identify themselves. If we're going to start the discussion, it has to be started from that point. Thanks.

HOLLY RAICHE: I love you too. It's okay.

MATTHIEU CAMUS: Matthieu Camus, Internet Society France. I'm here as an At-Large Member for Internet Society France, but I'm a volunteer at that. Besides that, I work for the Authority for Data Protection in France. [Applause] I'm from the technical field, I'm not a legal expert. The French Agency is a part of the European group, that's the Data Protection Authority G29, and for over a year there's been discussions on agreements, and particularly on the RAA 2013.

There are two items that are an issue to us, regarding how long we should keep data – the data retention policy. For legal aspects, particularly in Europe, we seek to have data retention justified for [unclear 00:45:59], so when that is legal when that ends, the data retention is considered to be justified. That is why we asked for a procedure to be exempt from this data retention, because we considered that by default, data is retained for too long after agreements are over.

So that's two years, by default. So the G29 group, that's the European Authorities Data Protection Group, asked for a maximum duration of one year for data retention. So for each agreement we should likewise have an exemption request. G29, at the European level, asks to have recognition for a homogeneity of legal aspects, legal implications at the regional level, for there to be an ease in the request for exemption.

Each individual exemption request is too long a procedure. That is a concern that's being discussed at G29 right now, and I'd like to discuss this with you. Thank you.

HOLLY RAICHE: We're going to run out time fairly soon, and I want to give Carlton a bit of time to talk about the EWG and why people should participate. Next. Could you keep the comments very short? Kathy, you wanted to say something? No? Okay.

HAMZA: Thank you. I'm Hamza. I'm a registrar from Morocco. We are talking here about WHOIS proxy. What about registrar proxy? Back in

Morocco, law enforcement really don't care about WHOIS data. Once they see a genius as a registrar, they know who we are, and then they just send a cop into our office and ask us to come to their police to get whatever they want.

Of course, there is no judge decision, there is nothing, and we just have to give them whatever they want. If we don't, well probably I wouldn't be sitting here and talking to you. The best thing for us is just to have the genius name disappear from the WHOIS and not even know the registrar. This is how we could actually be protected and protect our users and registrants. Thank you.

HOLLY RAICHE: Neil?

NEIL SCHWARTZMAN: My name is Neil Schwartzman. I've been fighting abuse longer than most people have been on the net. I wrote the first distributed anti-spam filters, and so as an individual hobbyist and now as a professional, fighting to protect real people from real abuse on a daily basis, I can assure you wholeheartedly that whoever quoted Dave Piscitello is misquoting him. I can also tell you that…

I'll give you an example. [Captainbeats@yahoo.fr.] Look it up in WHOIS. Look it up in Google. One address allows to dovetail to numerous different abusive domains on the net. That is a simple fact. If you redact that I have the inability to block and protect tens of millions of users on a daily basis from malicious phish and worse, these are real cases. No,

it's not just law enforcement. I don't have the ability to subpoena or issue a warrant.

I do have the ability to investigate, and WHOIS is something that every single anti-abuse researcher on the net uses continually, so don't listen to these excuses about… I'm sorry, but three registrars with deep financial interest in maintaining and expanding proxy services so that you can double your profits on a daily basis for every registrant that uses it, sorry. I get why you need it, why you want it, but that doesn't help. GoDaddy is one of the good players. So is Tucows.

I work regularly with your abuse teams and it's great, absolutely, but that doesn't splay across, as you well know. There are many people who just ignore any kind of attempt to try to get information. As I said, I don't have a warrant, so it's a problem.

HOLLY RAICHE: Thank you. Alan?

ALAN GREENBERG: Thank you. I had my hand up from way before, and I was going to say something akin to what Steve Metalitz did. It's hard to understand why people responsible for data protection do not show up at a place like this. It's obvious right now that one of the single largest or most visible sources of privacy violations, of identify theft and a variety of other things, is computer based.

I would think it would be an easy argument to say that they need to be present at discussions like this. Perhaps offline, but I'd really like to understand why they don't see that as part of their responsibility.

HOLLY RAICHE: Yes Sir? Could you identify yourself for the transcript records please, and then talk?

MURRAY MCKERCHER: This is Murray McKercher speaking. I'm with NARALO, unaffiliated. I was at the law enforcement meeting earlier this morning, which is packed by the way. No room in there. With respect, I think we also need to reach out to them. They may be here, but just knowing where everyone is… I simply wanted to say that we should probably also be participating in their sessions. I've learned a lot. That's all. Thanks.

HOLLY RAICHE: Thank you Murray. [Victoria 00:53:13], then Stephanie, and then I'm going to have to cut it off. I would like Carlton to talk, at least briefly, about the EWG. So two more speakers and then Carlton.

[VICTORIA BELTORA]: Thank you. This is [Victoria Beltora 00:53:29] from ISOC Italy. I have apologized, since I participated a lot until five years ago and then I've not been participating a lot in the last four or five years. Maybe I should have made these comments before this point. First of all, it's my fault, and I apologize for that. I still see a fundamental issue with the way the problem is posed.

The very idea of a privacy proxy is somewhat bloated, because privacy, at least for us in Europe, is not a service that you have to buy. It's a fundamental right. You should be able to get it and have it by default, without having to go to a third party and spend some money to get it. I can understand the idea of a privacy proxy for organizations. By the way, for organizations it's even too much.

European law says that individuals are entitled to privacy, whilst organizations are not. Actually, it's bloated in two ways, because it's too much for organizations and it's not enough for individuals. I'm fine if ICANN wants to push this, but it's not a solution to the problem of privacy in WHOIS, at least for Europeans and for the European law. It's a good way to extract more money from the registrants, which is something ICANN is very good at, but it's not a solution to the privacy problem.

Also, I have a problem with the discussion on whether there are legitimate or illegitimate users of privacy, because privacy is a right, so by definition there is not an illegitimate use of privacy. It's like saying that my freedom to go out and go wherever I go can be legitimate or illegitimate depending on where I want to go, and whether I commit a crime when I exit my hotel room, so I have to declare where I'm going to go every time I exit my hotel room and someone has to check whether I am allowed to exit my hotel room and go wherever I want to go.

HOLLY RAICHE: Okay. Thank you. I would say probably it's the wrong terminology, but what we're talking about is that there are people who use the privacy proxy services, and there are those who actually abuse it.

[VICTORIA]: I'm right. There is an abuse of any right, but… Can I finish? I'll try to be short. If the problem is having a point of contact, then if you disclose an email address for every domain name, but not your telephone number and your identity and whatever, if the problem is that someone commits crime by using one of [WHOIS 00:55:53] fundamental rights, you go the police.

We don't need the self-appointed sheriffs of the net, and I don't want anyone to think they have to police the net to be able to access my information, track me down, and do whatever they think is right to do. The idea of what is right to do is very different according to the parts of the world you live in. I don't want anyone from another culture, who doesn't understand what I'm doing, to be able to police myself.

Finally, I'd like to ask who you contact in the Italian data protection commission authority, because I'd like to check why they're not attending the meetings. Maybe it depends on the contact. It's also true that the Article 29 Working Party has been stating positions for over 12 years now. They've been welcomed by ICANN by saying, "You're not binding, because you're just a consulting body so we don't even care about what you say."

Why they should spend time on ICANN is just… It's just the law. Why are you requiring the European governments to come to ICANN and advocate for ICANN to abide by the European law? This is really an insult to European sovereignty.

HOLLY RAICHE: Thank you for that. Stephanie, and then we have a comment remotely, and the Carlton.

STEPHANIE PERRIN: I just wanted to say I strongly supported everything that the last speaker just said. There is a fundamental problem here between fundamental rights and freedom. Holly will be cutting me off if I start waxing on about the Canadian Constitution, but I did want to respond, because I did work in a data protection commissioner's office, namely the Canadian one, and I also worked in the department that brought in the private sector law.

It's been a long, hard struggle to try to get data protection commissioners to spend some of their scarce resources staffing… I tried in the '90s to get them to go to standards committees, because the mobile standards are basically breaking the law. They just don't have the staff and the resources to send guys to standards committees, because if you've ever worked in standards committees you know what kind of a thing that is. It's like coming to ICANN – almost as painful.

The other thing is I don't think it's the responsibility… I wound up doing the speech for whoever was invited to give this speech at ICANN in Vancouver, whenever that was.

SPEAKER: December 2005, because I invited Stephanie. There has been participation from data protection commissioners and the Article 29, and I'll stop there.

STEPHANIE PERRIN: But if they're not expert in the particular area, then they're reluctant to come to this crowd, heaven knows why, and stand up and oppugn on things like the legal principles, in an alien environment where the jargon is just impenetrable. I think there's a responsibility, if ICANN is styling itself as a global, multistakeholder, bottom-up, consensus-driven organization, they have to start translating things into plain language, so that some of the legitimate public policy players can actually understand what they're on about.

I don't think we do a good job of it. I certainly don't think the EWG did a good job in its report.

HOLLY RAICHE: Thank you Stephanie. We've got a remote question. I've promised 30 seconds to James, and then you have it.

GISELLA GRUBER: Sorry. If I can please remind everyone to state their names when speaking for transcript and for interpretation purposes. Thank you.

ARIEL LIANG: Thank you Holly. There is a question from the remote participant, Xavier Rodriguez: "To the Director of the table, or any person on the table, I am reading on Twitter critiques about EWG not allowing decent points of view in reports, etcetera. Can you clarify the issues?" Thank you.

HOLLY RAICHE: That's EWG. We're not there yet. Let's move onto James, then to Carlton and EWG.

JAMES BLADEL: Thank you Holly. Thank you Carlton. I want to respond to two or three speakers ago. I do support a lot of what was being said, however I want to point out that while privacy may be a right, and a right that one should not have to necessarily expect to pay a third party for, maintaining that privacy is not a right and it is expensive to intervene, to operate those types of communications, to filter them, to relay them, and to act as an intermediary for all of the unsolicited communications that may be coming through.

I just wanted to put that into the record; that we don't feel it's inappropriate for a service provider to say, "You may have a right to privacy." Maintaining that privacy online, in the context of WHOIS, it's not free for us. We feel perfectly justified to say that that's a proper role for a service provider. Thank you.

HOLLY RAICHE: Thanks James. Carlton, we're going to briefly talk about EWG. We are over time, but in fact there's nobody slotted here so we can keep going.

CARLTON SAMUELS: Thank you Holly. I'm going to give you a little background on the EWG, and I have my colleagues here that will be helping me to fill it out. For more than 15 months we had a whole set of us get together on the bequest of the ICANN Board, to see if we could bring a new canvas to

the problem of registration data services. We spent a lot of time together in developing this, which is our Final Report.

That's what we were trying to address – this gridlock around WHOIS and registration data, and to see if we could figure out a better way to move forward. The idea was, let's start with a clean slate. Let's look at the issues holistically and then see if we could come up with something. These are the Members of the EWG. You see a couple of us are here.

There's Michele Neylon, there's Stephanie Perrin, myself, Fabricio, Rod, Michael Niebel, Lanre, two Members from the Board – Steve Crocker and Chris Disspain, Nora Nanayakkara. All of us, together, spent 15 months, now running into 16, trying to get this thing together. We're not going to do a lot of these slides. We're just telling you a little bit of the background. We waded through a lot of stuff to get to where we are.

Thousands of hours of research. You see up there 2,600-odd pages of comments, responses, results. We had to wade through 19 public community consultations, 35 meeting days, we had calls and calls, we had sub-team calls… For example, Michele and I were on a separate sub-team with Scott. I was on a separate sub-team with Stephanie and Michael and we were looking at different aspects of the problem. We had hundreds of calls in the sub-team.

This is just to tell you the effort that went into producing this report. All of this effort answered just one question. Is there an alternative to today's WHOIS that is better positioned to serve the entire community? We thought yes, there was. The team thought there was. We felt the case because from out of all of that work and that review, we found that

the model that is open to everybody, and all the data anonymous, had a lot of inaccurate data and it wasn't serving the purpose. In other words, we thought that most of it is full of garbage.

We put out the Final Report. You will have seen the Final Report. It was published. In it we put in the details forward that we considered the next generation directory services [ideas 01:05:55] there. We had a lot of compromises to make. We have to strike balances between principles, between needs and responsibilities, accuracy, access, accountability, all of these things.

We thought it would be important for us to collect, validate and disclose registration data for permissible purposes only. In all of this we agreed that there should be a minimum data set that would be available for everybody. We have to have safeguards to protect data, especially personal data, and it would only be revealed for specific purposes. We call that gated data and gated access.

If it's gated it means you have to have some kind of process to access that data beyond the gate. Looking at this holistically, we also thought we needed two sets of new contracted parties. We had the validate contact data. So we had to validate the data officially, and the objective there was to improve the accuracy of the registration data. Then, because we had the data that was sequestered behind the gate, we'd have to have some kind of accreditation mechanism and some accreditors, so that we know who is accessing that personal data that's held behind the gate.

We're not going to go any further on this, because we have some of our friends here who'll be able to give their views. I'm going to start with Michele.

MICHELE NEYLON: Thanks Carlton. As Carlton said, and I think you'll hear this from several other people throughout the week, the EWG Report is a very big report, and I'd urge you to read it in its entirety, because the big problem with the EWG thing is that it's quite complicated. If you pick paragraphs, sentences and other bits of it out of context, you'll get a very strange view of things, because it's not simple.

The kind of issues that we've tried to address – whether we've succeeded or not I suppose we'll all know over time – is to go from the basis that privacy does matter. Yes, Neil, I'm going to aim that straight at you, because I was actually quite offended by your intervention there. Privacy is a right. Privacy is something that exists under law. As the French gentleman mentioned, there are serious issues with respect to the ICANN contracts and European data protection law.

Demanding that registrars retain data for two years is excessive. Forcing regsitrars to jump through hoops in order to comply with their local laws is completely illogical. The EWG worked on the basis that privacy needs to be respected from the beginning and all the way through the entire system. The idea that the data should be available – okay, yes, but only under certain circumstances and not to everybody. You can't just go in there and have a party, "Hey, data, let's go play!"

The reality these days is that it's not 1995, it's not 2001, it's 2014. If you look around you, I've got here beside me one laptop and one smartphone device with me now. If I was at home though, I'd probably b e surrounded by a lot of other little gadgets with nice shiny lights and blinky things on them. We all bank online. We transact online. We interact online on a daily basis. Our digital footprints are growing, growing and growing.

From my personal perspective, sure, I'm a vester, I've got a vested interest. I run a business in this space. It's not as big a business as Tucows or GoDaddy, but I still make a living of some kind. The system that was put in place originally evolved over time, and it's being used these days by entities of all shapes and sizes, for all sorts of different reasons and for different purposes. What was there just didn't really fit anymore.

As James said, everybody who comes along to ICANN for the first time says they can fix WHOIS, and he really hit the nail on the head. I can remember the first ICANN Meeting I came to, which was Lisbon in 2007. Nice venue, great city, great place. I think the first thing I actually said anything in an ICANN Meeting was in relation to WHOIS. I was immediately jumped on by ICANN staff, like, "Oh my God, you're Irish!" I've been stuck in this circus ever since.

All the previous efforts around WHOIS looked at fixing what was there; revising it, tweaking it, rejigging it. The reality is that that never worked. It was like putting a Band-Aid on a broken arm. That's a totally inappropriate way of fixing something. When we started work on this

16 months ago… Sorry, Carlton, some of the others and I live through various people's lives at this stage.

There's been births, there's been deaths. I don't know if we've had any marriages, but it hasn't been far off it. Considering some of the amount of time some of us ended up spending on this, if I had been married I probably would be divorced. The reality is that the system that was there didn't really work, so coming up with a new way of handling the data, giving people access and giving people protection needed to be designed.

What we've come up with is a big beastie of a report. I'm not going to try and tell you, "No, you misunderstood us! It's really simple!" I'm not going to say that to you. It is a big beastie. It is very complex and complicated, but hopefully, what we've come up with makes everybody equally unhappy or equally happy, depending on what way you want to look at it. If you go through the report we do look at the strengths and weaknesses of the old system, versus what we've introduced.

Actually, there are some slides up there. We've got lots of tables where we examine the various different elements. We look at how you access it, why you would access it, and those kinds of differences. One thing I will say, because I think people seem to have misunderstood one basic principle, is we're not saying that public access to data will disappear.

We've never said that. This is one of the great big misconceptions, because the concept of gating data does not mean that you lose all "anonymous access", it just means that we are forcing you to access it in a slightly more controlled manner. That means that you might lose a certain degree of anonymity, but for those of you who've been dealing

with data for years, what would you prefer? A service that you can reach all the time, or a service that falls over every five minutes?

It's okay, Neil, you don't have to answer that one. There's a lot of different things that I think registrars and registries were dealing with but weren't actually saying explicitly. The idea, for example, of [rake-limiting 01:14:34] access. There's abuses of the system at the moment. There are companies and entities that try to mine data for all sorts of nefarious purposes.

There are people putting in all sorts of interesting but absolutely bogus information into systems. The idea behind putting it all behind some sort of protective layer is that one would hope people would be incentivized to provide better quality data overall, and so on and so forth. I'll shut up. I could talk about this for hours, but it wouldn't really be of help to anybody. Carlton, over to you.

CARLTON SAMUELS: There's a public comment. Then I'm going to ask Stephanie to weigh in. Then we'll go around the room.

ARIEL LIANG: There is a comment from the remote participant, SDSH. I am surprised to see no reaction in the room to the GoDaddy comment: "Privacy may be a right. Maintaining it is not a right. How can you possibly have one without the other?"

JAMES BLADEL: For clarity, I said maintaining it is not free.

CARLTON SAMUELS: Yes, I think that was what James said. I hope that satisfied the remote participant. We're going to go to Stephanie now to hear her comments, and then we're going to go straight out into Kathy, then Garth, and then Neil. Could he hold it for a while? Yes.

STEPHANIE PERRIN: Fear not. I'm sure Neil will have more things to respond to by the time I'm done. He's hunched over his terminal, for those who can't see. I think I'll start by responding to the Tweet from outside the room, concerning this dissent. Basically, we had a very hectic last week, as all Working Groups do when you're trying to get your Report out.

My life was further complicated by the fact that I lost my Internet signal, and I live 45 minutes from the nation's capital in Canada. If anybody thinks ubiquitous broadband is easy and cheap, forget it. I was a week and a half with no Internet, running up to my poor neighbors or driving into town for an hour to get an Internet signal, because sadly there's no Starbucks near me or where my farm is.

We were under some deadline pressure, and I finally said, "I really have to dissent, if you're not going to accept some amended language." I had no clue how to dissent, because this wasn't planned. There will be people who say, "Obviously, this was going to happen."

No. It wasn't going to happen until certain provisions were fully fleshed out in the final version, and I believe that the balance was upset in the report; the balance between enforcement of privacy principles and enforcement of accountability and accuracy principles.

I did send a dissent in. It made it, two minutes before the deadline. The determination of the group was that it was just too far reaching to be included with the report. At that point I said, "Okay, what do I do now?" Milton Mueller, who's on the NCSG promptly published it, which he wasn't supposed to do, but nevertheless at least it got out there. He then hopped on a plane to Berlin and I couldn't reach him and get it down over the weekend. I believe that's what happened.

The first dissent is out there on his blog at the moment. I've received quite a bit of commentary on how I've misunderstood the report, and so I'm going over it. I have a new version with citations, chapter and verse, and I'm currently adding to that. I'm going to publish it on my own blog, for which I availed myself of GoDaddy's privacy and proxy services and registered by own name. Sorry, Tucows. Next one will be Tucows.

I must say that using domains by proxy was quick, easy, not free. I have heard from the EWG that using privacy proxy services is free. Well, it isn't free yet, folks, so… Nevertheless, it certainly worked. Anyway, watch for a blog to be up there shortly. I don't know what the EWG is going to do with my dissenting comments. Unfortunately, from their perspective, the more people criticize what I've said so far, the more I go and find more citations.

If you read the report, it is like a fugue, it's so complex. You have tp go back and forth, back and forth, and read this provision with that provision to see how it all works together. That is not a criticism of the EWG, or the excellent writer that we have on board. Lisa Pfeiffer has done a sterling job of trying to pull all these pieces together.

It's a criticism of the problem with WHOIS. It's inherently complex and it's very difficult to pull all these bits together so that they balance each other out. All I'm saying is we're now a little balanced too far on the accountability side. Let me get down to some specific detail on why I'm saying that.

The principle objection that I have is we have some good material in there on privacy. The gate itself is an improvement on the wide-open WHOIS. The only problem is there's also an awful lot of data validation that's in there now, so whatever is inside that gate is going to be well validated, or it isn't going to be there. You're not going to get your registration, because there's mandatory validation recommendations.

So the price of getting good, validated data, was supposed to be effective privacy provisions. Now, as we know – well, maybe we don't know this, so I'm going to assert it and people can argue with me if they wish. From my perspective, of a some-30-year privacy practitioner, in pretty much all aspects, working in the government to get the law through, working in the private sector to implement it and work on privacy councils…

Working in a data protection commissioner's office as a director of research and policy, going to at least 15 international data protection commissioners, doing research prior to bringing the law in and consulting all of the data protection commissioners about what works in their law and what doesn't, I think I know a little bit about this.

I've got to say, ICANN is not a great place for enforcement of data protection law. The 2013 RAA is not the way you enforce data protection law, in my humble opinion. We don't have at ICANN a

comprehensive policy for privacy, which I find shocking for a global multistakeholder organization operating across many jurisdictions that have privacy law.

That's outside the remit of the EWG, commenting on whether ICANN has appropriate privacy policy, but the bits and pieces that govern the actual accumulation of data that should be subject to data protection law is not outside that remit. If it's going into the WHOIS, and it gets there through the 2013 RAA, then that piece has to be covered by a privacy policy.

Now, our recommendations on crafting privacy policies within the report are light touch. We said that ICANN should investigate the creation of a policy. We talk about creating a basic floor that can be applied through contractual provisions. We do not necessarily talk about what I think would be a logical step, and that's binding corporate rules. You will see that discussed, and the report does not adopt that.

So I lost that battle, and that's not something that I'm dissenting on. I think now that we've talked a little about that, I'm going to move onto what I'm dissenting on. The principle provision that I have a problem with is that of consent. There is a provision in there related to the purpose-based contacts, that says that registrars must provide an opportunity for individuals to consent to the provision of their personal information in their purpose-based contacts.

Basically, with the new system of purpose-based contacts – namely one for legal, one for admin, one for technical, there's a total of six, I believe – if you don't name someone to represent you, or you don't hire a privacy proxy service, then you must provide your own information.

That's problem number one. Problem number two is some confusion as to which data is outside the gate and which isn't.

In my view, our language is contradictory. I've been told that I'm misreading it, that in fact this is all inside the gate and you have to be authenticated. Well, some of the language says "public and published" and "mandatory". Wait for the annotated version and I'll show you the language that in my view, read out of context, is going to say, "That's published."

Whether we have another clause somewhere else in the fugue that picks up a different note or a different instrument and says, "Actually, that's behind the gate," then that's going to be difficult to argue in a PDP afterwards. We have a duty to make these things clear. We can't just drop them muddy. I think one more good, plain language edit would have helped this report.

Anyway, that's an issue. Is it outside the gate? If it's inside the gate then what do you have to do to be accredited? Here's another problem with the consent clause. The consent clause says if you're not going to consent to the user of your contact data for all permissible purposes, then you should be given opportunity to back out of the registration. Now, getting back to the earlier discussion about rights, that doesn't fit with data protection law, nor does it fit with constitutional rights.

It's a condition of service, contractual arrangement. That's a huge, huge issue. If, in order to get a domain name, I have to do this, or buy a proxy, then I've got a problem. From the perspective of a non-ICANN expert – in other words, okay, I've been here 14 months, I may know a

little bit about ICANN. I am not in a position where I could say that access to privacy proxy services is equally available in the global south.

I just don't know. I'm not sure that we have the data that would support the attestation that it is available. I'm sure probably GoDaddy and Tucows would love to say, "We're global. Buy us anywhere." Is it really true? If I'm in Zambia, can I purchase… Are there jurisdictions where they stop you from purchasing a privacy proxy service? I just don't know.

Give me answers to that and I'll feel much better. I should have said at the beginning, with respect to all of these dissents, I don't profess to be an expert in ICANN, at all. This is a very complex place. Please show me where I'm wrong. So far, I haven't got any evidence that's causing me to back off on this.

People have shown me where something says something different, but I've got three pages that say what I say it says, so as long as there's a conflict we've got a problem. I think that's about it. I've done my two minutes and I'd be happy to answer any questions.

CARLTON SAMUELS: Thank you Steph. We have another 15 minutes to go so we're going to go very quickly. Kathy, you're up. Then Neil and Garth.

KATHY KLEIMAN: It's hard to follow up Stephanie and Michele and Carlton. Thank you for the amazing amount of effort you dedicated to this. James mentioned we're veteran survivors of the WHOIS Review Team. These are long,

long efforts. They're very difficult. I wanted to make two quick comments and then talk a little bit about looking at the EWG Report, without commenting on the [fairly 01:29:35] big picture that might help people.

First, on the issue of paying for privacy. In the United States we do pay for privacy; unlisted phone numbers, you pay for, so there is a precedent on that. Second, on the history of dissent we've had a history of dissent in ICANN dating back to Working Group A. They are always published and they're always published with the report, so this is surprising. It's upsetting for many of us who've been part of that procedure of openness, not to see the dissents published. Please find the dissent on Milton's page, or wherever Stephanie republishes.

Second, this is a report that came out as an Interim Report. It was 84 pages. This is the report that came out as a Final Report. It's more than double. A lot of stuff seems to have changed. These are hard things to read, so we have to read them very carefully. There does seem to have been evolution, change. I'm confused as I read through this. I'm confused as to what's inside the gate and what's not inside the gate. I urge people to read these things.

I'm confused. I'm not confused, I'm troubled by whether in this era of Snowden we want to create a centralized database for all gTLD WHOIS data. I'm confused by the change of purpose of the WHOIS. When I talk to the old-timers we were very technically orientated for what the WHOIS is. Now, is the purpose really to contact the registrar about any kind of speech, anything they're doing with the domain name? Do we want that purpose?

Then, what happens with the little guys – the individuals, small businesses, home-based business, small organizations? They no longer seem to be as protected. Just some questions overall. Thank you.

CARLTON SAMUELS: Thank you Kathy. We have a remote question, before I get to Neil and Garth.

ARIEL LIANG: This is a follow up comment to the GoDaddy comment from SDSH: "Thanks for the clarification. This just proves as another nice example of industry interests running their foot over fundamental rights. Privacy and data protection, two distinct fundamental human rights, are guaranteed by treaties, constitutions, laws, universally.

"If I want protection of these rights I need to pay industries some fees for something that should be there and guaranteed in the first place. Perhaps you would be kind enough to further explain if I misunderstood your statement."

CARLTON SAMUELS: Thank you Ariel. Probably later on James will get a chance to get to that, but i have little time and several people lined up.

NEIL SCHWARTZMAN: I'd like to know what kind of jackboot is on the throat of the proletariat, but we'll discuss that afterwards, I'm sure. The fact is you can't open a bank account, drive a car, buy a house or even rent a hotel room

privately. When you buy a domain name you have a responsibility to declare that. Now, you can buy a proxy service to protect yourself if you are doing things that are of a sensitive nature.

However, as anybody in a post-Snowden world would know, if you're relying only on a proxy service on a domain to protect you from government intrusion then you are going to get busted. It is as simple as that. I can tell you, I've got five different ways I can identify somebody, without just that. So please, anybody who thinks that this is a huge privacy protection bubble around a registrant is silly.

There are a number of points that you raised. I'll say this: the bottom line is, again, I'm not a cop. I don't have access to the data. You asked whether or not I'd want gated access to a reliable, solid system. Of course. Absolutely. That's entirely reasonable. For professional or quasi-professional interest of individual researchers, or professional researchers, yes, without a doubt, if it's reliable and there's a way to actually do investigations to help protect real people's privacy, I'm all for it. There's your answer.

CARLTON SAMUELS: Thank you Neil. Garth?

GARTH BRUEN: I like the idea of the concept of having a gated access. I'm opposed to the idea that I'm supposed to accept that because the data's been validated everything's okay. The data's validated but you can't see it. That's a Shrödinger's cat. I have to go on pure faith. Secondly, I think

we're consistently mixing two incompatible populations, which are individual domain owners, and then really commercial entities.

The ones we're talking about are specifically illicit commercial entities, and the idea that concerns us, Neil and others, is that we're going to be continually faced with these illicit commercial entities, and then we're going to have to beg and ask for permission to find out who they are.

I'm also bothered by the fact that much of this debate and this confusion has been caused by ICANN itself; by not coming up with the standard, not addressing it over the years, and not enforcing the existing rules. Here we have the commercial entities and the consumer representatives here, stabbing each other in a room, and ICANN's not here. That bothers me. Thanks.

CARLTON SAMUELS: Thank you Garth. Michele, and then we have a remote from Siva.

MICHELE NEYLON: Very briefly, the EWG will be holding several sessions throughout the week. Some of the sessions we'll be doing the presentation type thing where we kill you all slowly with massive slide decks. Look, there's nothing like death by PowerPoint. Come on. You know you love it. The thing is, all of the sessions that we're doing throughout the week – and pretty much all of the Members of the EWG are here in London – is meant to be interactive.

It's to allow you all to come along and ask us questions, to ask us to explain the rationale behind why certain things are the way they are.

With respect to some of the points some people will raise around this, "Why isn't user group X's thing in there?" We've said in the report, we came up with a whole bunch of different potential use cases, user groups, permissible purposes, etcetera, etcetera.

We couldn't think of all of them and we never said that we had. We made it very clear that there were a lot of permissible purposes that we hadn't thought of. As to Kathy's point, I totally agree with you, Kathy. Kathy and I tend to agree, and disagree, on many things. The reality unfortunately is that while we may not like what WHOIS is being used for, you can't ignore it. That's the real problem.

I hate the way people use WHOIS today. I absolutely hate it. I think it's ridiculous. I think it's unreasonable, but it's the reality. I can't ignore it.

CARLTON SAMUELS: Thank you Michele.

SIVA MUTHASAMY: Sivasubramanian from India. I'm in the room. There is an [elaborately 01:38:41] for gated access, as to who gets the data, who has access to the data, after the data is collected. Before it's collected, in the process of collection, the domain industry operates with resellers, and some resellers could have a front page. Let's assume that it's a bad reseller.

If the rules laid down here are not known to the average user, and if the reseller is to ask for particulars that he's not supposed to ask and collects more data than required, the registrant would not know that

he's not required to give that data. Suppose he calls for his passport number and so on?

Once they've got [unclear 01:39:37] and what comes to my mind is if such a safeguard is built in at the collection stage by the banking system – for example VeriSign. Not as a domain name registry, but as a security service authentication provider, as a system whereby the data is not collected by the reseller or the front person, but goes direct to the bank. From there, if required, it can be shared with somebody.

Is that possible? Is that possible, or has it already been thought of that such a system of centralized, harmonized data collection, across registries, across resellers, at least a form of it…?

CARLTON SAMUELS: Thank you Siva. We have to cut you off there. Stephanie, we're going to give you a minute to answer and then we have to…

STEPHANIE PERRIN: Thank you very much, because you're making my preliminary point in the dissent, which is that we ought to develop a privacy policy first, not last. If we had a privacy policy at ICANN that stipulated what could be gathered and for what purpose, that would stop that. It would trickle down through the system. You should be able to count on local law, but sadly we can't. I don't know what jurisdiction you're in, but your reseller is likely to be located in a vicinity without strong local law. You wouldn't get away with that in Germany, but you might get away with it in… Pick a country. That's why ICANN has a duty to come up with a privacy policy that sets a high bar harmonizing what's in available data protection law.

That makes life a whole lot simpler. Binding corporate rules would make it binding on the organization. It treats ICANN as a data controller, which I will argue forcefully it is, and then it would distribute out to the various parts in the ecosystem.

CARLTON SAMUELS: Thank you. Michele, you wanted one…?

MICHELE NEYLON: Thank you. What Stephanie is saying is of course correct. The reality is that as a retailer, the entity that is selling the services, the domains, the hosting, in whichever country, we collect and ask for a lot of different information, which is completely separate to what you're dealing with for the registration. As a rule, I will have access to a whole load of extra data. The point you're raising is a very valid one.

What if the company, the entity, are basically scumbags and asking for ridiculous, crazy things? It happens. We all know it happens. I don't have an answer for you. All I would suggest and recommend is that you all educate people. If a registrar or a hosting provider is asking your for your blood type when you go to register a domain name it's probably not appropriate. Really. Honestly.

Now, if they're asking you for a passport number or a photocopy of your passport, you might feel a bit nervous about it, but I can assure you – we do it sometimes, when we're doing fraud checks, and a lot of companies do that. People do it in different ways. It's just a matter of educating yourself and being careful. Check: do they have contact details on their website?

Is the address on the website an actual building in a real place? We had a client once that apparently lived at a crossroads 50km from God knows where, in the middle of nowhere. We saw satellite images. There was nothing there. I think this is all down to education and common sense. Some of the stuff really is outside the scope of anything we can do, because it's beyond that. We say in English, it's beyond the pail. Thanks.

CARLTON SAMUELS: Thank you Michele. I'm afraid I have to bring the session to an end. Just a few closing comments. As you'd know, the EWG Report is up and it's available. I'd ask that some of you look at the highlights. We have three public sessions this week. This afternoon from 15:15 until 16:30 we have one, and then I think we have one 17:00 until 19:00. Then on Wednesday we also have one starting at 8:00 until 10:00.

Please look for us. Please come into the room and ask your questions, or ask them remotely. This leaves me now to thank everyone for showing up. On behalf of my Co-Chair, Holly, thank you so much for coming and sharing with us. Thank you to the interpreters and the members of the support team. Thank you remote participants. We are closing the session. Thank you very much.

[END OF TRANSCRIPTION]