
COPENHAGEN – ALAC and Regional Leaders Working Session Part 9

Tuesday, March 14, 2017 – 13:45 to 15:00 CET

ICANN58 | Copenhagen, Denmark

UNIDENTIFIED MALE: Good afternoon. This is ICANN 58, March 14th, ALAC and Regional Leaders Working Session Part 9.

ALAN GREENBERG: Folks, we're five minutes late. We have a really packed agenda and we have to add a few items to it, so we will be starting in one minute.

HOLLY RAICHE: Sorry. And, we've got to get going. This session is really a policy session. Does anybody know what WHOIS means? Garth isn't allowed to answer. Anybody else?

MAUREEN HILYARD: I do.

HOLLY RAICHE: Maureen, can you explain what WHOIS is because that's the title of this presentation.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

The title of this presentation is WHOIS and it is one of the longest running issues in ICANN. I joined ICANN back in 2009 and one of the issues was WHOIS and it has not gone away. It's transmogrified into God knows how many working parties, most of which I've been involved in or somebody has been involved in. Alan is also a veteran of WHOIS. So, if can go to the next slide and we can talk about WHOIS and why it's really an important and long going, long lived issue for this community, as well as everybody else.

WHOIS started off its life in the very early days of the Internet. It was essentially how geeks communicated with each other. So, this was we're talking about University of Southern California and we're talking about people like Jon Postel and others. And, all it was used for essentially was – look, can you tell me what computer you're at and now I'll get to you. It wasn't actually a lot of personal information in the sense as just geeks having a little directory so they could figure out how to get to each other and then how to send messages to each other, data to each other.

As the Internet grew, there were other people who begin to figure out that WHOIS information about a person and where they're connected to was actually interesting, important, helpful. And the user started to include besides all of these geeks, law enforcement agencies, so that when there is

communication between would-be crims of any sort or that's actually criminality on the net, it's information that we understand may have help law enforcement agencies to track people down.

Certainly, it's one of the pieces of information the Intellectual Property Constituency and the trademark owners absolutely want so they can actually hunt down people who they believe are actually in violation of copyright and trademark law. It's used by businesses, consumers – consumers in the sense that if you think an online portal has defrauded you of something, at least there's some kind of information that sits behind a website.

Now, this isn't a misleading statement in a sense that protocol was adopted by ICANN. What it means is ICANN said, "Okay, this is actually a request for [inaudible] and we are going to make it the basis of our contractual relationship with both registries and registrars."

There is a long screed on the ICANN website that actually has a history of WHOIS. It's very interesting. And if you want to find out a lot about it, you can.

Next slide, please.

UNIDENTIFIED FEMALE: [Inaudible].

HOLLY RAICHE: Sorry? Garth.

GARTH BRUEN: Thank you. Garth Bruen, ALAC North America. I just want to add a few points to your review of WHOIS history. The actual original intent of the WHOIS record system was responsibility through identification, an accountability thread and that's written into the spec, is that people who are using this common space to communicate with each other are expected to be responsible for the usage of such. And I would submit that that actually hasn't changed. Thank you.

HOLLY RAICHE: It probably hasn't. Going back again, ARPANET was – and Garth can talk about ARPANET. It was a precursor, one of the early forms of the Internet per se.

Next slide, please. Next slide. Is anybody moving the slide or do I?

UNIDENTIFIED MALE: [Inaudible].

HOLLY RAICHE:

The requirements – when I say that ICANN adapted WHOIS, what I mean is ICANN actually wrote into its relationship, its contractual relationship with the gTLD registrars, the gTLD registries, some requirements in terms about the provision of WHOIS information. And this is actually what you will find in the contracts for both registrars and registries. They have to provide an interactive webpage in the 43 service providing free public query-based access to all of the data of the active registered names that's the registrants.

And so, the next slide, it's for registries as well. This is taken straight from the contract that's between the ICANN and the registrars. This is the WHOIS data and once you look at the data, you'll understand why in many cases it's actually sensitive. So, you get the name of the registered name – obviously, the name – you get the name server, which is sort of technical information, you get the identify in the registrar, that's fine, the creation date, the expiring date but then you start to get into personal information.

The name and postal address of the registered name holder, that's the individual. You get the voice telephone number and available – if it's available – a fax number. The board – is this out

of date. Technical conduct for the registered name, e-mail address and so forth.

So, if this is referring to individuals, its contact information for individuals who are the holders of domain name. And you will note a lot of that information, well, much of that information is about the person and how they can be reached.

The next slide.

When we move from one relationship with it was finally the NTIA but for that was the NSI. Our ICANN's agreement with the U.S. government included a commitment to enforce the existing policy about WHOIS subject to – when you say subject to applicable laws, that becomes really a fly in the ointment. Such existing policy requires that ICANN implement measures to maintain the unrestricted and timely public access to all of that data.

So, this was actually a contractual obligation on registrars to make public information about the registrant, the domain name holder that includes contact information and names. Not only that, but this particular commitment is supposed to be regularly reviewed.

Next slide, please.

The WHOIS policy has been the subject of an awful lot of discussion simply because it in essence requires names and contact information to be publicly available. And by now, what you're getting is a lot of concern and legislation that protects personal information including the names and their contact details.

So by now, what you have is a very clear understanding from many people including myself that there's a direct contradiction between the WHOIS requirements and privacy law. One of the many reports that have been undertaken by ICANN, this was a big WHOIS, this is a huge team that got together, and look at all of the issues surrounding WHOIS. The actual title of WHOIS that was the name of the protocol but the term has been used in a variety of ways and not always the same.

In terms of accuracy, one of the issues from WHOIS is because the data is public, a lot of registrants will actually provide their name and address, and it will be Mickey Mouse and they live in 1 Sunset Boulevard in Los Angeles and their telephone is 12345678. When this team looked at the accuracy of WHOIS information, a lot of the information I found was not accurate. Indeed, 25% of the information they found was totally inaccurate. Probably another 25% was somewhat accurate. And perhaps, in half the cases or less, they could actually find a way to contact the registrant from the WHOIS information. And it was

seen that one of the reasons why, in fact, people don't put correct information was because it's made publicly available to anybody.

Next slide, please.

The policy surrounding WHOIS have been added to over the years. There have been policies that require the registrars and the registries to regularly check the accuracy of the data, and there's been a whole lot of work on what accuracy of data means and can it be verified, and how can it be verified.

One of the early arguments that law enforcement made was we really need this information. And, there has to be an abuse point of contact 24/7. So, if we find that there's criminality going on of some sort, we, the law enforcement agencies, have to be able to contact somebody and we need that abuse point of contact.

Also, written into the contracts between ICANN and the gTLD registrars are restrictions on the use of that data for marketing purposes. They're not supposed to. Now, that doesn't say that they don't but it says they're not supposed to and I think most of them don't.

There's also comments on privacy and proxy services. Now, these are services that many but not all registrars provide and there are two types of services that were discussed in the report.

One is simply where say a legal firm or other firm will put their name as the contact point for a particular domain name. Businesses use that for instance when they're about to start up a new product line or a new service and they don't want to telegraph to everybody what the names of that will be. They will have their lawyers take out domain names they want. And that will – in essence, that's an agency service. That's where the proxy provider is really providing just – it's just being the agent.

The privacy is when in fact the name of the service provider is in place of and not related to the person who wants to remain anonymous.

So there are different types of services but for a lot of the policy that's going on on WHOIS, you usually get the phrase privacy proxy service as a way of just saying there are your services where the name of the registrant and their contact details will not be publicly available.

And, because of a lot of I would say pressures from, if nothing else, ALAC, compliance checks in terms of have you as the registrar, the registry carried out all of the requirements that you are supposed to be undertaking in respect of WHOIS. So there's been a range of policies that have been developed. In fact, a major change – well, so major changes in the 2013 RAA largely to

accommodate a lot of the issues that were raised by WHOIS services.

Next slide. Thank you.

As part of a really big look at WHOIS because this has been on a policy calendar for a long time, the SSAC came up with one of the reports, SAC055 and I said, “Look, people have been using the terminology wrongly or at least in a confused way.” And we propose that in fact, we use – we, all of us use correct terminology to distinguish what we’re talking about.

[Ringing]

That’s all right. You’re forgiven.

UNIDENTIFIED MALE: [It was an accident].

HOLLY RAICHE: Okay, so this is the terminology that’s been adapted since then, so you don’t see WHOIS anymore. You see RDS. First of all, the terminology starts with domain name registration data. This refers to just the information that is being sought or that it’s provided about – well, that is provided when a registrant is registering a domain name.

This is the information that the registrars and the registries collect. There's a protocol called RDAP. And this is about the communications exchange whereby registration data is accessed or is made access to to the registration data for – and really, it's not RDAP. It's actually 2 RFCs, so it's RFC 3912 and the hypertext protocol.

But they are collectively referred to as the RDAP with the registration data access protocol. And then, there is the service that is providing the access to the data. It's a way of trying to unpack when everybody says or when people say WHOIS, they're actually might be saying one of three things and this is a way – this is the language that's now being used to distinguish when you're talking about a protocol or service or the data itself.

Next slide, Alan, go ahead.

ALAN GREENBERG: Just small, if you look at the last paragraph, it says, "Registration Data Directory Service." That should be RDDS.

HOLLY RAICHE: That's right.

ALAN GREENBERG: There is as subtle difference between a registration... I'm not even sure when it's just RDS, if it's the data or the directory. There is a subtle difference for our own intensive purpose treat them as the same and sometimes you'll see RDDS and these days in ICANN, we tend to use RDS.

HOLLY RAICHE: Yeah.

ALAN GREENBERG: Ignore the difference. It will make your life a lot easier. Although technically, there is a subtle difference but it doesn't matter to the large extent.

HOLLY RAICHE: Alan has also lived and breathed WHOIS for too long. We both have.

Next slide, please.

ALAN GREENBERG: I was around when the WHOIS discussion failed in 2007 that had been going on for about four years, so yeah.

HOLLY RAICHE: It might fail again. Sebastian.

SEBASTIAN BACHOLLET: Yeah, just a very short point of story if I can. Before the SSAC finalize the wording Registration Data Services or whatever, RDS was meaning was a request from the Board of ICANN when as a Board – and I was member at that time – received first WHOIS review to stop to talk about something old discussion from ten years and to change, to shift to something new. But I guess this organization lamentably failed on that because we are always coming back to what is WHOIS and how it’s organized. It was a tentative to take its way to the AWG [inaudible] talk to that later on. But a group of expert was supposed to help ICANN to figure out how to go in the future but we are always take back to the past. Thank you.

HOLLY RAICHE: It’s probably because so many of us have started with WHOIS and it’s a shorthand for huge and intractable problem, and it encompasses everything. Actually, it doesn’t.

ALAN GREENBERG: But moreover, ICANN has said, “Let’s call it RDS or RDDDS.” But if you go to a registry or a registrar website, it’s still called WHOIS. So we can’t ignore the fact that the term is still being used.

HOLLY RAICHE: Now, in the discussion about WHOIS – we’ll call it the WHOIS protocol – in terms of what the problems were and this was identified back in the WHOIS report. It was started in 2012, reported in 2014. One of the problems was it was never internationalized. So here we are, we’re going to introduce IDNs but with the protocol that can’t manage it.

There wasn’t a framework for data. So, in fact, from one registry to the next, there wasn’t a uniform way to present the data, for expressing dates, foreign numbers, etc. So, in fact, the WHOIS data could be displayed completely differently from one place to the next. It doesn’t make finding it very easier.

But mainly, the problem was that the old RFC could not support differentiated access and by differentiated access, what I mean is a system whereby data where you’re talking about – by the way, the Chair of the IRB, that’s the Internet Architecture Board and probably, somebody who knows so much more about WHOIS than I. Personally, Andrew Sullivan, this is where I’m up to.

ANDREW SULLIVAN: I’ve been here. I’ve been sitting over there.

HOLLY RAICHE: Oh, dear. And you thought you better intervene.

ANDREW SULLIVAN: No, I didn't.

HOLLY RAICHE: Differentiated accesses is a phrase to indicate if you have a database and you want some people or few people to have access to all the data in that database, you want another group of people to have access to some information of that database. And finally, a third group that have very little access to a very little information, you need a protocol that's going to say, "Well, unless you establish who you are, you're only going to get a minimum amount of information."

So, in 2012, a team of ICANN and these were the technical people. Were you part of this?

UNIDENTIFIED MALE: Which one?

HOLLY RAICHE: [WiIRD].

UNIDENTIFIED MALE: Yeah, I was the chair that got that thing going.

HOLLY RAICHE: Right.

UNIDENTIFIED MALE: [Inaudible] you are WiiRD Chair.

UNIDENTIFIED MALE: I wasn't the Chair of the Working Group. I was the Chair of the group that came together to make it happen. So, we got upset about WHOIS several times. I've said this in the chat. But the RIRs had an experimental system, started at [errand] and some of the other RIRs got involved. And, this was an adjacent-based sort of restful kind of thing, those of you who are – I mean, with the web these days, REST and JSON are the thing. And that's the new hotness. The old hotness was XML of course. The last time we tried to replace this, we produced IRESS and it was awful.

So, this was supposed to be fast, cheap and easy instead and the RIRs already had one running and the idea was that they wanted to standardize it and then people who noticed, well, there's this WHOIS thing that sucks for names, too. They said, "Okay, well, we'll come along." And that's how RDAP got done.

Oh, sorry.

HOLLY RAICHE: And I don't know how they're going to interpret some of that.

Anyway, this [WiiRD] group and it is an acronym. It's not a description. Sorry, it's both. Developed protocol that would address all of those issues. It could accommodate IDNs. There was a framework in which the standardized way to put data, access it and support a differentiated access became RDAP.

Now, the next page – and have I actually... Next page.

Before I get to that – no, actually, I'll wait until after [inaudible]. What's the problem? Because all of this, you're wondering why I'm talking about WHOIS and why this is such a big policy issue for ALAC and why Alan and I get up at really weird hours to talk about this.

AWG Working Group was established after the 2014 WHOIS final report, the Board took a deep breath and said, "This is an intractable problem." What we have here aside from the difficulty with the protocol, the difficulty with managing IDNs, we have a lot of countries like the EU for start but a lot of countries by then had data protection law, which had restrictions on how has access to what personal data and what circumstances. And yet we have a contract that requires registrars and registries to make all of that data public.

So, Fadi Chehadé took a deep breath and said, "We have to step back and work through how we're going to manage and possibly change the WHOIS, the RDAP, the Registration Data Service and

what is required so that at least the EU countries, 27, soon to be 26, Canada and other people with data protection laws, you're not putting the registrars and the registries in violation of their own national law.”

Under the AWG, the Working Group recognize that personal information is protected this data protection law and even when there's no law, they are legitimate reasons – and this is quoting from them – for individuals to seek heightened protection of their personal information. And you can think of these circumstances for that, whether it's a woman's refuge, whether it's a human rights group in many countries of this world, individual psychiatrist who don't want their patients after them. There can be a range of reasons, quite legitimate why people do not want their personal information particularly contact information publicly available.

And indeed, businesses and organizations for quite legitimate purposes may want to protect their information. It may be as simple as they are trying to protect or to launch a new product and they don't want that information to be public or where in the case of small business, if you release contact information, you're in fact releasing personal data. Or if for example, and you're in some countries in the world where it is an organization or growth of some kind of human rights, and they will be – just put these people in personal danger.

So, this was the basis of – what did E stand for?

UNIDENTIFIED MALE: Extensible.

HOLLY RAICHE: Extensible Working Group.

UNIDENTIFIED MALE: Oh, no, no. Sorry.

UNIDENTIFIED MALE: Experts [inaudible].

HOLLY RAICHE: No.

UNIDENTIFIED MALE: Expert group.

HOLLY RAICHE: Expert Working Group, sorry, I've known that, something I actually used to forget.

Next slide, please.

One of the things that the Expert Working Group did was to sit down and say, “Now, who is using this data?” We’re talking about WHOIS data. How many people are actually involved? And if you look at the [inaudible], you can realize it’s lot of people. It’s the public. It’s the tech heads. It’s the registrants, the registrars. It could be businesses. It can be IP people. It can be law enforcement. You’d be a range of people.

And, a lot of it up until... If you look down the right, there are mis [inaudible]. There is no question that there are people with less than legitimate intent. Do you misuse the data? But there are awful lot of people, with quite legitimate interest who do you use the data.

Next slide.

See, there it is, Expert Working Group. They unanimously recommended abandoning the WHOIS model. Just said, “Look, we’ve got to move to a different model,” that the model that they’ve got to move away from is the one that provides entirely anonymous public access to data, accurate or otherwise. And, what they said was there’s going to be a paradigm shift to a next generation RDS and that’s standing for the service that collects, validates and discloses generic top-level registration data. Do I want to say anything about that? No.

Next slide, please.

Now, this is a part – there are several diagrams and I said I’ll only deal with one. The idea and we haven’t decided and indeed, the Expert Working Group didn’t decide whether they would be one huge database or each registry or registrar would hold their own databases. There are arguments why you might put all of the registration data somewhere, which would then become a huge target for every single mis [inaudible] in the country, in the globe or decentralize the registration data such that it’s held in each registry.

In other case, the young idea is that the data that is collected for generic top-level domains is held and again, that’s a kind of where it’s going to be held. But then it has the ability to provide access to everyone of a minimum data, probably just the registrant name and an e-mail. If you have a legitimate purpose and can in some way be, I won’t say authenticated or authorized, in some way established your identity as a group of people who should have access to more, then you can use that database to access more data.

Clearly, access seekers such as the law enforcement agencies would probably have access to a lot but that has then the problem of how do you define law enforcement agencies. Now, do you want to come in?

ANDREW SULLIVAN:

Sure. So, just on this point of how you identify the people who are asking for access to this, RDAP, the protocol is built on top of HTTP. And, as you all know, because presumably you all use Facebook or something else. There are lots of ways to authenticate for services, using HTTP because we've already developed all of that technology.

So, the nice thing about this is that there's a protocol called OAuth and this would allow a service to be set up, multiple services to be set up that can authenticate various people. So the nice feature about this is that ICANN or anybody else doesn't have to have a theory about who could be authenticated here, instead various agencies could offer the relevant service. So, if the association of chiefs of police or Interpol or anybody else that you like wanted to authenticate law enforcement people, they would be able to offer that system and then the RDAP that various people run could authenticate against that and that way, you don't have to develop a theory of who is a police officer.

This is very similar to the approach that was taken in adapting the ISO protocol for deciding who gets a country code, right? Somebody else gets to decide who's the country and now the IANA didn't have to decide who is a country. Similarly, this would be a way of not deciding who is a law enforcement agency, who is an appropriate person who has credentials within a country

who's a government and so on. So, that's one of the goals of that, of the design of that system and the feature is already built.

HOLLY RAICHE: Next slide, please. Oh, Garth.

GARTH BRUEN: Thank you. Garth Bruen, ALAC. Holly, I've heard you did this presentation a few times before and I'm going to beg you to maybe include some more information and make some adjustments. I think that there are some things missing.

I mean, in addition to the comment about the context of responsibility being in the original spec, there was also a very specific instruction to not put sensitive information into the records and that is on the person who wants the service on the network, is that the responsibility is on them not to put sensitive information on.

And now, there are lots of problems with that and the Internet grew so fast and nobody really thought about that to protect ordinary people and consumers who are registrants. That's a problem.

I also would request that you acknowledge the huge, enormous, vast criminal abuse of the DNS that is responsible for the need

for obtaining this information. And the need for obtaining this information does not solely reside within law enforcement.

And, in terms of law enforcement – and I’m almost done – in terms of law enforcement, the idea that, well, a law enforcement will have access to this data automatically and then citizens might not. The idea that in some countries and in some societies, the law enforcement has automatic access to it, may not make a lot of people very happy.

HOLLY RAICHE:

That’s exactly my point and in terms of who has access, I point out that the RAA basically says, “This information will be available.” If you have sensitive information, that information – the name and address, and so forth are supposed to be published.

Now, the way that people get around that as I said is putting in my name is Mickey Mouse and my phone number is 1234. That’s not exactly the best way to deal with things but that’s the way that I would probably get around it.

In terms of the other – first, Alan, you want to go ahead?

ALAN GREENBERG: Thank you. Just a brief comment. Andrew talked about the theoretical capabilities. There is an interesting non-trivial transition from what it can do to actually building it. And Garth alluded to one of the things. Knowing who is an authorized police officer does not necessarily mean I want an authorized police officer in Iran to access my data in Canada because the standards are different and things...

The second issue – and that’s just a glimpse into this complexity. And the second issue of course, these days, we cannot live in this world without understanding the concept of data breach and virtually, every organization in the world no matter how secure they think has been subject to data breach is then what happens if either the single system or the multiple systems are breached. And, that some of the things that make this such a complex process.

HOLLY RAICHE: Exactly. I admit I’ve left a lot out, Garth, but I’ve been given – people have got 20 minutes, so I’m hoping there’s time for questions and I hope people are interested.

UNIDENTIFIED MALE: [Inaudible].

ANDREW SULLIVAN:

Just to be perfectly clear, I am not arguing that any particular policy are to come out of this. My point is rather that we have the technical capabilities to provide the policy, flexibility that people could do. The reason that all of the data appears in the WHOIS the way it is today, it's because of a technical flaw in WHOIS. It doesn't have the ability to provide you with multiple different views of the data depending on who you are.

We have that mechanism now. We've built it. It's already running. The RIRs are using it. And, in fact, Verisign is also offering an experimental service that you can play with if you want to do this, so you can see that it works.

The point is that we have a number of policies that could be made and now is the time in fact to make those policy decisions. And so, I would say that the purpose of the current PDP in which I am participating rather to my surprise, the opportunity is there now to make sensible policies and to make those policies in a way that are flexible enough.

Certainly, I mean, I work for a DNS company. I'm perfectly aware of this situation in respect of needing access to some of these things but that doesn't mean that I need access to all of the things. I need access to some things. And this is the opportunity to make those policies and to make them in the same way.

HOLLY RAICHE: Thank you, Andrew.

Now, we've gotten up to the fact that we have a protocol that does allow what's called different access. And, that's an illustration of a situation where someone who is authorized queries the database, and because their authorization is such that they are allowed certain data, they will get the data.

Another diagram from the same AWG report shows where in fact you are not an authenticated requester, so you get a lot less information and that's the whole idea of addressing the issue of data protection law, which basically recognizes that you have limited access to personal information except in certain circumstances and allows you to determine what those circumstances are, which would be far more appropriate to existing data protection law in many countries.

Next slide, please.

For his sins and for our sins, Alan and I, and Andrew are on a –

ANDREW SULLIVAN: And 400 of our closest friends.

HOLLY RAICHE: Right. After the Board accepted the Expert Working Group recommendations, which was essentially for – the main

recommendation was about differentiated access, the Board then realized there had to be a policy process because policies would have to be changed. The policy in the contract right now is all that is public. To support any change of protocol, you have to have a policy that says, “By the way, we are now changing the requirements that we have in contract such that differentiated access is allowed.”

So, for our sins, there are a bunch of us and the name goes long – list goes long every time that have to work through the changes in policy. We are tasked with, first of all, asking, “Well, why is this information collected?” and under privacy law, you do that because first of all in basic privacy principles, you are not supposed as a corporation or organization, you’re not supposed to collect personal information unless it is actually required for you to implement the purposes of your corporation. And you’re not allowed to provide access except as what has been told to the individual and they’ve consented.

So, there’s a whole process of working out what information you’re collecting and why and then who should have access to that. So, this is obviously the first thing that we’re charged within this Working Group.

The next thing is, well, now that we have an RDAP protocol, if and why a next-generation Registration Directory Service, in

other words, do we need to replace the WHOIS policy of many years? And, if so, what policies are needed and can they coexist with or do we need to change the policy?

So, it's a huge task. We've only been talking to each other for how long?

UNIDENTIFIED MALE: [Too long].

HOLLY RAICHE: And it looks like it's not going to stop. But essentially, it is now trying to change the nature of the requirements in the contracts from one of collecting a range of information that includes personal information and then displaying all of that that's publicly accessible to everyone with something that recognizes data protection law that follows the principles about the collection of information only what's necessary and then who has access to it under certain circumstances.

We are still talking about what? Purpose?

UNIDENTIFIED FEMALE: Yeah.

HOLLY RAICHE:

We're talking about purpose. We've been talking about purpose for a long time. We'll continue to talk about purpose for a long time but that's where we're up to. And for anyone who has any interest in privacy law, in protecting private information, this is really an absolutely critical working group. It takes a long time because the people we have as part of the working group aside from our chief [guru] will be people with interest in privacy, you have the Intellectual Property group, you've got law enforcement groups, you've got lawyers who want to act for businesses. You've got a range of interest and they're all there. And, we meet 90 minutes every week trying to get through just these variations. It's not necessarily easy if I can put it that way.

Can I have the next slide, please?

These are the questions that the Working Group of the GNSO is now charged with. The first is when addressing this question, a PDP should consider – and that's the fundamental requirements for generic top-level domain name [inaudible]. At a minimum, the users and purposes, and access accuracy data, etc. requirements. In other words, go back to the original contract you have between ICANN and the registries, ICANN and the registrars for generic top-level domains, what information do you really need?

The next thing is the new policy framework and the Next-Generation RDS needed to address these requirements? In other words, we've got WIIRDs, we have the protocol, do we actually need it? I think you'd say yes. Don't cry.

Do we need a protocol and do we need new policies? And I would probably say yes, certainly from a privacy perspective, you would. If yes, what crosscutting requirements must a next generation address including coexistence, etc? In other words, what have we got? What is it that a next RDS policy going to require in terms of collection of information and then access to the information?

The last question we've kind of answered: does the existing WHOIS policy framework sufficiently address the requirements? And I think we've pretty well said no. And, if not, what revisions are recommended to the current policy? We've probably already mentally answered the question no and now, we're stuck on what to do about it.

Is that a fair summation?

ANDREW SULLIVAN:

It is a fair summation with the proviso that there are still some people who want to argue really that no new policies are needed. So there are some people who clearly think that open

access for everyone is an acceptable status quo and that it should continue.

SATISH BABU:

Thank you. Satish for the record. I'd like to know something about the IDN side of things and that are the data that is center that the distribution time is translated in English and whose responsibility is it to get the information translated if it is being done.

ANDREW SULLIVAN:

Well, at the moment, it is not being done. I understand that there is a working party talking about that. Both WHOIS and more fully RDAP are access protocol, so they give you whatever is in the repository, the registry. We say registry, right? But formally, it's a repository of data. And so, you can get whatever is in there. And so, the question is, what's in there now, you can get out.

The problem of course with WHOIS is that the way that it works is completely undefined. It was defined in a period of ASCII-only and so formally, it's an ASCII-only protocol but there's not very much protocol there. Really, it's connect, ask a question, get back something, whatever it is and there's no formatting or anything.

RDAP provides you with a framework in which you can ask giving the indicators of your language settings because it uses HTTP and so you have this header that you can say, “These are the languages that I can use.” And so, you could get back localized data assuming that the other side can provide that.

ALAN GREENBERG:

Thank you. Andrew pointed out there are some people who believe that we should just have open access and why are we wasting all this time talking about it. On the other side, there are people who believe that privacy should be close to ultimate or complete. And, this is to the extent that we had spent a significant amount of time discussing whether it was known as Thin WHOIS, the stuff that’s currently kept by .com and .net in the registry, which consists of the name, the expiration date, the registration date and they point you to the name servers.

We have spent extensive amount of time talking about whether the pointers to the name server should be public information or not. And, for those of you who are not technically astute, if you don’t tell people where the name servers are, you can’t get to the domain name. Yet, we spent significant amount of time discussing that. So, it’s going to take a while.

HOLLY RAICHE:

The final statement I'd like to make before questions, and first of all, the reason that I'm very keen for everybody to have at least a little bit of a snapshot of this issue is because this issue has been around for a long time. It actually impacts on a lot of the discussions about privacy and about access to information. I'm not promising it will be solved tomorrow or even next year but it is one of the issues it's been on the ALAC policy for a very long time.

Now, yesterday, the data privacy commissioners of Europe, many of them, had a very interesting session. It was data protection, there was law enforcement, there was a range of people all talking about the privacy requirements. And Jim from Afiliis basically said, "Look, if we decide to go down this path, there's going to have to be an awful lot of technical work because we never built a 24/7 on all the time system that is globally accessible that will tell you whether you can have access to the information. And the extent to which you can because you qualify as either someone authorized to access certain levels of information or not."

We haven't got there yet. We are still talking about the sorts of philosophical questions about what sort of information should be and – Alan is right. We're still talking about Thin WHOIS trying to tease out some principles as to how we decide what information should be collected in the first place. Because once

you figured that out, then you have to figure out, well, who should get access to how and then we have to figure out some crazy definitions of how we decide if somebody is a law enforcement person. And if it's a law enforcement person from some countries versus other countries, that's going to be only difficult. Well, I don't know what. What other issues have I missed?

ANDREW SULLIVAN:

Well, I mean, this is a general problem, right? Because it's not just law enforcement agencies as somebody mentioned already, the general problem though, I agree with Jim that registries have never actually developed to this sort of thing. But I presume that most of us know what Facebook is. I mean, there are lots of examples of this on the Internet. This is not a weird problem. It's a solved problem and it's not actually that hard.

So, I recognized that there is development work that has to go into this but the hard problems here are not the technical ones. The hard problems here are the policy ones.

HOLLY RAICHE:

Now, Andrew is going to have to go. We're almost out of time. But have you got any questions about either the work that we're doing or... Okay, Olivier.

OLIVIER CRÉPIN-LEBLOND: Yeah, thanks very much, Holly. And, I was looking around the table as the discussion was taking place. This, as you said is in age-old discussion, WHOIS. I think it started even before ICANN ever existed. So, we're reaching the – was it 18-year or 19-year mark?

Two things – well, several things. First, I was looking on the table and people were like this and like that, and like that and like that. And, the body language basically shows that we're starting to get really sick of this topic. I think everyone is turning to get really sick of this topic.

It's obvious that there are some people that believe that the status quo is fine since it seems to be that we haven't moved in 18 years on this topic, which is personally pretty outrageous because I guess the Internet has changed in 18 years and that seems to be one of the oldest things and topics on the table.

Then again, there are also people who believe that climate change is a fad and it doesn't exist, and there are people who continue to smoke even though they are told that it's very bad for their health. So, you can imagine the state of the world is all resumed in this WHOIS problem.

Is there something that we can do to break this deadlock? Because ultimately, it's clear that those people that do not want to put hand to pocket to design and to implement a new system are not going to dodge because if after 18 years you don't dodge, you pretty much are cast to the ground, you become fossilized in place. And so, short of a nuclear explosion, you will not move from the position that you're in.

And yet, it's plain obvious that there are many issues related to this, otherwise, we wouldn't waste not even hours or years of volunteer at work. But I think some lifetimes of volunteer work, we've gone through several generations of people discussing this around the table. What can we do if we can to break the deadlock and move things forward? Could we set an end point and say a little bit like the CWG or the CCWGs that we have with the IANA Stewardship Transition and everything else? That always seemed to be the case at ICANN.

For example, the next round of new gTLDs, oh, let's have a date when it will be launched before we even start the work on finding out what's going on. Should we suggest a date for this work to end? In which case, if it's not ready by then, well, we'll go with what's on the table at the time and if it breaks, then obviously, something will have to fixed and quickly. Thank you.

HOLLY RAICHE: Well, Chuck Gomes is already retiring, so he's giving up. Your comments.

CHUCK GOMES: Well, I don't know how to make people come to agreement. It does appear from my point of view. And it's not like – I mean, I come from the IETF and it's not like we're speedy. Things take a long time there and yet I am astonished at the re-litigation that happens in this PDP. It is impressive the way that people can find a hole into which to draw everyone and then we explore all of the molecules that make up the mud on the side of the rat hole. So, I would encourage people actually to go a different direction and that is it seems to me that on the Internet, one of the things that happens is things get deployed if people want it.

ICANN is in fact going to require that registries deploy RDAP. They're going to require it. There's a session tomorrow about how that's going to happen. So, the new protocol is going to get deployed and it seems to me that the way to – once the protocol is already in place, then people have an argument to make, which is – well, this protocol also allows you to protect my data under my national law in a way that the old protocol didn't.

So you now have the technical capability to do data protection consistent with the laws under which you are operating, why don't you follow the law? And if people demand that, it seems to

me that puts pressure in the other direction. So the policy cannot stand the way it is despite the desire the people have.

ALAN GREENBERG:

It is typical to hear me say at the beginning of a PDP when someone says I want an exact detailed schedule of when we're going to get to each stage and when we're going to end. For me to say that's not realistic at this point. This particular PDP I think we need to set some targets and dates. And if we start missing them, that's a red flag waving. Because without it, we are going to re-litigate, we are going to ad infinitum debate issues, which are not really debatable and we're going to try to settle issues that are ultimately not settleable on the general case, and are going to be specific.

It's not our job to set: how do we define law enforcement in this particular thing. Yet, we are having that discussion of who is law enforcement. I'm not talking about a one-line thread. I think we have to use multiple methodologies. Andrew has described one of let's just start implementing and maybe someone will see the light and realize it's real. I think the PDP itself has stats and deadlines, which we may miss. But there are just so many impediments to getting this done that we've got to start removing them one by one.

HOLLY RAICHE:

Olivier, I agree with you and I agree with Andrew, and Alan, this has taken a ridiculous amount of time. We've got to the point where there was a survey taken about how people felt [inaudible] somebody. And then, there was a question about whether the results should be published. So there was a survey about whether the results of the survey takers should be published. And at that point, I thought, I get up at 2:00 to do this. Forget it.

Because this has been going on so long but now we've got RDAP that actually is going to enable something, it may be time for ALAC to say, "This is a problem about data protection. It's a problem that actually impacts on users potentially." And could we set some deadlines?

I mean, literally, Chuck is going to retire and he's going to be – let's put it this way. The frustration yesterday, which I found was such that Elliot from Tucows stood up in front of the line and said, "We need a privacy protection commissioner right now and because somebody has got to protect us from the law enforcement and the IP community," and I was stunned.

But when Tucows is standing up saying, "This is too much," I suspect... Were you there?

UNIDENTIFIED MALE: I have a different... I had a conflict.

HOLLY RAICHE: Yeah, it was a surprising statement coming from a very large registrar saying enough is enough. Now, I hope never to do this again. I hope that we're going to... or if I do it again, I'm going to say, "I've done the first 15 slides. Go back, look at them and number 16 is we're on our way."

But this is still a problem. It is still an issue in front of ALAC. It is still a big problem about privacy and hopefully, it will go away.

ALAN GREENBERG: We are over time. I see Sebastian has his hand up and we'll call upon him. I just want to make one editorial comment.

I don't know how many of you know Chuck Gomes. He's one of the more balanced, pleasant people around and very much in control. I've seen him until this PDP lose his cool once in ten years. And it was over a really substantive issue. It's happening to him more than once now.

That just gives you a measure of something. Sebastian, last question, we are a little bit over time. We have a very, very tight agenda for the rest of the afternoon. So, Sebastian, go ahead.

SEBASTIAN BACHOLLET: Thank you. I will try to be very short. First, I was hoping when the Board decide to set up this discussion about RDS and not about WHOIS. And as a matter of fact, just for you to know, it was not the CEO who came [with this] proposal but it was the one you select to be member of the Board at that time. Sometime I was not the only one but I was one of the first one to say we need to find a new way to go. That's the first point.

The second, I hope – really I hope – that the technical community have done a great job. I don't want to be in the same situation that with the IDN where we have to do a policy after a decision, technical decision. I really hope that it's not the case. Because if not, it's not 10 years but it will take us 20 years to fix that, and that would be wrong. Then, I really hope that the technical community have done great this time.

And I am sorry to say that. I prefer always that we decide policy here before we develop something. But it's happened in these communities that we need your help. And once again, I hope it was in the good direction and thank you.

ALAN GREENBERG: Thank you, Sebastian. Thank you, Holly. Thank you, Andrew.

HOLLY RAICHE: I'm sorry?

ALAN GREENBERG: I said thank you, Sebastian. Thank you, Holly. Thank you, Andrew.

SEBASTIAN BACHOLLET: Thank you, Olivier. Thank you, Alan. Thank you, everyone.

ALAN GREENBERG: All right. Sorry. We're just having a debate on what we're doing next. This is a 15-minute break.

HOLLY RAICHE: Ten-minute, okay.

ALAN GREENBERG: Ten-minute break. We reconvene at 3:15, 15:15. We will reconvene quickly. This is a discussion on a very substantive issue for the future of At-Large. Please be back on time.

[END OF TRANSCRIPTION]