

MARIO ALEMAN: Good morning, good afternoon, and good evening, everyone. Welcome to the At-Large Capacity Building Program 2017, our eighth webinar on the topic Update on WHOIS-related Initiative, Next Generation Registration Services and Its Impact on End Users, on Wednesday the 4th of October, 2017 at 21:00 UTC.

We will not be doing the roll call since it's a webinar, but if I could please remind all participants on the phone bridge as well as computers to mute your speakers and microphones when not speaking. Please do not forget to say your name before speaking, not only for transcription purposes but also to allow our interpreters to identify you on the different language channels.

We have English, Spanish and French interpretation for this webinar, and thank you all for joining. I will now turn it back over to you, Tijani, the Chair of At-Large Capacity Building Webinar Working Group. Over to you.

TIJANI BEN JEMAA: Thank you very much, Mario. Good morning, good afternoon, good evening, everyone. So this is, as Mario said, our eighth capacity building webinar for the year 2017. Today, we will speak about the next generation registration services and its impact on the end users, and it will be presented by our dear friend and ALAC member from APRALO, Holly Raiche, who is member of the working group on the next

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.

generation registration services and who has always worked on this issue. I think she's the best person to speak about it.

Of course, we had also Carlton who also worked on the subject and is still working on the subject, and unfortunately he cannot join us because of the conflict of time. But Holly will do the whole work and she is wonderful she actually had to do that. Thank you very much, Holly.

HOLLY RAICHE: Thank you.

TIJANI BEN JEMAA: Before I give the floor to Holly, I will come back to Mario for some housekeeping announcements.

MARIO ALEMAN: Thank you, Tijani. Let's take a quick look at the housekeeping presentation we have here displayed now. We'll have questions and answers [folder] in the webinar. As you see, it's located on the left-hand side of the Adobe Connect room. If you have any question, we do encourage you to type them here, and they will be directed to the presenters.

We also have a pop quiz section, and that is located on the right side of the Adobe Connect room once we finish the presentation. After the speakers' presentation, please be ready to answer those questions that will be posted on the pod.

Finally, we'll have a user experience part. There will be a five-question survey at the end of this webinar. Please do stay around for an extra three minutes or so to complete that. Back to you, Tijani. Thank you very much.

TIJANI BEN JEMAA: Thank you, Mario. And without any delay, I will give the floor to Holly to make the presentation. Holly, please.

HOLLY RAICHE: Thank you. And could I have my presentation slides? And Mario, can you move the slide as I ask you to? Thank you.

MARIO ALEMAN: Absolutely. Thank you.

HOLLY RAICHE: Thank you. Now, could I have the first slide, please? Or the next slide. Okay, this is about WHOIS, but it's really about the whole WHOIS issue. The background to the WHOIS protocol is that it was developed in the very early days of the Internet when we were talking about APRANET, and it was a system whereby people who were using this newfangled thing called the Internet could look each other up. So it would be just a little server somewhere that would say, "Well, look, if Steve Crocker wants to talk to Jon Postel, then this is what he's got to do, and we'll

just transfer this little message over between these people who know each other.”

As everybody on the call is aware, the Internet grew by leaps and bounds, and it was no longer a communication system between geeks. It started to be used by law enforcement agencies, defense departments I would say, people intellectual property and trademark owners beginning to find out that there were perhaps issues arising from domain names, businesses wanted to use the system to publish their business, and of course, consumers to find out a range of information.

So between the early ‘80s and the ‘90s, the system of the Internet went from a few people who knew each other to millions of people who didn’t. However, the protocol which was really the system of communications that was used in the very days was adopted with the formation of ICANN in 1998.

The website that’s on the first slide, ICANN has a huge amount of historical information about WHOIS if you’re interested. Also if you attend the policy seminars – as I’m sure you will – ALAC has done a number of policy statements about WHOIS as well. So there’s a huge range of information out there if you’d like to follow it up.

Mario, could I have the next slide, please?

In fact, WHOIS is really three things. Now, these definitions came from an SSAC paper, SSAC 051 to be specific, pointing out that we’re really referring to three separate things when we say WHOIS. The first is the

data itself, and [I have a further] slide about what that data is. It is the data that the registrants – that is the people who hold the domain names – are required to provide to their registrar, particularly for generic top-level domains when they actually register a domain name.

The second meaning is the protocol itself. That's the elements of the communication exchange that provides the public with access to the data. It's called the WHOIS protocol, and there was an earlier number. It's become RFC 3912, and in on second I'll give you an update on the protocol.

The third is simply the service itself, the service of providing public access to the data. Now, I'm not going to spend a lot of time on the protocol, except to say that it has been updated. There's a new protocol that was developed in 2012, and it's actually called WEIRDS, the Web Extensible Internet Registration Data Service, that allows stuff that the original protocol won't, for example access to international domain names. So the protocol itself has been replaced, but that's the terminology that we should use to be very clear about what we mean. Next slide, please.

Okay. Under ICANN's requirement with all gTLD registrars, the requirement is that the registrar has to provide an interactive webpage and a Port 43 service providing free public access to the data concerned. And for registries, which have a separate contract with ICANN, those requirements are very similar. So in fact, the registration data – and we're talking about the data – the service must be provided that

provides public free access to registration data. Could I have the next slide, please? Thank you.

This is the data. Now, it's a range of data. It's obviously the name, and then it's technical information. People forget that the registration data is not just personal information. It's the nameservers, it's the actual registrar, it's the creation date of the registration, the expiration date, but then you get into possibly personal information about the registrant. The registrant's name and postal address, fax number – good heavens, some people still use faxes. That's fine. Technical contacts, and then information about administrative contacts.

So registration data is a combination of some technical information about the registration, as well as contact information. Next slide, please.

Now, this slide, I don't know what happened to it, but it should say the Affirmation of Commitments. This was the agreement before the IANA transition. This is the Affirmation of Commitments that was an agreement between the NTIA and ICANN, and it required ICANN to enforce its existing policy relating to WHOIS. Subject to applicable laws, obviously.

It required ICANN to maintain timely, unrestricted and public access to the accurately complete WHOIS information. That becomes an issue that has bedeviled the whole WHOIS debate for some time, because as I've stated, the gTLDs are required to provide public access to a range of data, some of which might be classified as personal information about the registrant. And this is why it's a problem. ICANN must, according to

the Affirmation of Commitments and agreements before that, continue to provide that public access. Next slide, please.

So, what is the problem? And there have been many ICANN reports, working committees and so forth on WHOIS. There was a cross-community – I'm not sure it was titled cross-community – WHOIS final report that included representatives from ALAC, from GAC, from GNSO, from ccTLDs, to look at the actual issues that arise from the WHOIS requirements as well as the service.

Their conclusion – this is way back in 2014 now – there are lots of issues regarding WHOIS in terms of both the service and the data that is required. As they point out, it's about accuracy. One of the issues about accuracy was because registrants are required to have their personal information publicly available, many people simply said, "We will use what's called a privacy proxy service" – and I'll define that in one second – "so that our personal information is not made public."

People can do that for a variety of reasons. They can do it because, for example, it might be a women's refuge, they don't want people to know how to get a hold of the women's refuge. It might be any range, or businesses that want to take out domain names but they don't want their product known for whatever reason, as well as people who simply want what – what we call the miscreants – to promote mischief.

So there can be a range of reasons why people did not want their name known. They could use a privacy proxy service, or some of them simply gave a lot of incorrect information. They said their name is Mickey

Mouse and they live in Disneyland. There were lots of studies done about the accuracy of WHOIS data, and many of them pointed to the fact that it was anything from a quarter to a half of the WHOIS data was simply incorrect.

So accuracy was a real issue, still is. Privacy is an issue. Anonymity. People wanted not to have their information made available. Policing. The law enforcement has always been concerned that the information is accurate so they can actually track down people. And spam. If that information is available, is this going to be used by people to send spam?

So there were a lot of issues that surround WHOIS, and they were all identified in the WHOIS final report. And the summation of what they said – it's a gross understatement – tensions exist between the constituencies. If you sit in on a WHOIS working party, you'll find that there are many people and they represent many legitimate points of view, and they spend a lot of time explaining their points of view. Next slide, please.

Okay. One of the issues – and remember, this is only one of the issues that are raised by the WHOIS requirements – is privacy. Now, a lot of people would say this is all about the European directive. It's not. It's about basic privacy principles that have been in place literally since the OECD promulgated the privacy principles back in 1980. And most of the privacy protection rules, whether it's in the European Union or many other countries, whether it's in Asia or North America, have as these principles their foundation.

The first is the collection limitation principle. As a business, an organization, you only collect the information you need. And you collect it lawfully, and you collect it with the consent of the person about whom the information. That's really fundamental, and it becomes a touchstone of many other issues, such as what information do you need?

Data quality. Personal data should be only necessary for the purpose that you've stated in your collections, and you do have to specify the purpose. You do have to be very clear on, "I need this information because of the following reasons. And if I need that information, that's why I collect it." These have been principles in place for 40+ years. Next slide, please.

The other relevant one, you only use and disclose data in relation to your original collection purpose. That principle is in place unless the data subject – that's the person – agrees otherwise or in accordance with law. And that's usually law enforcement agencies. And then the data must be kept secure.

And for those of you following this very closely, you realize that this set of principles really challenges the rules regarding WHOIS and its requirement to make all of that information public to anyone regardless of the purpose and regardless of who the person is. Next slide, please.

The OECD principles were updated in 2013 to reflect the massive changes in communications and the massive changes in the Internet. Information is collected in ways we never thought about. Every time

you put an entry into Facebook or every time you look something up in Google, a lot of information is collected and held by them.

As this is the introduction to the changes, we leave huge digital data trails which makes it a lot easier to figure out what we are and who we are. And as everybody would be aware, there's a lot of security breaches all the time as people hack into information sources. Next slide, please.

What happened probably about two, three years ago – no, more – is the ICANN Board took a step back and said, "WHOIS – meaning not only the data itself but the data that is collected and then made public – is presenting a real challenge in terms of the growing awareness of people's privacy and the growing number of countries that are enacting rules about data protection, about what should be made available and how it should be collected, and how it should be displayed."

They charged a thing called the Expert Working Group – and Carlton was a member of the working group. I wasn't – with taking a fresh look at the whole issue in terms of what information is actually collected, what information is public, how it's used, how it's accessed, does it need to be accessed by everybody that uses it? We need to have a complete rethink.

And this was the ICANN Board's way of saying, "Let's stand back and say we need to update our whole collection and use of personal information in terms of everybody who uses it and everybody who

accesses it, and see if those rules really reflect people's expectations in the 21st century."

So the problem. There's a growing expectation of privacy. This is so true throughout the world. Not just the European Union. There are also legitimate reasons for individuals to want protection. And this is not just individuals, this is businesses, it's organizations. So the EWG spent a couple of years going through, looking first at what is collected, how it's collected, what people are told, how it's used. Next slide, please.

The first thing they did was get a full understanding of who actually uses all of the WHOIS data. And as I said way back in the beginning, we're not talking about geeks anymore. We're talking about billions of people. We're talking about members of the public just going, "I wonder who's behind that domain name."

Obviously, Internet technical staff. Researchers. You'd have to say a lot of businesses, a lot of intellectual property people. And certainly for the law enforcement agencies, agencies with the mandate to track down miscreants, anti-spam people. So what this slide demonstrates is EWG sat down and said, "You know, there are a lot of people with quite reasonable reasons to access all of the WHOIS information, particularly the personal information that includes contact information."

And if you notice down in the bottom in the little pink, it's the miscreants, everybody who wants to send spam, the hackers, and it's the criminals. So what we've got in front of us is a range of seemingly

legitimate users as well as the criminals, the miscreants who actually use the data. Next slide, please.

And the conclusion of the Expert Working Group is we can do something better. There is a better way. And the recommendation was simply abandon the whole WHOIS model that gives everybody anonymous public access to a range of data. Just say no. And they suggested a paradigm shift to the next generation [that's] registration data service that actually collects and discloses the information, and they propose what's called gated access. Basic data – by the way, we haven't decided what that means yet, but some basic data would be publicly available. But the rest of the information that is collected would require some kind of identification of someone, of an individual or an organization, that had a legitimate reason to accessing that particular personal information. And that person could be held accountable for the appropriate use. So it was a completely different paradigm. It was a paradigm shift from the existing WHOIS, and this was what's been followed on from now. Next slide, please.

This is a conceptual model of what the EWG proposed, that the data sits in a little container whether it's one huge database or whether registries would hold the data. And then depending on the status of the requester of information, they would only get a minimum amount of public data, or depending on their status – whether that is an intellectual property lawyer, a law enforcement person or whatever – they would get information appropriate to their status. And they would only get the information that was necessary to achieve their particular legitimate purpose.

This is what we've called gated access, that in fact the gate basically stops everyone from getting anything but basic information. And then depending on who you are depends on what gates you get through and what information you get. Next slide, please.

Resulting from the report of the EWG which the Board accepted, the Board then said, "Okay, to go down a new path in relation to the WHOIS data, we're going to have to set up a new working group called the RDS, and they're going to be tasked with standing back and looking at the actual purpose – starting with the purpose – of the collection, the maintenance and who gets access to the range of data that is currently required under the RAA."

And then safeguards. What do we put in place to make sure that only the people who should have access get access? And then how do you create the policies to implement what you have decided in terms of the purpose and the safeguards? Next slide, please.

These are the charter questions, and to be very honest, this is where we're stuck. When addressing the question of the PDP should consider the users and purposes. So really, we're going back to [inaudible]. If you remember the OECD privacy principles, essentially that is what we're asking in terms of all of the data that is required to be publicly accessible.

And then if we've gone through the first question, then we have to say what are the requirements, and then is the current WHOIS policy

framework capable of addressing the problems? And if not, what do we do?

Some of you will already have said, "Well, actually, the EWG already said we need to throw out the WHOIS policy and we need a new one." But that was not part of the PDP, that was an Expert Working Group. This is now the official policy – the policy development process to say, "Okay, the Board wants us to follow through with the EWG reports." That's what this group is doing. Next slide, please.

I've put up their progress to date, and then I just take a deep breath and go "Mmm... I'm not sure we have." The working group is established beginning of 2016. We have massive membership. Not everybody shows up all the time. The meetings started at 60 minutes and then we just realized we were not going to make any progress at all if we started with 30-60 minutes. So now we're at 90 minutes.

And what's happened because the progress is as slow as it is – and I'll explain why – is every week, there are surveys to say, "Well, we think we've made this progress, but not everybody was on the call. Are you comfortable with where we've got up to on our discussions about – do we need to change the whole WHOIS system?" We're still on the first question. That was the question – yes, it's alright. We're still on the first question, what's the purpose? And next slide, please.

Okay. Those are the issues that we're supposed to get through for phase one. To show you how slow the progress is, we're still stuck on

purposes. Because we have to determine what are the legitimate purposes and who should have access to the purposes.

If you go back to one of the really – and Mario, don't do that – but if you remember the collection principle, we have to ask ourselves as a working group, what information do you really need to make the DNS system work? And I have to say there was an e-mail from – many of you won't know Andrew Sullivan. He's one of the really very smart tech heads in ICANN, and he has spoken to ALAC before. I think it was last time. And he practically said, "Just to make the DNS system work, just to transfer, just to get somebody from one computer to another, you don't need any of the information. What you need for the reputational systems and some of the security surrounding it is more information, more personal contact information."

But based on – this was an e-mail two days ago – it's going to actually put us all back again to what is it that we need to have in terms of a primary purpose and a secondary purpose that will give personal information, how much of that should be available. We're really still stuck on that question. Next slide, please.

Okay. Why the urgency? And for those of you who have attended ICANN meetings or watched the sessions on ICANN, for two sessions in a row – and Cheryl knows this because she was involved in the last ICANN meeting and playing Chair to another discussion on what everybody is beginning to call the GDPR, the General Data Protection Regulation. This is something that's come from the EU directive on privacy. It strengthens their privacy directive. It was adopted in April

2016. The magic date for everybody who actually collects the information is May 25, 2018, in which case the new, revised EU directive will become directly applicable to all 27 – although 26 when the UK leaves the EU – countries without national legislation, which is not how the EU normally works. But this is going to become applicable.

And it strengthened the EU data protection rules in a couple of really important ways. First of all, in things like what you mean by consent, the accountability of the person who holds the information, the requirement that you have to have data protection by design and default, not simply added on where possible, and the big one, the rules will apply for organizations and individuals not only if they operate in EU countries, but if they sell into EU countries or they sell or control or process data on EU citizens.

And if you think about the registrars and registries, think about something like Tucows or GoDaddy. How on earth do they know if they've got EU citizens as registrants? They don't. But it means that they have to be very aware of all of the EU requirements just in case some of their registrars are in fact EU citizens.

So it's really a red flag to the whole of the registry and registrar community saying, "In fact, you all have to go back to the EU directive and look at the information you're collecting, look at the information that's made public."

There seems to be – if you read the Registration Accreditation Agreement – the statement registrars shall abide by applicable laws,

and some people have said, “Well, that means that if the registrar or registry says, ‘I’m sorry but I can’t publish all that personal information, I won’t,’ that they will then be let off from their requirements under the ICANN RAA.” Because clearly, look at the fines. If you as a registrar or registry do not comply with the updated and strengthened EU directives, after warnings and audits, you can be fined 4% of your annual worldwide turnover, which is just staring all of the registrars and the registries in the face.

However, there was a process in ICANN for the use of 372 – and I’ve sat on one of the working groups – none of the registries or registrars are finding that is a workable process, because it requires legal opinions that they will be in breach of applicable laws, and no lawyer will give it and no data protection agency will give it. So the clause is there, but it’s never been used and it’s not seen as particularly helpful. Next slide, please.

Okay. This is from the General Data Protection. What data are we talking about that has to be protected that is the subject to the directives? And it’s an expanded definition. So if it says, “What is protected?” It’s any information about an identified or identifiable – and that word identifiable means information you can use to identify somebody, and that has been interpreted to include things like IP addresses.

So I’ll go on with the definition. “An identifiable person is one who can be identified directly or indirectly – and that’s important – by reference

to an identifier such as a name, an identification number, location data, online identifiers.”

So in fact, that’s a huge definition of personal data. And remember, it’s personal data that is protected by the EU directive. So if you think about this very broad definition and you think this is what the EU directive as expanded by the General Data Protection Regulation, you understand why there is such urgency on behalf of ICANN to have a system in place that will accommodate the growing privacy laws, but also legitimately understand and deal with some of the other legitimate reasons for the use of data. Next slide, please.

And Cheryl has made a very good point. It affects how ICANN manages its data too, because ICANN is also a data controller. So ICANN has become very aware of not only the GDPR, but privacy regulation generally, and the fact that it is covered by a lot of privacy law.

What the working group did in trying to understand the extent of the protections involved and what is covered by the GDPR, they used a law firm that had a great deal of expertise in European data law, and we’ve received – I think it was just last week – an opinion from this law firm which is a very interesting opinion. We’ve had some criticisms of it, but it’s got some very interesting parts in it.

The purpose. In terms of the purpose, this legal opinion said the purpose for collection should relate to the actual registration of domains, but more broadly, the functioning of the domain name system. If you go beyond that, it’s a secondary purpose.

Now, secondary purpose doesn't mean you can't collect it. It means though that you have to be aware that it has to relate to the first purpose as well. And so in terms of our discussions about purpose, we have to go back to that phrase, the functioning of the domain name system and what does it mean. We're still working on that, the data element.

And as I've pointed out in the definition of personal information, the factor is not just about the name of a natural legal person. It's about the data fields and whether taken together, they actually get you back to the purpose. And if you remember the definition of personal information, that's a lot of online information. It's location information. So potentially, there's a lot of information that might wind up looking as if it's personal information.

However – and this is another extract from that legal opinion – for the purposes of prevention, investigation, detection or prosecution of criminal offences, clearly, there's an exception from the GDPR, but more broadly, any other body or entity to exercise public authority or powers for the purposes of directive also would have access. So we have to decide what that means. It may be, for example, that your consumer protection bodies in a country would have access for a legitimate purpose.

It may be, for example, that your corporate watchdogs would have access to the information because they're there to prevent fraud. We haven't really gotten to the bottom of that sentence, but it means that

probably the people who have access are wider than just your normal law enforcement agencies or security or defense.

However – and they note – the fact that anonymous public access to registration data may have some potential benefit with regard to consumer protection, it can't mean that that overrides the basic protections.

So in terms of, "Should individual consumers have access to personal data?" The legal opinion we have seems to say no. So this is so far what we know in terms of a legal opinion. And of course, like any good lawyer, they all say, "Well, actually this is just an advice, it isn't binding," etc.

But this is the guidance that we have so far on the meaning of the GDPR and how that's going to access some of the rules regarding what information is out there and who should have access to what data. Next slide, please.

And I think that is the end. Oh. What ICANN has done is establish a small team to work through all of the requirements of the General Data Protection Regulation and work through what that means in terms of the requirements on ICANN itself as well as registries and registrars.

There was a webinar about seven or eight hours ago which I did not attend but which is updating the ICANN community on where that group is up to. I don't know what the outcome of the meeting was, but I will be checking on a webinar. So that's the latest update on where we're up to. Next slide, and I think it's the final slide. No.

For those who have not been following the whole WHOIS debate all the way to the WHOIS RDS, there have been any number of working groups, and this is the main one starting I think about eight years ago there was a survey requirement. We've had a lot of discussion on privacy proxy accreditation, which is really all about if you do not want your data made public and you want to use one of these services, what are the rules regarding if you can, how you can, what information is made available and who gets access to the information.

Throughout the whole RAA negotiation which resulted in the 2013 RAA, there was a lot of discussion about privacy proxy and about the accuracy of registration data, because people wanted to hide. I've talked about the WHOIS Review Team. Thick WHOIS was about the registries and whether they should also carry all of the registration data or only some of the registration data and not including the personal information.

I've mentioned the privacy proxy services waiver in terms of how you say I have to comply with my national laws, so how do I get out of my RAA responsibilities? And as I've told you, that wound up – months later – saying, "Well, the process doesn't work," and we've just amended it and it doesn't work either, to be truthful.

The RDAP was about the registration data protocol. It was updating the protocol and whether the use of that protocol should include the concept of gated access, which is what the EWG recommended. Turns out it didn't, actually. And then I mentioned the EWG.

So for those of us who have lived in the WHOIS world, there are any number of working groups that have discussed this issue, and I have to say we're still not at the stage where we have a working group that is yet going to change the RAA, but we're working on it.

And Carlton's assessment of the likely end date for our RDS Working Group is two years' time. Next slide, which is questions. Any questions? There's a lot there.

TIJANI BEN JEMAA:

Thank you very much, Holly, for this wonderful presentation. Let's say this very detailed presentation. Yes, if there is any immediate question, yes, please. I don't see any hands. If there is not... Yes, Olivier. Go ahead, please.

OLIVIER CRÉPIN-LEBLOND:

Yes. Thank you very much, Tijani. I just wanted to ask a question with regards to this gated access. When one looks at all of this theoretical stuff, it all looks absolutely nice and proper and all this, but when you actually get down to the implementation of it, we all know what's happened with the new gTLDs – as I by the way despair in recent days to have thousands of messages from .streams, .trade and .bids, gTLDs that are likely to be banned from our servers shortly because they're just not respecting rules.

You're having all these rules that would one day be implemented one way or the other. It seems to be very complex in a certain way, and at

the same time, it seems to be that it all requires a big master database that will be in the background. Two questions on that.

First, the master database itself I gather would have to be absolutely secure. What happens if that master database of all details that would be available – including the details for law enforcement, etc. – what happens if that leaks in the real world? And we know that this is entirely possible.

And secondly, what stops anyone from marketing this database, from actually monetizing it? Because we know we live in a world – especially in ICANN – where everything seems to be monetized. So, have you guys considered monetization and all that, or is that out of the question? And how would it be stopped from happening?

HOLLY RAICHE:

Okay. First, one of the criticisms of EWG that a lot of people made – and including if you talk to people like Andrew Sullivan and Scott and others – the first thing they'll say is there should not be one database, because that would be like a honeypot. Everybody will go there and it'll be hacked within five minutes.

That the way to deal with that would be every registry only hold the data that's relevant for that registry, and so instead of having one database, you have several databases. Now, we're so far from discussing that, I can't tell you. But there are a lot of people I've talked to who, like you, share a great deal of apprehension about there being one database, and simply have rules regarding each repository of data

having the same rules. That raises a range of other questions, but I have to say I think a lot of people share your concern about one database. That's just really too dangerous.

In terms of marketing, if you look at the RAA, currently the RAA already says you shouldn't be using this stuff for marketing. So you'd have to look at the RAA and say, "Well, do we need to strengthen those rules as well? Because it's already against the rules." Now, that doesn't stop anybody. And the next question would that be, "What is the role of ICANN Compliance in terms of the misuse of data for marketing?" That's probably one of the really good questions.

And theoretically, gated access should stop a lot of the use of data for marketing, because marketing would not be considered probably as an accredited purpose for which you should gather information. And when it comes to uses, which are followed per purposes, I would imagine that would be one of the things that we would be saying. Does that answer your questions, Olivier?

OLIVIER CRÉPIN-LEBLOND: Yes. Thank you very much, Holly. Let me just tell you a little story. I've held some .com domain names for a very long time, since '95. And at some point, I started receiving marketing e-mails from the very registry that had sold me those domains through their registrar. I complained to ICANN, I sent a report to the Compliance department, and at the end of the day, it was filed as that was not a breach as such because it was about the registry and the registrar dealing with their own customers.

So it's kind of more of a customer database, and it didn't come out from WHOIS.

Interesting, but the loopholes here are things that I think you might have to check on this, because I don't see this as – you mentioned marketing. I said monetizing, and I'm very concerned that there is an opportunity here for contracted parties to monetize this thing of having another database or parts of databases with even more information in their power that they could actually sell elsewhere. And how the hell would we know if they're selling it or not?

That's a big concern that I have on this. And just to finalize this, the last question then for you is, who owns that database? Because I think the ownership is going to be really important, because whoever owns it is owning a lot of money. You know how it's all worth so much these days. Thanks.

HOLLY RAICHE:

Okay. First of all, monetizing. I'd like to say that Australia has solved the problem. We haven't. And I imagine most other countries haven't with their own country codes. I don't think that having a WHOIS database restriction is necessarily going to address that problem. And given that the topic that what the implications for end users, I think that's a debate that ALAC should have, actually, and I'm not sure that it's just a problem about WHOIS. I think it's a larger problem, frankly, and I think it's a problem of looking at the RAA and Compliance and saying, "Well, what do we do about this?"

And in terms of ownership, my gut feeling – lawyers always say this is only an opinion, and so I'm a nonpracticing solicitor, I'm saying this is a nonpracticing solicitor's opinion. ICANN doesn't own the database. They don't hold the databases. I think you'll find the data controller is going to be the registry or the registrar, because they're the ones that have that contractual relationship with the registrant.

But in a sense, ICANN has control, because in relation to the new gTLDs, the reason the information is being collected is a contractual relationship between the registry or registrar and ICANN. So ICANN has some responsibility in that, although probably not ownership. Now, take that as a nonpracticing solicitor's nonbinding legal opinion. Okay?

TIJANI BEN JEMAA:

Okay. Thank you very much, Holly. Thank you, Olivier, for those questions. And Alberto Soto wants to ask a question. Alberto.

ALBERTO SOTO:

Hello. In relation to Olivier's remark, whenever there is any legislation on database uses in countries, there is typically a segmentation, first of all, of personal data. Personal data segmentation. There is some data that is entirely public, and other data that is typically defined as sensitive data.

That might be a way to divide, to provide segmentation to databases, and even located in different physical locations. For instance, if I have data one to ten in ABC, one from two would be entirely public, three to

five would be just accessed by those who are accredited to request that data, and from then on, only according to the law.

I know that what law provides will certainly be on which piece of legislation is applicable in each country, and that is the problem, that it is decided by the owners of the ccTLDs. Thank you.

HOLLY RAICHE:

Thank you, Alberto. The system of gated access that the Expert Working Group talked about adopts that concept to say, basically, there's some data that can be public and some data that can't be.

Now, the data that is not related to an individual – and when I say that, remember that the definition of personal information can include information that points to an individual as well as being the name of the individual. But that information, only basic information under the EWG, possibly a person's name, would be available. A lot of other information would be not accessible except to people who have a legitimate reason or purpose to access that information.

Now, that's what the current RDS Working Group is working through, and that is, what information should the registries and registrars be collecting in the first place that's necessary? And then the next question would be, "Okay, well, what purposes should it be used? And then who gets access to that?"

So conceptually, it's not that different to what you're arguing. And I have not talked about the ccTLDs, because each ccTLD will have rules

that reflect individual countries' rules about protection of personal information, and access to that information.

So this is only in relation to new gTLDs, but it is because they are so widely used, it will be important to get these rules right. And some of the issues that are being discussed are the ones that were raised by Olivier as well. I hope that answers your questions. Thank you.

TIJANI BEN JEMAA: Thank you, Holly. Any other question before we go to the pop quiz questions? Yes. Dev, go ahead.

HOLLY RAICHE: I've –

TIJANI BEN JEMAA: Yes, Holly.

HOLLY RAICHE: I'm just pointing out to Raymond how the committee members for various groups are selected. If you really want to be part of this working group, put your hand up and you can be #141. And you're most welcome.

TIJANI BEN JEMAA: Okay. Thank you very much. Dev.

DEV ANAND TEELUCKSINGH: Thank you very much. This ties in exactly to what Raymond was alluding to. Is there an At-Large Working Group that is looking at the WHOIS and the NextGen, and therefore regularly meeting, so that at least I can begin to get a sense of all of the issues related to the WHOIS issues? And also, how do you join such a working group within At-Large?

HOLLY RAICHE: The At-Large does not have a specific working group. We had the registration data, and the only issue on the Registration Data Working Group is this WHOIS thing, and Carlton and I are members. And we talk to each other a lot. But at the last ICANN meeting, I gave a presentation on WHOIS. I'm absolutely happy to have meetings – informal or otherwise – and continue this debate. It's going to be a long debate, Dev. Just as I listed the issues, we're still stuck on purpose. We haven't even got to users yet.

But look, if you would like a meeting of the working group, absolutely happy to arrange it and continue this dialog much more broadly. It's just people like Olivier throw their hands up and go, "Oh my gosh, this raises so many issues." And it does. It really does. So, I think I've just grabbed you as a member. Is that okay?

DEV ANAND TEELUCKSINGH: Okay. Well, I would say I would like to be a member, but I have to admit, my time is limited. That's why I was asking if there's a working group

where I could follow the discussions. I am on some of those GNSO working groups as an observer.

HOLLY RAICHE:

Okay. As I said, Carlton and I – and in fact, we should be putting Alan on there too, because he’s a member of the WHOIS group that was convened by the ICANN Board to say, “Look, this is a really urgent issue. The May 27, 2018 date is coming up where there are going to be fines doled out and so forth for everybody who breaks the GDPR.”

I’m not sure where that progress is up to. They’re having a meeting in Brussels, and there was a webinar last night that I haven’t seen. But that’s just another piece of the puzzle, and I’m not sure where that’s up to right now. I hope that helps.

TIJANI BEN JEMAA:

Thank you, Holly, and thank you, Dev. Olivier has another question.

OLIVIER CRÉPIN-LEBLOND:

Yes. Thanks very much, Tijani. Actually, no, just to comment on the At-Large Registration Issues Working Group. I thought it was still in place, but I stand corrected. I found out it’s been archived in 2017, so it no longer exists, which is quite unfortunate when this is such a hot topic. So I’m a little miffed about this, and interpreters will have to look at the word miffed. It’s a colloquial English term for someone who’s not too happy.

I also notice that the At-Large Technical Issues Working Group issue is archived at the time when we're dealing with key rollover and we have problems with the spreading of the key rollover. But there you go. Anyway, just a little rant. Thanks.

TIJANI BEN JEMAA: Thank you, Olivier.

HOLLY RAICHE: In reply to Olivier, I would say that Carlton and I and Alan are just plugging away on the WHOIS, and I think people have – I won't say they've lost interest, but it is such a long process and the issues are so [interactable.] And the people who want access to people's individual information are very adamant that they should still have it. The people who believe that they shouldn't have it are equally adamant. I can say that in 90 minutes, we don't make much progress, and sometimes we go absolutely backwards.

So, Olivier, if you want to sit in on those meetings, you're most welcome. But look, I'm absolutely happy to keep people up to date. But I have to say the progress reports are going to be very boring. I hope that helps.

OLIVIER CRÉPIN-LEBLOND. The question is, how do you get the input of the end users into these processes when the only solution now is to sit through these really boring 100-something meetings of the Cross-Community Working

Group? That to me is not the way to do it, because not everyone is an expert and not everyone has 10,000 hours to spend on these boring groups. So I'm just very surprised.

HOLLY RAICHE: I know. And that's –

OLIVIER CRÉPIN-LEBLOND: And [inaudible] where one has their local working group that can update the local community once a month and say, "Hey, this is what's happened in the past eight calls of the Cross-Community Working Group. You're so lucky not to have been on there, but this is what we've done." It would have been a lot more helpful than doing this. But okay. Thanks.

HOLLY RAICHE: No. Look, I will take that as a severe scolding for myself and Carlton. I think we've tried to keep people updated. I'm not sure that – I think it's part of a larger problem. We should be requiring every single working group to report, if not monthly, quarterly. Something that says, "Well, this is what we're stuck on and this is the issue. Same issues as last month, or not. But it's going to be a time-consuming group." So, Olivier, you're quite right. My apologies.

TIJANI BEN JEMAA: Okay. Thank you very much, Holly. Any other question before we go to the pop quiz questions? I don't see any hands, so Mario, please, can you go to the pop quiz questions? No, before, we have Alberto Soto. Alberto, please go ahead.

HOLLY RAICHE: Oh, no. I think he's just taken his hand down.

TIJANI BEN JEMAA: Okay.

ALBERTO SOTO: Thank you very much, Tijani. Holly, when you talk about that single database, are you talking that it will be physically located – and excuse my words, but I will try to be simple and straightforward – will it all be placed in a single computer, or are we talking about a database that is partitioned and is located in different computers and at different supplier facilities? Thank you.

HOLLY RAICHE: Thank you, Alberto. I don't think we've gotten to that detail yet. Taking a lead from Olivier, I would be horrified if I thought all of those names were in the same database in the same place. All we're doing is saying conceptually, would there be one database managed by a particular organization or ICANN or something, or would the idea of each

registry/registrar managing their own database and managing gated access?

Now, that has the idea of a distributed database which is far less dangerous, but it does raise issues about who would manage, who would oversee, what the rules would be, who would ensure there is compliance. So, there are probably arguments on both sides, but I think in terms of a single supplier, clearly there'd be data held in escrow, of course, but where it physically would be, who physically would manage – we haven't got there yet.

You can look at the Expert Working Group final report, but I think it's at a conceptual level at this stage. And the mandate of the RDS Working Group, the mandate really is to have a good look at the EWG and other issues, and come up with policies that better reflect both the growing privacy rules and the way that the data is used now. Okay? Thank you.

TIJANI BEN JEMAA:

Okay. Thank you very much, Holly. I think that even if you go with the single database as you just described, managed by another party or by ICANN, this will not prevent registrars to have their own database, since all the data will come from them, and then they can [inaudible] those data and have their own database. So it is a very complicated situation.

HOLLY RAICHE:

You're so right.

TIJANI BEN JEMAA: Thank you very much. If there are no other questions, we will go with Mario [for the pop] quiz questions. Mario, please.

MARIO ALEMAN: Thank you, Tijani. We'll be running [three] questions of our pop quiz, and here is the first one. What is WHOIS? And we have four different options. A) the protocol, B) a service, C) a dataset, and D) all of the above. Please cast your votes. Thank you very much.

Moving on to the second question, it is personal information under the GDPR does not include IP addresses or online information. Is this true, or is this false? Please cast your votes now.

HOLLY RAICHE: Yay. Good.

MARIO ALEMAN: Thank you very much. And Tijani, are we going to the end of the questions to the right answers? Is that correct? Okay, we'll finish the three questions. Yes, please go ahead, but we can do it at the end actually and review them. Number one, number two, number three.

HOLLY RAICHE: Okay.

MARIO ALEMAN: Thank you. Question #3 is under the GDPR, all access to personal information held by the data controller is not allowed. And there are two options: true, and the second option is false. Thank you very much for all who responded to the pop quiz. We're now going to be back to the first question, and Holly will have [inaudible] which is the correct answer.

HOLLY RAICHE: The correct answer is D, all of the above. If you remember my second slide, which basically says the SSAC very early in the piece said, "Look, WHOIS means very different things. It actually means the protocol, the service. Next slide. Next slide." So, WHOIS really is three things. It's the data, it's the protocol, and it's also the service.

And the reason that SSAC said we've got to be much clearer in our language is because if you just use the term WHOIS, you're not being clear as to whether you mean the actual data that's being made public, the protocol by which it's being made public, or the actual service that makes it public. So, next question.

MARIO ALEMAN: Thank you, Holly. Could you please provide your correct answer for the second question?

HOLLY RAICHE: Right. Personal information – remember, I read the definition of personal information. And I don't remember the slide, but it's towards

the end. Basically, it's much broader than simply [inaudible] some people's names. And they specifically do list online information. And there's a recent decision of the European Court of Justice that makes it very clear that actually, it includes IP addresses as well. But the definition on the slides makes it clear it's talking about information that's online. Okay, next question.

All access to personal information is not allowed. Well, maybe that's a little tricky question and I could have phrased it better, but in fact, access to personal information is generally allowed, at least to all law enforcement agencies. And when we talk about that – it's one of the slides, and I forgot which – basically says, well, law enforcement agencies are generally exempt from the requirements of the GDPR, and that most privacy protection laws internationally always have an exemption for probably defense and law enforcement agencies. Okay.

MARIO ALEMAN:

Alright. Thank you very much, Holly. Tijani, back over to you. Are you still there, Tijani? Okay. [inaudible]

TIJANI BEN JEMAA:

Sorry. I was muted, that's why you didn't hear me. Thank you very much, Holly, for the answers, and thank you, Mario, for the pop quiz. Now, is there any other question for Holly? We still have time for that. I see that no one raised their hands, so we will go to the evaluation questions, Mario.

MARIO ALEMAN: Sure. Thank you, Tijani. We're going for the first question. How was the timing of the webinar? And we have three different options: Too early, just right, too late. Thank you very much.

Moving into the second survey question, how is the technology used for the webinar? I appreciate it for your votes, and we'll move into the third survey question. Sorry, this was the wrong one. This is the correct one. Did the speaker demonstrate mastery of the topic?

TIJANI BEN JEMAA: Bravo, Holly. [inaudible]

MARIO ALEMAN: Very good, yes. We're having 100%. You did a good job, Holly.

HOLLY RAICHE: Tijani you owe me a cup of coffee.

MARIO ALEMAN: The next question, are you satisfied with the webinar? Good. Very good. We're going to survey question #5. What region do you live in at the moment?

TIJANI BEN JEMAA: Holly, you are very poor on this question. Nobody [inaudible]

HOLLY RAICHE: [inaudible] Look at the perfect time for Asia Pacific.

MARIO ALEMAN: I think we're complete with the #5 and moving into the #6. Any final comments?

TIJANI BEN JEMAA: So, those comments, even if you don't feel them now, you can send them to the staff. It is preferable that you put them on the Adobe Connect, but if you don't have time or you remember after the webinar any other comment, you can send them to the staff. It'll help us very much to improve our work. Okay. And this is the final question, isn't it? Yes.

MARIO ALEMAN: We are going to move to the final question now, which is, what topics would you like us to cover for future webinars?

TIJANI BEN JEMAA: And also, this question, if you can put your proposals now on the Adobe Connect, it will be perfect. Otherwise, if you remember or if you want to suggest topics after the webinar, you can send them to the staff, and this will help us to program the topics that you ask for for the next year.

So, last call for questions. We still have eight minutes, so if you have any question now for Holly, please don't hesitate.

HOLLY RAICHE: They can send me questions as well. And based on what Olivier says, at the ICANN meeting I'm very happy to report back on where we're not up to and where we can move forward.

TIJANI BEN JEMAA: Okay. Thank you very much. So if you have a question for Holly, you can send it also by e-mail to Holly or to staff, and staff will forward it to Holly. So I see that there are no other questions. I will thank you all very much for attending this webinar.

My special thanks to Holly to accept to make this presentation and to deal with us during one hour and a half. And she did a magnifique work. Thank you very much, Holly.

My thanks also to our interpreters and to our staff who are always helping us to do our webinars. Thank you very much. Thank you all, and this webinar is now adjourned.

HOLLY RAICHE: Thank you, Tijani. Thank you.

TIJANI BEN JEMAA: Thank you, Holly.

MARIO ALEMAN:

Thank you, Tijani and Holly, and our interpreters too. Please remember to disconnect all remaining lines. This webinar has been adjourned. Bye-bye.

[END OF TRANSCRIPTION]