Transcription ICANN London
Privacy Discussion Hosted by the Non Commercial Stakeholder Group (NCSG)
Wednesday 25 June 2014

Note: The following is the output of transcribing from an audio. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

On page: http://gnso.icann.org/en/calendar/#jun
The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page

Man: It is 3 o'clock, Wednesday, June 25. This is the sovereign room and we are starting the privacy discussion hosted by the noncommercial stakeholder group, NCSG.

Woman: Yes, no, there's (unintelligible).

Rafik Dammak: Okay, sorry, we'll just spend two minutes. So I'll encourage everybody to seat at this big table. Yes.

((Crosstalk))

Rafik Dammak: Don't worry. Okay, so we'll (unintelligible) - come to the front. Yes, (unintelligible), yes. No, I didn't call you. Why I will call an Irish which is (unintelligible).

Michele Neylon: Rafik, I love you too.

Rafik Dammak: Okay, thanks. Which one? Okay, so let's start. So my name is Rafik Dammak, I'm the Chair of the Noncommercial Stakeholder Group. I'm really happy that we have you here today to talk about privacy issue within ICANN. It's (unintelligible) to say that ICANN has a few issues, there are a lot of issues regarding privacy and things that (unintelligible) to bring many people

from outside the ICANN community to get some insight into what's happening here in terms of policy and the impact on data protection privacy.

I'm not privacy expert. I'm just a computer engineer. But we have a lot of - I mean many people within our group who are interested and they fight a lot about privacy in ICANN.

So I'm not going to speak much more and we - maybe we'll try to have self introduction - self introduction through - to the table starting from the right with - from our friend from Germany. Sorry, can you just introduce yourself? I mean quickly and then we will...

(Sven Herdsman): Hello, my name is (Sven Herdsman) from the German association for data protection and privacy.

(Bob): Hello, I'm (Bob) (unintelligible) from the Association for Technology and Internet in Romania.

(John Laprese): (John Laprese) from Northwestern University.

(Julia Powell): (Julia Powell), University of Cambridge.

(Katherine Microson): I'm (Katherine Microson) from ccTLD (unintelligible).

Man: (Unintelligible) from the University of (unintelligible).

(Gail): (Gail) (unintelligible), federal security resource from (unintelligible) Institute, Germany.

(Mona): (Mona) (unintelligible).

(Alex Decan): I'm just curious if I can opt out? I'm just kidding. My name is (Alex Decan) from the Motion Picture Association of America.

(Chris Lahan): (Chris Lahan), ICANN ombudsman.

Robin Gross: I'm Robin Gross with the Noncommercial Stakeholders Group.

Milton Mueller: Milton Mueller, Syracuse University, Internet Governance Project.

(Stephanie Perrin): (Stephanie Perrin), I'm on the expert working group at ICANN that's looking at the renovation of Whois, also with the University of Toronto.

(Hannah McLaughlin): (Hannah McLaughlin) from the Information Commissioner's Office, UK.

Man: (Unintelligible) from the (unintelligible) Office of the UK with the UK (unintelligible) protection authority.

Man: My name is (unintelligible) from the European Data Protection Supervisor.

Woman: (Unintelligible), association for (unintelligible) communications and member of the (unintelligible).

Bill Drake: Bill Drake, University of Zurich, Chair of the Noncommercial Users Constituency.

(Deborah Deamer): (Deborah Deamer), (unintelligible) team, member of the NCSG.

Woman: (Unintelligible), privacy international.

Man: (Unintelligible), privacy international.

(Chris Parsons): (Chris Parsons) with the (unintelligible) University of Toronto.

(Kevin Macarthur): (Kevin Macarthur) at (unintelligible).

Michele Neylon: Michele Neylon, I don't know which group I'm supposed to be representing today but anyway...

Woman: Expert working group.

Michele Neylon: Okay, expert working group, registrar - happy to chair the registrars, European registrar, and finally one who actually managed to extricate a waiver from ICANN.

Holly Raiche: Holly Raiche (unintelligible). And I suppose member of the privacy proxy server working group.

Michele Neylon: (Unintelligible).

Holly Raiche : I know, (unintelligible).

Kathy Kleinman: They've never met before in their lives. Kathy Kleinman, I'm an attorney with the firm of (Fletcher, Hill, and Hildred) in Washington, D.C. And I'm with the noncommercial stakeholders group and I was also vice chair of the Whois review team that met 2010 to 2011.

(Patty): (Patty) (unintelligible), Center for Technology and society of (unintelligible) in Brazil, NCUC, NCSG policy committee.

Man: (Unintelligible), International Society of Hong Kong.

(Frank Tellen): (Frank Tellen) with the Global Intellectual Property Center for the US Chamber of Commerce.

Rafik Dammak: Thank you, that was quick. Just I want to remind everybody here that this session is recorded and it will be available online in transcript and so on and also people can participate remotely.

Okay, so to move on - so as you say, you can see in this screen our agenda as we will start basically by introduction about privacy issue and this will be led by (Stephanie Perrin). And then we will have kind of really brief history about Whois privacy issue and it will be done by Professor Mueller and Kathy Kleinman.

And then we will go more to real (unintelligible) and going to (unintelligible) about expert working group having some members here and then we will kind of - presentation, discussion. We will then have an open discussion and hope that the audience here will ask a lot - many questions to the speakers.

And then we will have a break. And we will continue at the end by a session to really kind of agree or discuss on some action to follow up. So then we will start with the first session with (Stephanie).

Stephanie Perrin: Rafik has told me to be concise and brief. So for the record, Stephanie Perrin. We have vacant seats at the table so please don't be shy. This isn't the coziest room but the concept here was that we would have a free and open discussion about the privacy issues.

So if you'd like to join us at the - up at the table, please do. And don't be shy about going to the microphone. I think we only have one but we'd like to hear from you.

I think - can we pull up the slide, the summary of current privacy issues at ICANN? I hope we can. I'm going to leave it to folks here on my right to figure this one out. I'm going to get talking.

What we have here is a very brief summary of some of the key privacy issues that are before us here at ICANN. The first and probably the most prominent one at the moment is that the expert working group - I'm a member, Michele's

a member, and I'm hoping we will have a couple more people arrive from the group to talk about what we've been doing.

We've been working for the last 14 months on what is kind of a perennial problem at ICANN, namely the Whois directory and from a privacy perspective the expectations of privacy within that directive. That's not the only privacy issue at ICANN and invite Michele to weigh in on his when we get there.

So the EWG did release its report this week. I was - some would say the lone privacy person, others would say one of the privacy people on the expert working group. And unfortunately I did dissent and the dissent is up on the ICANN pages. We can talk about that a bit later in the discussion period about some of the long standing issues here.

But we would certainly like to discuss those issues with the experts that we've gathered here today.

One of the recommendations - this is Item 2 on that list of issues is we have a - we have a wonderful proposal in the experts working group for secure credential for anonymous domain name registration. So this was a recommendation to protect individuals who are at risk.

So journalists in hostile territory, people who are fleeing abusive partners, religious groups, whatever; we have a list of five basic categories in the - in the report. And the concept is that we would make use of secure cryptographic credentials to allow an anonymous domain name registration.

Now frankly, if you're under threat from someone or you're a journalist or blogger in a hostile country, really your domain name registration is the least of your worries.

But ICANN has a responsibility to look after those pieces of the puzzle and the registrars are faced with the pursuing party, whatever that may be, showing up at their gate and asking for address information and contact information.

So fixing this problem is probably the easiest part of that whole solution. And we look to civil society to help fix all the other problems such as where your web is hosted and how you're managing to be tracked through sniffing and all the rest of it.

So that is one recommendation that we're actually looking for help in civil society. I'm not speaking as a member of the expert working group here, I'm speaking as a member of the NCSG. We'll be looking at that as a major focus of our work.

The third item on our list, we also recommended investigating the drafting of a privacy policy to govern the RDS or the replacement for Whois. And the NCSG has been working on basically a critique of the privacy policies that ICANN currently has. They are - (unintelligible).

They are scattered throughout the ecosystem. So there's one for, you know, your web cookies and there is - there are elements of it in the registration agreement. We think they should be pulled into one comprehensive policy. I'm going to say we, I'm speaking to the NCSG.

So we're working on that and we'd love volunteers on that project because it's quite a bit of work. But we're trying to make a positive contribution to the ecosystem here.

So the fourth item is privacy proxy services and there is an existing working group on the accreditation of privacy proxy services at ICANN. I see quite a few members of that group actually around the room. The privacy proxy services are the key mechanism right now if you want privacy at ICANN.

You hire a privacy proxy service. They put their information into the Whois and that prevents spamming and immediately having people show up on your doorstep.

So those services are being accredited in accordance with another contractual obligation that came to the 2013 RAA. Michele, jump in and correct me if I misspeak here on how that arrived. And that working group has been going for six months and probably will continue for...

Michele Neylon: It has to end - I'm sorry, Michele Neylon for the record. It has to reach it's inclusion by a particular date in 2017. James Bladel or Volker might be able to confirm the exact date, 2017 has to be done.

Stephanie Perrin: If you had told me I was - could be signed up until 2017, Michele, I wouldn't have joined because I'm an old lady but anyway. Let me see now.

I think I've already talked about the ICANN privacy policy and ongoing issues with respect to how the ICANN governs the registrars and permits them to opt out of the 2013 RAA, now this has been the subject of certain letters back and forth to ICANN from the data protection authorities.

And who would like to speak about - Michele, would you like to talk about that? I can give you my view. Basically what happens in ICANN is if you are a registrar and you believe that you cannot gather and release and escrow the data as required by the 2013 RAA you apply for a waiver. So I see Michele going - not quite. Tell us.

Michele Neylon: Thanks, Stephanie. The - it's not quite that simple. The - under the 2013 RAA there is an option - I'm not even sure option is the correct word.

Stephanie Perrin: A requirement I think is what you think.

Michele Neylon: Well, no, there's - you can request a waiver around the part of the data retention requirements. Now as far as most Europeans are concerned, under - and we've all read the letters that Article 29 and others have written, the data retention requirements in the 2013 RAA would be incompatible with both national law and European law, but trying to persuade ICANN to actually give a registrar a waiver based on that is far from easy.

The - so far to date, over a dozen registrars have applied for waivers using this process. To date, I think maybe five registrars have been granted one so that means there's still seven or more registrars waiting for it.

The way ICANN approached it was that each - if a registrar in the UK applied then any of - was granted one, then any other registrar within the United Kingdom could apply to ICANN to get the same treatment. But there was no facility that would automatically give all registrars in the United Kingdom the same conditions without going through that process.

Stephanie Perrin: Right, thanks very much, that provides more needed detail. And the - a wonderful thing about ICANN for those who don't normally participate at ICANN is most documents are freely available on the website.

So you should be able to find out there the letter from the European Data Protection Supervisor advising ICANN that indeed, the Court of Human Rights has thrown out the escrow requirement - the data retention directive and that therefore we need to reexamine that.

So that is a nice segue into one thing that is not on this list because we only learned of it yesterday. The Council of Europe has released a report on ICANN's policies and procedures with respect to human rights and data protection.

And we are working our way through that report right now and the NCSG has made a commitment that we will provide comments and consider it in the light

of what's going on at ICANN. Now that includes not just privacy but also freedom of expression and several other fundamental human rights.

So that's an interesting new development. I believe it's dated June 14 if you want to look for it on the European - the Council of Europe website. But we can give you the link, thanks. And I think with that I'm going to turn it over to get the history of Whois.

Milton Mueller: Right, so this part of the program is brought to you by Kathy Kleinman who's working her way up to the top, and myself, Milton Mueller. Do you want me to start, Kathy? Or are you going to start?

Kathy Kleinman: I think you're doing ancient history so you start.

Milton Mueller: I'll start. It's actually not that ancient. The more you look back at it the more you realize that we've been banging our heads against the same issues for 14 years now. Essentially Whois was created as a directory service when the Internet was a small trusted group of computer scientists who just wanted to look each other up.

As soon as the Internet and particularly domain names became economically valuable, particularly around trademark and domain name conflicts, the Whois became an important - as what I'm going to call a surveillance tool.

That is you had no real identification system on the Internet and so the only mechanism that people had to use to track people down for service of legal process was the Whois record.

And because the trademark interests put a lot of economic stakes on to this and then they were joined by law enforcement interests, there became more and more pressure on Whois and more and more viewing of it as a strategic point for policy.

So the demand for accuracy in Whois data - of course, you can find earliest debates about this in ICANN back in 2000, the year 2000, with certain interests demanding that we somehow make the entry of data into the Whois more accurate.

And of course, there was pointed out the time that because this data was visible to anybody and everybody on the Internet that many people put in inaccurate data deliberately, both for nefarious purposes or for perfectly legitimate purposes of shielding themselves.

Now of course, we are using the denial of a domain to enforce accuracy as well as various kinds of verification that is all compulsory and put into the registrar accreditation contract.

We've also had long debates about the purpose of Whois data. We - as soon as the sort of privacy advocates within ICANN realized what a disaster was taking place around Whois we began to invoke these data protection principles and say, well, let's define what the purpose of Whois is and that will tell us what data needs to be out there and what data doesn't need to be out there.

And so around 2005, 2006 we had a long debate about the purpose of Whois and it's interesting to note that by a two-thirds super majority the GNSO actually agreed on a new definition of the purpose of Whois, which said that its purpose was simply for technical issues.

And this agreement was actually vetoed by certain members of the GAC who decided that they didn't like that. They wanted Whois to continued to be used for law enforcement purposes and other kinds of purposes, basically any purpose somebody wanted to use it for. And so we never got that new definition of purpose.

Indeed, the restrictions or the - on entry of data into the Whois through verification and data retention have intensified and you can look at the expert working group report as sort of the - taking of this trend to its largest conclusion.

I just want to conclude by saying that I personally am not convinced that this whole experiment will work because I view the expert working group idea as an attempt to reconcile two fundamentally irreconcilable things.

The Whois as a very powerful surveillance tool that can be searched and accessed almost at will by certain privileged people for purposes of law enforcement and identification and the attempt to shield personal data. And the better the Whois is at one, probably the worse it is at the other.

Now you can make a case, say you can reconcile these two things and that's certainly what we need to be discussing here today but with that I'll turn it over to Kathy.

Kathy Kleinman: Thanks, Milton. Kathy Kleinman and it's a pleasure to see so many people here. This is an issue indeed that we've been discussing since the founding of ICANN and we didn't inherit a database.

We inherited the Whois when I talked to - as Milton has done and let me just confirm, when I talked to the people who were part of the original Whois, there were people like (Scott Bradner) Whowas the original IT person for Harvard.edu back when it was (unintelligible).

And there was nothing personal about the data other than his name that was in the database. This was his office at Harvard. It was his office phone number. And it was his office email address.

By the time I entered the picture, which was slightly before the founding of ICANN this was material - 1996-97, this was material that was now home

addresses, home addresses of small organizations, small businesses, individuals, home phone numbers, home cell phone numbers, home email addresses - or personal email addressed now published in a 24/7 global database.

So we did start asking questions. And over time we've had commentary from Mr. (Buderelli), secretary - he was then Secretary General of the Italian Data Protection Authority; also (Peter Shar) Whowas then Chairman of the Article 29 working party have commented to ICANN that - or Whois policies aren't quite kosher, that they needed to be revised, they needed to be brought into plague given how much personal data within these databases.

I've been circulating a paper - I was kind of asked to say what is the existing Whois policy. And that was the same question that James Bladel of GoDaddy and I were asked on the Whois review team.

So you see something that's titled - and there's some copies of it back there, Part 2: ICANN's Whois policy and it's implementation. This is actually Chapter 3 of the Whois review team's final report from 2011. And it's called the complex history of Whois policy.

And so we tried to put this together and we tried to put together the Whois policy as it existed in ICANN at the time. And we were a review team. We met for 18 months. We came from every stakeholder group as well as other committees within ICANN.

And so what we did was we found that the Whois policy is actually buried in the contracts of the registry and registrar agreement. And we had to find it and pull it out and pull it together.

So this is kind of where things are now except that it's even been modified more by the 2013 registrar accreditation agreement or you'll hear it referred to as the 2013 RAA.

But indeed, it was complicated and what people have to do and what was buried and many people don't know that their data when they give it for domain name registration that their data was published in the Whois directory and available. And available on - in both bulk basis as well as individual queries.

And so again, I think copies are gone now but particularly if you have questions let me know because what we were a little surprised at was after 18 months of work where we created a number of recommendations that had to do with accuracy and access and making Whois a priority, a strategic priority and really working on it, one of our big recommendations was outreach, that there were a lot of the people in the world who cared about data protection, privacy, speech issues.

And - as well as law enforcement that we should be reaching out to that are aren't following the ICANN bubble and we should be doing outreach. You'll have to tell us whether that recommendation went into effect and whether you heard about some of the more recent privacy and Whois issues.

Because we said whenever you work on Whois make sure you reach out to the data protection communities, make sure you reach out to the law enforcement communities.

So we were a little surprised when almost on the heels of when we finished our work a new group was created to look at similar issues of Whois and privacy and that was the expert working group that has come up with its own set of recommendations that significantly changed the world.

And (Stephanie), I assume we're going to be talking about that a lot, the creation of a centralized database of Whois in what has been a decentralized world so far.

Whois data traditionally isn't spread between registrars and registries and now the idea of one database for all this information basically created to serve it up with not just fewer fields, actually more fields. Very interesting proposals and we certainly need everyone's evaluation. We need everyone's input on this. Thank you.

Rafik Dammak: Thanks, Kathy, that was informative. So we'll go to the next item, which is about the expert working group and several members here. So - sorry. Okay. Before that (Michael), yes?

Man: Do you want to...

Rafik Dammak: Okay, I am getting to many requests (unintelligible). So first, (Michael) will want to make additional comments about the history.

(Michael Neble): Just to follow up on Milton - on what Milton said. Two aspects, one is - (Michael) (unintelligible) for the record. On ccTLDs, in Paris 2004 I was perfectly free to have - to define for (unintelligible) a very limited purpose, a very limited purpose with a very limited set of data appearing publicly. So that is one thing.

Milton rightly said that in the GAC some - there was some resistance to limitations. I can testify that in the GAC there was this tension between what you described as almost a not reconcilable - the privacy and the law enforcement issues.

But what is probably - has to be said, it's not only that there was some resistance. The GAC adopted principles, GAC principles, in 2007 at the Lisbon GAC meeting, which was kind of extending the purpose according to more or less the users. This includes basically law enforcement but also IPR and other things.

So I think that has to be added. There is a statement of the GAC which is rather wider than just technical stability and that is something that we had started with - we went into the (EWGT).

Rafik Dammak: Thank you, (Michael). Before going to the expert working group report maybe we can get some question from the audience or ask - I mean they want to ask some clarification. Do we have the mic and the minutes? Please don't be shy. Yes, and we start with Avri Doria.

Avri Doria: Thank you, Avri Doria speaking. One of the questions I had - and it came up when (Fadhi) was speaking the other day is somehow already talking from the presumption as if we already had a directory service and that we had somehow already approved a directory service.

In all the time that I've been here, even when we had the - what is the function of the Whois, it never came out as being a directory service. We never went beyond the original definition of (Scott Bradner) and everyone else in the Whois, that it was for functional - for solving technical problems.

So I guess I'm wondering where did the - at the expert working group and all these other folks like (Fadhi) get the impression that there was an approved notion of a directory service that should exist at all. Because I know in my years in the GNSO we never approved one.

There's sort of been this assumption that Whois was used that way but all of a sudden there seems to be a presumption that, of course, we have to have one. And I don't understand where that comes from.

Woman: Rafik, may I? Avri, you raised a good point. I was shocked when I saw the change from Whois to directory services and the assumption that we were offering - that all this data that had been collected for what we thought was operational and technical purposes was now being repurposed for directory services - for the purpose of making it available to everyone for every thing.

And here we're talking about content, content which is outside the scope of ICANN to (fasi) regulate for lack of a better word. So a question for the experts here is is that right? Can you do that?

Can you repurpose hundreds of millions of registrant's data for something that wasn't gathered for? In the United States you probably can, and that's where I'm from, but in other countries is this right? Can you do this?

Woman: It is a question. Exactly, I wanted to know this information, how are they managed (unintelligible).

((Foreign Language Spoken 32:45-33:09))

Woman: Not translation.

Woman: Perhaps I'll just jump in and give you a quick translation. Where is the data? Who is responsible for it? Under what jurisdiction? Under what purpose? What are the rules that apply? And I think the quick answer to that is that - the quickest one is it's complicated. I think I have to go further than that. ICANN is a corporation incorporated in the State of California.

So subject to California law, however, the registrars that are gathering the data on behalf of the corporation under contract through contracts that are set by the corporation could be anywhere. So Michele's in Ireland and subject to Irish data protection law.

The guys in Canada are subject to Canadian data protection law. And the registrars should have a privacy policy that reflects Canadian law in my opinion as a Canadian data protection person. And Michele will have one that reflects Irish law.

But unfortunately the terms and conditions of the contract don't necessarily respect that or they - the requirement to give up data becomes a term and condition of service, like when you deal with your bank. So does that help?

((Foreign Language Spoken 34:38))

Woman: Actually I knew what you were going to say but the question is are we working towards having a privacy policy adopted by the ICANN and that could be implemented, whatever. There is this gathering of data because we know that this personal - especially the personal data is used most of the time for illegal objectives and it can help, let's say, abuse the right of privacy - of people.

And it was, I think, the main (unintelligible) of this net (unintelligible) or this revolution - or evolution, whatever, against the - what is happening in the Internet governance.

Rafik Dammak: Okay, thank you. So before responding, (Stephanie), we have Kathy and Milton want to reply. But want to take question from (Andrea) before.

(Andrea): Thank you, this question is really addressed to the Office of Communications, excuse me. Even I once did have a death threat as a result of Whois being so insecure. And my name was associated with a domain.

Existing data protection as you apply it, does it apply to registries and registrars? You know, I'm familiar with the Internet service provider, a sector, and understand how data protection applies to information held by Internet service providers. But how does it apply, if it does, to information held by industries and registrars?

Man: Okay, so to answer your question is that if registrars are established in new member states and they collect the information as well as move out

(unintelligible) citizens then you will comply with European data (unintelligible).

And the whole issue about the way for - that is today with a simple (unintelligible) trying to get European based registries to comply with European data (unintelligible) against the backdrop of (unintelligible) sensitivity, both here and actually across the Atlantic over the collection and retention and accessing of data for law enforcement, national security purposes of which there's enormous sensitivity in Europe right now.

And around kind of biggest - kind of data retention (unintelligible) telecom's data was recently struck down by the highest court in Europe.

So you're in a very kind of dangerous area and we've been trying to do is Article 29 is individual - data protection authorities has been to get European based registries to comply with the law and the waiver arrangement while not perfect is a kind of reasonable way of doing that.

But to your point - if you're collecting information about our citizens then, sure, our rules apply fully, yes, absolutely.

Rafik Dammak: Okay, thanks. So just to remind everybody, please state your name when you speak. And we have another question from the audience, please.

Man: Thank you, when I came in to listen to this session I really wasn't planning on speaking. And hearing the interjections on the issue of Whois and privacy and adding another component to the conversation if I may is factoring those - factoring Whois and privacy in the new Internet ecosystem.

I'm going to share a story with you that happened to me on Sunday. Some of you may have seen me walking around with a little girl, my daughter, she's 11 years old. Decided to engage at ICANN because London's our city.

So had her mom drop her off, spend about three or four hours together, and took her to the GAC. Sat down, I said, these are people who represent their governments. Okay, and then she yawned.

And then as we're walking by - as a child, she said - and I register by the way, she said to me, Dad, can I get that little newcomer tag that I can put on my - you know, that green little tag. And I said, sure. So we went to the area where the newcomers are and we discovered some of the newcomers there were newcomers themselves.

And one of the people there observed my 40 plus ICANN meetings who said, what do you do? And we started talking. And the young man was so impressed that, you know, I'm a dinosaur in this space so he started taking pictures of us. Finished the conversation and we walked away.

My daughter said to me, Daddy, you see what that man was doing? I said, no, what was he doing? She said, he was taking pictures of us. I said, yes, that's fine because we're - she said, we - but I don't know him. So I said, I'll tell you what, let's do this.

So let's go back to the - she was, no, no, no, I don't want to do this. So we went back and I said to them, I said, guess what? This is what my daughter told me and all of them - four of them, the same voice, said oh my God, she's right. It's her privacy.

As a matter of fact the gentleman Whowas taking the photos said, I apologize for not taking your permission, may I keep your photos? And she said to him, yes, sure. As a child, she said sure.

Now relate this into if we were to move the Whois to a information services. Are we going to go and ask permission of every single user on the planet for their permission? I mean unless we're doing that - are we doing the ethical

thing? So for whatever it's worth, take it for - you know, just as a mind - a though process.

The engagement of Whois, what it was, and I think Milton's explanations of the history is absolutely spot on. And what's becoming and going to the heart of privacy, cyber security, child protection online in the new Internet ecosystem - if we're not weighing all of these conversations visa vie all of these factors, we're probably missing the point. That's my conclusion, thank you.

Rafik Dammak: Thanks, (unintelligible). So I think we have two questions from remote participation but - also we have Kathy, Milton, and (Stephanie) want to respond. Okay, let's start with remote participation.

Man: Yes, sorry. I have two questions in remote participation. The first one is what do people think of naming (unintelligible) in relevance to this debate? And name coin being a crypto currency which also acts as an alternative (unintelligible) DNS, which could avoid domain sensitive by making a new top level domain outside of ICANN control.

And the other question is, is the whole data protection issue complicated by the perception that data protection commissioners tend to be reactive, acting in the case of breech or disclosure rather than proactive?

Rafik Dammak: Okay, so let's start with (Stephanie)?

Stephanie Perrin: To respond to that one?

Rafik Dammak: Yes, quickly.

Stephanie Perrin: I think I'm not going to comment on how you evade the ICANN ecosystem. These systems exist and if we don't get a good policy people are going to use them more.

In terms of is this complicated, I think it absolutely is complicated. People have said, well, why don't the data commissioners tell us what the rules are and - or come to ICANN meetings and the answer is many of them in my view - at least my answer, I should turn it over to you to answer.

But many of them are independent authorities that must opine on these things in quasi traditional manner or even in a judicial manner when a complaint comes to them so that makes them reluctant to provide advice in some cases.

And in other cases you can't expect data protection commissioners to show up to every industry association meeting in the world though they'd be out on the road all the time and they have jobs to do. So perhaps you'd like to respond to that as well, I'm speaking for you.

Man: Speaking under the control of colleagues of course. There's two answers to that. One the one hand, of course, there's limitation when you are supervisory authority to engage with those that you supervise.

So I mean that's like if the banking authority would start involving in some bank's individual business decisions, that would compromise their independence.

But actually I think we are far from that being the real situation and the situation is more the - the case is more that supervisory authority for data protection do engage proactively.

I mean the Article 29 working party, which is the secretary body comprising all European national data protection authorities plus the EDPS has written over the past 14 years like eight to ten letters to different governance bodies in ICANN and constantly and repeatedly pointed out what was said at the - that there's no reason for the high degree of publicity that Whois data is being

given, that the purpose is not clear enough, that the - there's been no convincing argument that the privacy risks which are created by making individual's personal address and contact data publicly available are counterbalanced by any (unintelligible) purposes that has been raised and that have pointed out ideas for making privacy compliant rules for that.

I mean the latest communication that I'm aware of is a letter of (Peter) (unintelligible), my supervisor of 8 January this year. And we have also reiterated these ideas to some extent in the opinion of the (EDPS) which was adopted this Monday.

So data protection authorities are as proactive as they can be and a letter of last year was actually laying out the legal situation in Europe and telling ICANN please consider this the action of a state authority declaring that all European DP - registrars need to be granted the waiver under the RAA 2013 rules.

So it's not complicated, really it's not complicated. It's just clearly explained what needs to be done. Thank you.

Man: (Unintelligible) quickly that - yes, I agree with all that and that we are really (unintelligible) positive engagement coworking designing solutions to the - really quite considerable problems you've got.

And sure, there are limits to what we can do because we are regulated, we can't fine you money, we can't do all those kind of nasty hard enforcement type things. We do need to keep our distance.

But we're very, very up for coworking and very, very pleased that you arranged this event and engaged on the kind of privacy ICANN (unintelligible) fairly sparse. And this is a very good start, I think, to try and move things along a little bit and that we are certainly up for that.

Rafik Dammak: Thank you. Milton, please?

Milton Mueller: Yes, I just want to address the issue of, you know, where is the data, who is the jurisdiction. I think what wasn't said is that in actuality - in real world operational actuality the jurisdiction is global. There is no jurisdiction. It's a global system. It's the DNS, okay, and we want it to be global in some sense but we have this problem with the variation of laws.

And what we have here is a triumph of technology over law and this is a point I want to make to our data protection commissioners is that you guys have been just losing this battle for 15 years. Your law is being ignored.

You have adequately - documented the various objections that the Article 29 working party has made and what's happened? Why hasn't anything happened? It's because, number one, the system is global and the default is the openness of the data.

And there is a political barrier to getting ICANN to embrace and accept the changes that I agree would actually be very simple to make. You could indeed have a very minimal exposure of data as a default and then if other jurisdictions wanted to require more they could require it.

But that's not where we are. The default is, you know, the information is exposed and if you want to carve out any exemptions from that you have to do a lot of work.

And so this is precisely the dilemma that - the interesting thing about Whois is that we have established a global system, which does not conform to standard territorial privacy law.

And just to respond to (Collette) are we asking for permission of everybody? In effect we are. We're saying, if you want a domain name you have to

consent to what we're doing with your data. And if you don't, well, you just don't get a gTLD domain name, period. It's pretty a good point of leverage.

Rafik Dammak: Thanks, Milton. Let's get a question from James. Sorry, Kathy. Yes, yes, sorry. Because we have James standing for a while. Yes.

Kathy Kleinman: A comment that was made to me this morning - I apologize James, but a comment that was made to me this morning from somebody very senior - very senior US intellectual property attorney, some (unintelligible) - some (unintelligible) an attitude that we've seen in ICANN very well that you should know.

And he said, Kathy, you've been telling us since 1998 that there are problems. You've shared letters, letters have come. You solicited letters. You shared letters from the Article 29 working party from data protection commissioners. But nobody's brought any legal action. How - you know, nobody's done anything. It doesn't...

James Bladel: My mic is working. Thank you. So I'm James Bladel, not speaking as a registrar, not speaking as a - you know, any other capacity. I was with Kathy on the Whois review team but - which was a great learning experience but not even speaking in that capacity either.

I just had a couple of points to make. Actually Milton made a number of them for me which was that, you know, I think of a map - Whois as a map and maps usually tend to represent something big onto something small.

And Whois an attempt to map the Internet and all of the information that it contains and exchanges onto something small, which is an international legal framework. And it doesn't work and those genies are not going back into bottles. And I think it's - you know, it's futile in my opinion but, you know, we continue to struggle.

I wanted to raise a question because we had noted in this session and in other sessions that, you know, one of the primary concerns is that someone puts information, personal contact information including their home address, into a global database like Whois that, you know, what the consequences of doing a simple action might be.

And I think that the concern that I have is that I noticed there is mentioned in the EWG report of Whowas services. And these services for those who aren't familiar are achieving Whois, data that's in Whois even for a brief period of time, even if a domain name is later cancelled, expired, sold, transferred or even if you engage a wonderful privacy service to protect your information at a later date.

You will always be in Whois. You will always be in the - sorry, that provider's Whois. Now some of those aggregators or Whowas services operate within the ICANN sphere and I guess I'm curious if anyone has any insights on why they have not been subject to the same level of scrutiny as registries and registrars as far as the accuracy on the in bound?

Why there is no effort to examine the practices of these folks who are essentially keeping Whois data forever? And then selling it.

Woman: (Unintelligible).

James Bladel: I am sorry, I do have a 4 o'clock so I was going to rush out but if it can be very quick I will certainly stick around for an answer.

Woman: No, I'm not asking in a question. I just wanted to say that maybe - it's not the law who lost the bottle or it's not the law who's late to give an answer. But maybe because things are changing very fast and we are not following the track. We cannot as legal - you know, there are some - the long process to make a - the legislation.

Maybe even privacy will change because our privacy were decided according to our physical world. Now we have digital and frontiers which are very different. So I'm not giving an answer. I'm just raising an idea or a question.

Woman: You're off the hook, James. We'll sign up you for that law suite working party later.

Rafik Dammak: Okay. Okay. So please send in (unintelligible).

(Carol Douglas): Yes, hello, hi. (Carol Douglas) from Trinidad and Tobago. It's a related question in the sense - well, first of all I took a picture just a second ago and I realize I didn't ask anybody's permission so I hope that's okay.

The second question is - or the second - the point is in the case of privacy when somebody, as the lady said she was threatened, are there any cases where someone has actually sued ICANN for releasing information that is contained in the Whois?

Or let's say, breech in their privacy rights? In other words, given our information against - in which case, not just mainly giving out information but somehow or the other engage in their rights. And as a result, a person would want to then pursue the matter in court to seek some sort of injunctive relief done being - to have that name removed off the list.

Rafik Dammak: So we'll have two more comments for this (unintelligible).

Man: (Unintelligible).

Rafik Dammak: So we have (unintelligible). Okay, so we'll have three comments and then we will move to the expert working group. So let's start with - wait. Okay, yes.

Woman: Is my microphone working? Okay, great. The answer is I don't know and I've been following this for a while. I don't know of anyone who's sued ICANN

over this. There is this mandatory disclosure requirement when you sign on with the registrar in order to get a domain name.

I do know of people who have been subject to stalking, harassment, spamming, and anticompetitive activity because of the Whois and they've been (unintelligible) and intimidated in their homes and through all sorts of identification in their homes and they felt very violated.

But taking on an organization like ICANN is a lot to ask an individual or small business. And that seems to be where a lot of the concern has been. So no, the answer is no, I don't know of any official lawsuits or complaints. A lot of private complaints.

Rafik Dammak: It's really hard to moderate anyway. So (unintelligible).

Man: I was actually going to answer to the last two questions and maybe one more. Starting with the last one, has anyone ever sued ICANN? Well, I think that in the current system there would be no point in suing ICANN because the civil lawsuit would be between the individual registrar and the individual not wanting to comply with these rules.

So suing ICANN wouldn't make much sense. It would be a very indirectly (unintelligible) construction which would probably be rejected by the court in California in the first place because ICANN isn't involved in the Whois system. It's the individual mix and even the individual registrars, which actually (unintelligible) this information.

So anyone refusing that would probably refuse and the effect would be that you would not be granted a domain name and then you would sue on a completely different legal ground where privacy only appears as one as a argument promoted by the lawyers for improper behavior of registrars. It's a very, very complicated way to get to - into the court systems by that way.

Another issue is - of course, the - well, the - my colleagues from the British ICO have already asked whether Milton's remarks have been - no (unintelligible) has ever fined a registrar for that, should be understood as an invitation. So I guess that's probably not exactly what - would want to be achieved here.

And I wanted to react to the - also to the remarks made by the lady across the gap and the tables. Privacy or the protection of personal data as we have it in the articulation in Europe, Canada, partly in the US, and in many other countries, has not been designed for the offline world.

It has been designed in the 1970s when some people started to understand how computers would change the use of data. And I'm still full of awe how much foresight these people exhibited when they designed legislation which in its basic principles still works today.

So no, it has always been in full understanding or in full awareness of the issues of the online world. And it's just - it's exactly the problems that we are having today are exactly what was expected at the time.

And they are now called new problems just because no one at the time could imagine the orders of magnitude of money that you can make by not respecting these rules. And that's where the pressure comes from today.

I should say that I'm speaking (unintelligible) but I'll make these historical remarks.

Rafik Dammak: Okay, thank you. (Unintelligible), please?

(Gus): (Unintelligible) from the ADPF, speaking as personal capacity stole a lot of my points. But nonetheless, I have one question. Let me just stress the - has a lawsuit occurred. I think the problem with surveillance is you don't actually know what was the trigger.

So I'm guessing a lot of the time when Whois was used the individual who's been subjected to abuse subsequent to that wasn't aware it was necessarily from the Whois registry.

Nonetheless, I'm curious going back to the Whowas point, because I'm still trying to get my head around this, we often talk about dissidence and how they must protect dissidence and journalists and other people who are seeking protection through anonymity.

But we often presume that the individual who's the dissident knows he or she's the dissident at the time that they actually register.

I don't think that is actually the case. And we don't often think that our government hates us until our government changes and then we discover they hate us and then that's when we're a dissident.

So I'm curious if this consent regime that exists within whatever odd framework of law and policy, if it can be revoked and if it - if you can change a registration and once it has occurred. I'm getting the impression that even if you could with the Whowas there's always going to be a link back to the individual.

So basically it's a one-off policy that is if you have it - if you've registered and then you become somebody who's targeted then you have to abandon that registration and come up with a new one. Is that essentially the only right you have? There is no more than that?

Rafik Dammak: Yes, thank you. So who wants to respond to this? Okay.

Man: Well, thank you for that question, (Gus), but the duty of consent is actually that you can revoke it at any moment. And the law says it must be informed specific and freely given.

And when, of course, the question - when is it really freely given if you are foregoing a unparalleled and (unintelligible) service by that can you still really say that this content is freely given in the first place?

But in any case, whether or not you could - you must have the opportunity to revoke it otherwise it's not consent. If it's for lifetime then it's just something different but not freely given consent for sure.

Rafik Dammak: First we have a comment from a remote participation. Then we will go to (unintelligible).

Man: We just had a couple of comments from remote participates. One of them notes that - voicing the same remote that is actually (John) (unintelligible) .com. One of the comments was - he goes, I think that (unintelligible) took a legal action against the Whois (unintelligible) a few years back but that data was being used for domain slamming/fraud.

And the other one was just to amplify on James' point there, sorry it past somewhat, there's been a notable uptick on Whois scrappers in the last few years and Google is casing that data as well.

Rafik Dammak: Okay, (unintelligible).

Kathy Kleinman: Kathy Kleinman, following up on what (David Tick) was saying, Whowas services happened private. They've been collected - this has been data that's been collected by private organizations and offering it up as private services.

The proposal and I guess we'll talk about it with the EWG, the expert working group, is that it becomes service mandated and offered through ICANN and through the ICANN contracts. So moving it to a new level.

And I just wanted to add something, it hasn't been made that - the case with the registrars collecting the data and publishing the data because they have to through their contacts with ICANN, the registrars have been on the frontlines of ICANN protecting privacy. They've been fighting for their registrants. They've been fighting for privacy. And I just wanted to make sure everybody knew that.

Rafik Dammak: Thanks, Kathy. I think we will take the last question from (Brandish) because we need to move to the expert working group session. So yes, (Brandish), please.

(Brandish): I just wanted to make two quick points, this is (Brandish) (unintelligible) for the record. One was about protection of dissidents, etc. As long as certain kinds of information exists I don't think any legal regime can exist which effectively protects dissidents because legal regimes are written and then forced by the various states that we're asking not to make these dissidents into dissidents.

So there is a clear problem there. You can't protect - you can't cross law to protect against the state from interpreting it. So that's just not possible, one.

And the second thing that there seems to be a bit of a tension here between wanting decentralization on the one hand as a pro-privacy feature of Whois and having that, you know, federated structure and wanting to guard against private scrapping of wanting - you know, the Whowas kinds of services, things like domain tools, etc. provide, more strongly regulated. So on the one hand if you don't want too much power to come in the hands of ICANN and to mandate directory services then you want decentralization.

On the other hand, if you want to regulate these private enterprises you do want centralization and you do want to empower ICANN even more. so there seems to be that tension there that I just wanted to note.

Rafik Dammak: Yes, thanks, (Brandish) for this. So let's move to the comments from expert working group members starting with (Stephanie) and going to (Michael).

Stephanie Perrin: I think since we've kept (Michael) 25 minutes past his due time - no, go ahead. Okay, basically I think we have a pretty good idea based on this discussion what the expert working group was facing.

And part of what we're facing - or we were facing is a legacy accumulation of value added services that had been established using the Whois data that was freely available, even if it was - a high proportion of that data was junk data.

Certainly individuals who were engaged in criminal activity, registering thousands of domain names, weren't putting good data in all the time. Mickey mouse appears to have a lot of domain names registered. Individuals who cared about their privacy or who were aware of the risks were using privacy proxy services.

So the new proposed system, which I should emphasize especially to folks not ICANN'ers, that this is just a report of another expert working group. It has to go through the policy councils at ICANN and working groups have to be established.

And then they decide whether they like the recommendations or not. And so there's already some discussion going on about whether the privacy recommendations are strong enough. I dissented because I believe that there is a consent clause in there that amounts to what we call a coerced consent.

It is not freely given, it's either take it or leave it. You consent to the use of your data within a gate now, we're not going to have everything wide open. The problem is there are so many accredited actors who can get access to the data for legitimate purposes or permissible purposes is the word we use within the document, that that's not really much comfort to an individual.

Plus, it's not clear how to police any trickling out or escape of the data from value added services. If I subscribe to - I don't go anywhere ICANN or Whois but I subscribe to Whowas and then I find out where (Gus) (unintelligible) has lived for all of his life when he had domains registered, how are you going to catch me? Because data protection law - you know, we would have to mount a series of cases.

And as the privacy person on the working group I was constantly waggling my fingers saying, do you know how long it would take me to set up a complaint (unintelligible) of my pals and have this place swamped in complaints? And you know, the only ones who's faces went completely white and drawn are the registrars because they're the ones who would be sued as (unintelligible) indicated.

ICANN I would argue is - and I'm sorry, Michele's left because I think I finally got him around to this, ICANN is the data controller in the sense of European construction of who's a data controller and data processor because ICANN sets the rules.

And so really even though we can't blaster ICANN it's hardly Michele if he has to do this and he can't get an exemption. And yet he's the one that's going to be dragged through the courts. So it is a very difficult situation.

But there have been some high profile cases. I met about a month ago a charming gentleman, young gentleman in Europe, who has been running Europe the Facebook. And they've just been cranking the cases out, you know. Three smart students, that's all it takes. I find it very surprising that ICANN hasn't had a barrage of complaints that would cause some litigation and some action.

And certainly people get damaged now. And I think that's enough from me. I'd like to catch (Michael) before he leaves. With respect to this problem that

James brought up and our colleague here brought up, there is a sort of a teeter-totter thing going on. And the gentleman Whowas speaking about his daughter, there are two things happening.

On the one hand, if you've been running for 20 or 30 years vacuuming up data and doing whatever you like with it and there has been no lawsuits and the entire ecosystem starts getting built on the premise that that data's available and not only that, now you can mine it with cheap available data mining software and you can aggregate it based on data from other databases, it's entirely what was predicted in the 60s and 70s when we did all the study commissions on privacy.

Who knew it would be as cheap as it is now? So you have that kind of thing. You also have huge risk coming because the daughter's picture now is probably taken from a cell phone that is good enough quality that with a couple of snaps you're going to get a retinal image.

And a retinal image gives you a constant biometric that you can use. And you can cruise through the system and tag any other pictures. And you can just - even with a poor camera you can do facial recognition now.

So the chances of linking people, of associating them, of imperiling their basic fundamental constitutional rights of freedom of association, that really wasn't so possible when most of our data protection laws were actually created.

So I do think that - especially as the EWG looks at its work, this teeter-totter's going back and forth. Yes on the one hand you have an installed, embedded, very prosperous industry that it's feeding on data, not just within ICANN but within the entire ecosystem, that's how the Internet pays for itself.

And on the other hand, you have mounting risk and as spy shops in every city where you can get all kinds of devices that will help you track down people. It's one of the reasons - it's well acknowledge that we need to protect

vulnerable people now. And government needs that provision as well as anybody else does.

So I think with that I'm going to pass the microphone to (Michael Neble) if he'd like to say something about how the EWG...

(Michael Neble): Yes, thank you. (Michael Neble) speaking. I just wanted to follow up on what you said and I know that (unintelligible) is such a young guy but I was one of the grandfathers of the 1990 effort to kick off European data protection directive at the time.

And I can assure you that we weren't aware of the possibilities that we have today. We knew that computers existed but I mean we were in a different mindset. So we're facing a different world and different possibilities.

When we started our work in the EWG we were really in this kind of tension that Milton described but not in the tension between data protection and law enforcement. This is something there - we didn't have to even discuss it, that's something there with - we seeing it every - almost every day.

But a question - are we going to start from users as to the world has - was such or going back to the roots kind of thing. (Stephanie) and I are representatives of the - kind of the (unintelligible) purpose camp. And I've said, the - there have been even statements by the GAC where the users are much, much wider than just the technical function.

Now if - to put it into context, this is a manual rather than - this is not rule making. This is a menu. And in the policy development process I think there is ample possibilities to say, guys, this is going too far. You should let down. I mean it's not like this is going on - this is an opening and I just wanted to stress that, this is not something that has - that is already a decision.

The second element I wanted to stress is where both of us - I saw a chance also in the (unintelligible) system is to make the point for finally have a privacy policy in the ecosystem, in the ICANN ecosystem.

And not only this kind of (unintelligible) thing, which wavers and stuff like that, but having a privacy policy where we can - where we have a good argument for putting the protection level as high as possible and if only for making the transfer of data possible and being - coming from Europe and having various adequacy principle that will be carried over into the next phase of legislation.

But there's a clear case, otherwise data will not leave if we don't have the adequacy and have different means to construct that. But basically otherwise nothing will work and let's not forget, this is not - the choice is not having today and something like we propose that the whole ecosystem will change because you have all these different gTLD territories possibly.

You're coming out of this - more or less, comfortable relationship where most of the gTLD land is in the United States so you have relationships of safe harbor and various legislation. But you might have - and multiplicity of relationships so you have to have a high standard.

The issue of consent - we, again, we are happy to have consent singled out. I - we have - in the last minute drafted a framing where this is only in the context of applicable law and (unintelligible) has already described what this means for us in the union, that of course it - it's - there is a problem if there is no applicable law.

I mean if you look, the global that is indeed - that remains an issue. So this is what I wanted to say here initially.

Rafik Dammak: Thanks, (Mike). And now we will go another - we will go to another (unintelligible) and that will be moderated by Robin.

Robin Gross: Hello, my name is Robin Gross. We're very lucky today to have a number of European data protection offices here and a number of European privacy activists, a lot of ICANN expertise on Whois in these issues.

So one of the things we really wanted to do was get some open discussion back and forth, questions and - so we want to open up the floor now if anyone has any questions, comments, please raise your hand or get in line at the mic. Yes, please. And please say your name for the record.

(John Laprese): (John Laprese) for the record. After sitting here and listening to many people speak on these issues today, I'm struck when I look around the room that most - I think I'm pretty safe saying it, most of the people in this room come from strong rule of law states. And all these policies and procedures work great in that environment, or maybe not so great because we're having the discussion about it.

In weak rule of law states, all the - all this good effort is going to go for naught and in fact on the law enforcement session earlier this week on the expert working group, law enforcement was of the opinion that, well, we'll leave it to the law enforcement to determine who is effectively law enforcement.

When someone files a criminal offense, you know, what is actually criminal? Will we be in - we're leaving the decision in the hands of law enforcement. So in these weak rule of law states where we have, you know, perhaps governments or police forces that we might not necessarily trust, these kinds of procedures are open doors to abuse.

And I think it's really problematic that we're all sitting around this table and we don't have the - and we're all sitting here from a strong rule of law position. Thank you.

Robin Gross: Thank you. Kathy, did you want to comment on...

Kathy Kleinman: There's no answer to the issue (John) raised but it's a question that's come up again and again in the ICANN world. If a registrar has data - and of course, registrars have data that both in the Whois and not in the Whois, such as credit card data, who do they have to give it to? Is all law enforcement equal? Here, let me talk about a human rights group.

If a human rights group has information - data with their local registrar in the United States and it is a critique site of China it - the Chinese government comes to the registrar in the United States, does the registrar have to give it to the Chinese government?

Most registrars that I know - and I don't want to speak for them because I'm not a registrar would say that they would follow their national law on that. And maybe not hand the data over to certain law enforcement.

What happens now if we create an aggregated centralized database? Who is there to say no?

Robin Gross: Okay, thank you. We believe we've got a comment from the UK Information Commissioner's Office, is that right? And then I'm taking a queue here. So then we've got...

Man: Yes, okay.

Robin Gross: (Stephanie) and then a remote participant. Go ahead.

Man: Well, that's a fine point and it's a classical problem of international law enforcement that we have really, really nasty policy forces doing really, really bad things to their own people.

I don't think we can reform that though I think what we can do, certainly in Europe and hopefully in many other territories, just develop standards that

strike a reasonable balance between being able to register domain names and your personal privacy as a registry. And that's I think all we can do really.

Woman: Yes, I'm also from the Information Commissioner's Office of the UK. I do apologize, I won't be able to be with you after the break which you've got coming up because I have to be at another meeting, which I've been invited to as well today. But I did want to ask everybody to think about how the regulatory and the legislative landscape is changing.

And to think about the update of the privacy and data protection laws in Europe, which is currently underway. It's been under way for quite some time now. The commission - the European Commission already presented it - update in 2012, it's draft proposal in 2012. And the idea - the latest commitment is to try and get that agreement on the proposal by 2015.

You know, there is still time - there are still discussions amongst member states on this and there are serious discussions about the extent of territorial scope on the European legislation.

So I mean, if you're looking at different solutions which are available I would recommend that you look at this reform, which is underway and the kind of opportunities which might be open to you there. Thank you.

Robin Gross: Thank you very much. So next in the queue I've got (Stephanie), a question from the remote participant, (Akum), (Chris Lahatch), and then did I see someone over here? Okay. (Stephanie)?

Stephanie Perrin: I'd like to respond to the problem over the rule of law. I totally, totally agree and part of my dissent was that I don't think - speaking as someone from the global north, I don't think I can speak for whether privacy proxy services are available equally in the south, whether people are aware of the risk, whether they have any idea what could be happening.

And in fact, whether it was morally and ethically okay for ICANN if we're running a global ecosystem to - and we're supposed to be a multi stakeholder community with outreach to the south. Don't we have a responsibility to harmonize at a high level and protect those whose states have not brought in data protection law. I would say we do.

And we did have a proposal which you'll see discussed in the text if you have the patience to dig through the 166 lovely pages. There's a recommendation in there in the privacy section. We discussed having the - a variant of binding corporate rules where we would adopt a high level policy and get it approved probably in a European data protection authority and then we could transfer the data.

Unfortunately that recommendation wasn't accepted by the group but that is one way of achieving the equivalent of law through contractual requirements. Because there are so many ways that data can get out once it's collected. It can be gamed at the local. It can leak. It can get scrapped up. It's just a never ending list. Thanks.

Robin Gross: Thank you, (Stephanie). Next we've got some comments from the remote participants, which (David) will read for us.

(David): So there's a question from (Casper) in the remote chat. And the question is doesn't the data retention decision mean that any mandatory identity escrow systems like Whois are basically now unlawful in the EU? If not technically necessary to keep that data?

And discussion in the chat has already noted the jurisdiction issues that this is why the EU metadata cannot be stored outside the EU according to the CJEU discussion.

And also noted that it is technically possible to create - that the - the situation created by Whois has drifted towards blanket identity escrow, which - and it

was certainly predictable (unintelligible) EU and it would be technically possible to design a DNS with integral private credential without normalizing the identity escrow aspect.

Just to revisit that, because I'm trying to summarize quite a discussion in chat. The original question, doesn't the EU data retention decision mean that any mandatory identity escrow systems like Whois are basically end out unlawful in the EU if not technically necessary?

Robin Gross: Thank you very much, (David) and (Casper). Next we've got (Akum). Go ahead.

(Akum): (Akum) (unintelligible) from (unintelligible). Well, I was actually going to refer to recent decisions by the European Court of Justice, which - well, rather quite fresh and to not fully analyzed by everyone and therefore to the extent but certainly it's clear that the decision and the case (unintelligible) Ireland and (unintelligible) on the data retention directive, the court has established principles that would have to be regarded for any data retention, which is not on a concrete purpose of suspicion.

And that the thresholds are set very, very high and the thresholds of the - our retention policy in ICANN system would need to be measured against that. And well, the European data protection authorities have already before the judgment found that the retention was not justified and have expressed in all their letters.

So basically what we have here is confirmation from the court subject to scrutiny and legal analysis to be continued but confirmation from the court of justice that this interpretation is correct and that the thresholds are quite high and proportionality and necessity considerations are important.

The second judgment is the more recent judgment in the case between - as the data protection authority of Spain and Google incorporated, California,

where the courts said, yes, you have jurisdiction over this company, which is registered in California because it has a subsidiary, whatever it's called, in Spain.

And the operations of this subsidiary, even if though it doesn't operate a search engine and (unintelligible) are intrinsically connected to the operations of the search engine. And it has led to - the court has laid down principles for the interpretation of having operations in - within the EU.

And well, again, lawyers will need to go through the points the court has made in very much detail but certainly this judgment would also need to be taken into account when seeing what ICANN operations would be judged here.

And if indeed ICANN would kind of replace the current (unintelligible) Whois system by something under more central control and more central government it would certainly - could more likely be considered the actual data controller in this operation.

I'm not sure that that would be - with the use of (unintelligible) old system already be the case. But I actually had asked for the floor because I wanted to ask a question to members of the expert working group and going to something which looks to me like a contradiction in the argumentation of (unintelligible).

Because the report on the one hand says the legal contact must be (unintelligible) publicly accessible. So it must be always possible to find the name and some contact data for the legal contact in this group of purpose based contacts.

However, if you really don't want to be accessible like that you are allowed to use a privacy proxy service, only the privacy proxy service will be accessible

and then the privacy proxy service will be your gate to have an independent party checking the certification for the request to get your actual data.

What I don't understand and if it is possible for anyone who can afford this to get their data behind privacy protection wall by using a privacy protection service, why is that acceptable and why is it so unacceptable to do that for everyone as part of the service when you can always do the same operation that you have as an IPR holder or as a law enforcement agency or whatever?

I mean when the privacy proxy services in use you don't have to go to get a (unintelligible), to get justified request, and then you would to do it - it's just for privileged people that can afford? I mean - I'm sorry. I'll stop here.

It's just really the question, it sounds like a contradiction in the argumentation of the majority of the group and I say on the one hand, you can use a privacy proxy service so your data is not easily accessible but on the other hand you say, to have it gated by default would disrupt the legitimate request services. So any clarification from members of the group would be really appreciated. Thank you.

Robin Gross: Thank you very much. I'm sorry. (Stephanie), did you want to respond to that point?

Stephanie Perrin: I think we have to. Unfortunately (Michael) and I are the two members of the working group that are here. And I think you're singing to the choir in some respects.

Certainly that was part of my descent. But I don't think that your way out of this situation should be to hire a privacy proxy service provider even though they offer an excellent service and the price is declining. I just availed myself of one of them the other day and it's not free. You know, it's 12 bucks a year but still, you know.

And I don't know what it is in Zambia, you know. So - and I don't even know whether countries around the world are all allowing their registrars to offer those services. And it's a bit of a stretch to think that someone in Zambia knows enough to go to GoDaddy in the United States. So that's that part of it.

In terms of the privacy proxy service puts another barrier, we did put into the report that if you use the privacy proxy service, there is a code that has to be there indicating that it's a privacy proxy service.

At that point the requesting party then goes to the privacy proxy service and follows the reveal procedures. In other words, they have to show some reason for getting it.

And the Privacy Proxy Accreditation Working Group that I mentioned earlier that many of us are on were busy going through all of the procedures for that working group.

So I'm in fundamental agreement with your question. But others are not including the folks who are in the privacy proxy service industry. So do we have any of them still - aha. I spy Volker. Would you like to answer the question as to why we should continue this sort of double gate of allowing privacy proxy services to fill that sort of monetary niche? I hate to pick on you Volker but.

Volker Greimann: Well currently as is in the Whois today privacy proxy services fill a need that's there for its (unintelligible) to keep their private commission in, which is in my view worthwhile.

It's sad mind you that this is necessary that an extra source is needed to keep the privacy of the customers hidden. But under the current regime there's no other option. If there's another option, I would be - I would welcome it.

And I hoped that the WG would be aware of that but the current proposal seems to be pointing in a direction that we can still make some money on privacy proxy service even though that is not exactly what I think is right.

(Stephanie Perrin): And I would just add to that that I think that we have a duty to advise registrants in the current system and potentially in the RDS ecosystem that if they - the informed consent must include a warning about more data to travel through the system.

So I don't see privacy - being the paranoid type, I'm not - I'm going to use privacy proxy in the future and - until we figure out all of these little - and that's going to take years, so.

Robin Gross: (Debbie), did you want to respond to that point really quickly and then we'll get back to our queue?

(Debbie): Sure. Just a quick comment to (Gus). He's raising some points that we spent hours and hours talking with the Expert Working Group, which I'm not on. But I was at the microphones a lot because it's not clear what fields are going to be gated or what fields are going to be private right now.

So the legal contact for small businesses, for individuals, it's likely to be the registrant themselves, which means their address right now appears to be public as is their phone number. So I'm sticking with my proxy privacy service.

Woman: (Unintelligible) spent a huge amount of time and it needs to be clarified.

Robin Gross: Okay. Thank you very much. Chris LaHatte, the ICANN Ombudsman, would you like to make your comments?

Chris LaHatte: Thank you Robin. Just a couple of observations. The Ombudsman already has a role in information within ICANN. Primarily it's expressed in its present

form as the right for the Ombudsman to access any information held by ICANN.

But certainly in the wider context of deletion of information or correction of information - certainly I and my predecessor have from time to time intervened.

I don't think we have been much involved in the Whois issues at all. Although occasionally we do get complaints into our office about information being on Whois and of course generally that has to be dealt with by compliance because of inaccuracies and that sort of thing.

But there is a wider picture and that is Ombudsmen traditionally and this is perhaps in the context of the national Ombudsmen typically have a role in privacy and in supervision of privacy breaches.

And I don't think it would be at all outside of my jurisdiction to have a role where that comes in because I think one aspect you need once you develop a central registry of information is who is going to be the custodian and who is going to watch the custodian.

And I just raise that as a point. I'm not looking for more work at all. But if there is such a central registry and it's going to be administered by ICANN, then it would be logical to put the Ombudsman in the loop as having a role in dealing with complaints with regard to that. And it just is something that you might want to think about.

Robin Gross: Okay. Thank you very much. I believe we had a question back here from the floor. Comment.

(Jana Belinska): Hello. My name is (Jana Belinska) and I work for the Polish Ministry of Administration and Digitization. And what I'm also interested in is what the lady from the U.K. was talking about, which is the - there is this move in the

European Union towards a single set of protection regulations. And I think - I believe you touched on that with the Spanish case.

And from what I understand if this project succeeds then it doesn't matter that ICANN is looking at it and so far now because it was so - because of that (process) the European users that have been processed and it's still jurisdiction in the European.

And I don't now if the working group looked on that. But I would be interested to hear if - what are the interactions between that work being done in the working group and the projected legislation in Europe.

Robin Gross: Okay. Thank you very much.

Woman: (Unintelligible).

Robin Gross: Do we have a response to that?

Man: Yes. You're absolutely right. And the new regulation and the (I speak) on the control of (unintelligible) in terms of U.K. So if the new regulation extends the projection of the data (set of the) services are offered within the union. So if that's the case, what I could say you can carry - you carry your protection status with it.

This is why I argued before if you want to have the data in a ecosystem that's global, if you want to have the data of European that is (unintelligible), you better make sure that the level is adequate.

However this is constructed and there are several possibilities, DCRs are one -- you mentioned that -- or other ways to have that if there's not adequacy in the general legislation. But it is absolutely one of the points to get basically the whole system up.

And that would also cover in a way the kind of the (hole) for those where the rule of law is not going far where people were less protected because the system then would apply this high level.

Man: This (unintelligible). But there will be some interesting challenges shall we say where we're dealing with companies say in the U.S. You got no physical presence whatsoever in Europe yet processing information about European systems. (It's in the) practicalities of how you do enforcement for example. Although there are the parallel situations where that does happen but it will be quite difficult in some cases I think.

(Michael Mitt): (Michael Mitt). The main point and actually the draft regulation addresses the two issues of to whom do we apply the law. And the second one that it would really be unique throughout all Europe, which is inequality and that is no longer has to go through the process of national legislation.

And but I think the other process that we really have to look here at is that the difference between the current system and the system by - provided by - proposed by the EWG is indeed that the EWG proposes one system, the directory system for gTLDs.

And that's no longer a protocol which is used by a number of independent actors, which also apply more or less equivalent rules. But also a different legal quality when we look at what's - what might come out of the process triggered by the report or continued by the report in the actual ICANN governance system.

Robin Gross: Thank you very much. Next in our queue we've got (Gus). Go ahead.

(Gus): I resent the fact that I have to keep on speaking after our friend from EDP actually keeps on making my points. But I have to just start by saying (unintelligible) addressed but that (Stephanie) supported and respond to the work - from their working group's results is certainly of great concern to us.

But bring it back to (Casper) and (John)'s points about the very existence of (unintelligible) register and question the rule of law. This may sound glib (John) but I resent the fact that you think that surveillance in the United Kingdom operations under the rule of law when we have a case where intelligence agencies are acting in ways that laws do not declare its been particular clear including the hacking of databases around the world.

And so I ask how could we ever set up a registry system where you have to participate in it that could actually be kept secure either from the so called law enforcement agencies from the countries where we lack rule of law or from other attempts at secret access or malicious access by those who have the capabilities.

And then my final point is we need to set the right standard here. Already because some European countries set incredibly insanely stupid standard of registration and technology and registration of SIM cards against your identity back in late 90s and early 200s.

That policy has spread like a disease across Africa and some countries in Southeast Asia. So you have mandatory SIM registrations. So the idea for like (Stephanie) kept on using the example of arbitrary Country X in Africa. Does this person actually know about this possibility of not registering?

Unfortunately the default because we've set the bad standards is oh, in order to use these technologies, in order to communicate, I actually have to register. If ICANN moves down this road and doesn't set the right standard, then this is going to get even worse in every country.

Robin Gross: Okay. Thank you very much. Let me just see what we've got in the queue here. We've got (Amria) and then a question down here and then Steve and then (Marilia). And anyone else want to get in the queue right now and right here? Okay. Thank you very much.

(Amria): And thanks Robin. Actually (Gus) said part of what I was going to say in response to (John)'s question about - or point about rule of law. And but just to add to (Gus)' point not only can we not assume that rule of law is being applied in the way we would assume it's being applied in countries where it's supposedly strong for those of us coming from countries where it's not that strong.

And what has happened as a result of the revelations about mass surveillance is that it's making our efforts to strengthen the rule of law so much harder. And governments are literally saying to us why should be - they are not. So, you know, that is a reality we are dealing with.

But then secondly my question I have about - so basically it's the lack of clarity and consistency at rule of law not being applied at national level. But what are the implications of this sort of self-regulatory practice that's happening where large Internet companies -- this is not about Whois per se -- and decide when to provide information and when not?

And often the negotiation between the holder of the information and the government that is requesting it is taking place not in a transparent form, not through traditional channels - rule of channels. And often we only know at the public or even the implicated individuals that information is being negotiated you would only find out what the decision was after the fact.

So I'm talking for example Twitter releasing information about who holds a particular Twitter handle. And to what extent does this undercover type practice beginning to set rules - new rules that exist at some level that is very difficult to incent and what are the implications of that?

And then for the Expert Working Group I have a very specific question. I haven't gone through the report. But what are - what is the group's

recommendations with regard to accountability and remedy should there be a complaint?

Robin Gross: All right. Let me go on to - I know but I didn't see anyone to answer it. Does anyone want to answer that? Yes. Okay. Go ahead (Stephanie).

Stephanie Perrin: Thanks for the question on that. There's quite a bit about accountability in the report. And it was not the job of the - and I'm not trying to slough this off. It really isn't the job of the EWG to build the entire system and put every little piece in.

And I do believe that in terms of accountability - so accountability for data protection is a reality. We have to be accountable for that. And if for instance we - ICANN has a contract with an operator to run the RDS, there would have to be some provision for dealing with data protection complaints.

If my supposition comes true, (Chris) would be totally swamped with privacy complaints were he to take it on. And in fact ICANN is one step removed from the processor.

But there would still be a responsibility on ICANN's part to have our data controller or in - at the moment it's probably (Chris) would be the logical one to supervise what's in that contract from an (Epicson) and data protection complaint point of view.

But it's got to be in the - they have to deal with complaints in the RDS ecosystem I would say. But all that has to be built in the Policy Development Working Groups that we're going to strike in volunteers - I know I sound like I'm recruiting here. But I am. Volunteers welcome to join those groups.

Robin Gross: All right. Thank you very much. Yes please, down here. And then we've got Steve.

Bogdan Manolea: Hi. I'm Bogdan Manolea from Romania Association for Technology and Internet and the Digital Civil Rights Group. And also member of (Atlas) too and members of (unintelligible). And we had a lot of discussions in the first base of your (unintelligible) about the public interest of ICANN.

And we thought that maybe ICANN needs to define its public interest because right now it's not too clear if the public interest of the registries or public interest of the Internet users.

And this relates very much to our discussion because we think that the public interest if it's based on user interest it should be - we should start discussing about user interest in terms of human rights. And we have the International Human Rights Treaty that do contain the right to privacy.

So this should be taken into consideration at the start when we're discussing about what ICANN needs to do in this respect. And this actually can be seen in practice. And there's been the question about name-calling and I'm sorry that no one think that thought and there's references to Mighty Mouse domain name holders.

And this is a practical example that Internet users car about the privacy. And that technology does not go beyond the law. It's just that the humans use the technology loopholes in order to protect the privacy.

And I coming there from my own experience. I have - I own several domain names actually for the city TLDs that I know that they protect my data. I (give) my real data. And for the .org and the .com you will not find my name there because I'm not stupid.

I will not give my data to a registry that I don't know and that I know that they would put it directly on the Internet. And I know that there are at least three or four companies that would reuse the data right away. So why would I do that?

So in this respect I think that there are two key questions that need to be...

Robin Gross: ...hear me? Okay. Would anyone like to respond to these questions before we go to Steve? No. Okay. (Cathy) will.

(Cathy): What you raised are open questions. What's sufficient to contact you is there's a huge disagreement and this is a multi stakeholder community and there are different opinions on that.

Some people think it's sufficient to contact you by email. Other people want physical address and a phone number. Centralized versus decentralized are coming in right at the crux of that debate. The current Whois policy is decentralized but the Expert Working Group has recommended centralized.

So please help us evaluate these questions. What information is necessary to contact you? What should the purpose of Whois or this collection of data from domain name registrants be? Because we're - there are differences of opinion and again, centralized versus decentralized. This is the perfect time to be asking these questions.

Robin Gross: Thank you very much. Steve, you've been waiting so patiently. Please, you have the floor.

Steve Metalitz: Thank you. I'm Steve Metalitz. I'm a member of the Intellectual Property Constituency. And I really just wanted to say that I'm pleased to see that representatives of at least some of the European Union member state data protection authorities are here and are representative of the Data Protection Supervisor's Office are here.

And I think as our constituency looks over this report over the next weeks and months and we're still digesting and assimilating it. There's a lot in there. I think it will be very useful not just to the - to our constituency but to the whole community to have the views of the member state's data protection

authorities and of the Data Protection Supervisor's Office after they've had a chance to assimilate all of this - all of what's in this report.

And particularly to have their views on the extent to which this proposal would help address the concerns that we know they have about the current Whois system. This is a new paradigm that's being proposed and it would be very helpful to have their views on the extent to which this addresses their concerns.

I apologize if this was raised at the beginning of the meeting because I did come in late. But if it was, I'll be glad to review the transcript. But I'm just glad to see these entities participating and look forward to hearing their views. Thank you.

Robin Gross: Thank you very much Steve. Did anyone want to respond to that question before we go on to our queue? Who did I see? Wait a minute. I see you first and then (Bill). Okay. And then did I see a hand here? Okay.

Man: Actually I was wanting to get into the queue but I can maybe say this. Just one remark on Steve's request. Well, I mean legitimate interests do not block the processing of data. I think there is a way to deal with this as it is happening in other context. And (unintelligible) to the interest of (IPR) holders.

And I think that there really should be no blocking (ground). But I would come back maybe later when my term is up in the normal queue Robin. Thank you.

Robin Gross: (Bill), were you wanting to get in the queue or were you wanting to respond to Steve?

(Bill): Just really wanted to echo enthusiastically Steve's openness to have this conversation and these terms with these kinds of folks. I think it's absolutely fantastic.

You know, for the years I was on Council and we talked about Whois over and over and over. We were always starting from the standpoint of well, there's this longstanding fight over Whois. We've never been able to get on the same page. We're all dah, dah, dah.

And there was never a framing of - and it's a very complex multidimensional issue that you come at from several angles, right. There was never a framing with privacy in the foreground that brought together interests that would really, you know, set that framing and then ask others to come to that framing and engage, right.

We were always trying to build the inner dimension that others regarded as very much in the background or kind of (unintelligible). So I think it's really, really helping now that we've got folks here like you guys to be adding so much to this conversation. And I hope we can actually build this out going forward.

I think that bringing privacy quote unquote into the agenda of ICANN in a more direct way and institutionalizing a set of relationships where we bring in folks like this and engage out colleagues and other constituencies in a dialog and then it turns in parallel with the dialog that has its other spaces is really, really constructive. So I'm really happy that you're happy. I'm really happy that I'm here and I just wanted to say that in case I didn't get a chance later.

Man: I was actually ready to (unintelligible) about that. Yes. Thank you very much for saying that. And we're very, very pleased to be here. And I think the right to privacy is going right with everybody's corporate agenda and we need to devote more time, more energy to solving it.

And to be frank I think this has kind of (standard for) the moment between European data protection authorities and the various registries operating in

EU. There's a kind of (standard thing) that we've said look, I think we've got real problems with the data retention policies.

But the next bit is what we do about it and to construct something which solves some of these problems out to some extent it what we need to get to I think and I hope this is part of that dialog.

Man: Okay. (Unintelligible) again from the EPS. I just want to make two points and I'm quoting an opinion that our organization published this Monday. It's more directed as our policy advisory role to (Michael) and the commission than to ICANN At Large. But of course we also speak to ICANN as such.

And let me just quote three thoughts from that and bring them in a specific order. One thing is we take notice that NETMundial in April committed to certain fundamental rights. And the listed - and the first three they list are freedom of speech, freedom of (cessation) and privacy. And of course they all belong together.

When you can't speak freely when you know the authorities will be (will come you) in ten minutes after you've spoken and you cannot speak freely or you - maybe I want to speak freely but once you are two or three people saying the same thing you will be subject to persecution or prosecution.

And of course (cessation) works only when you have the freedom to actually not do everything right in front of the eyes of the authorities. So there's three rights. And we have freedom of speech, freedom on (cessation) and privacy belong together very, very strongly. And I would say each one is a precondition to exercise the others.

Secondly, in Western democracies deriving their ethical systems and their (political) systems from the declarations of their French revolution and the (newest) Declaration of Independence we all agree on this for not 250 years or so.

And then we cannot get to operationally implement this is the little area of registering and cataloging domain names. I mean come on. That cannot be serious.

And I think - and that's also what the opinion says. The implementation of fundamental rights and this domain is also a litmus test for the model of mighty stakeholderism as it is propagated in this organization.

When this might stakeholderism cannot work in protecting fundamental rights then it's probably not the right model. And that's a very, very big question that we have put in this occasion.

We are glad that (Isaac), the European Commission in the communication that we responded to has taken the same basis and the same position that the fundamental rights protection is more important than the might stakeholder model and that the model must be established to protect fundamental rights. And I think this is really a very, very crucial question here. Thank you.

Robin Gross: Thank you very much. I'm sorry. You're next.

Woman: I didn't have really to (unintelligible). But I want to ask a question to the Expert Group. Did you consider the question of the (different) validation of this data and what it could present to as a challenge and a (danger) when it becomes a tool of (unintelligible)? Thank you?

Robin Gross: Thank you very much. So next in the queue is (Marilia). And then we - and then we've got (Lee Hubbard) from Council of Europe and (Chris Parsons) and remote participant. Was there anyone else who wanted to get in the queue? This guy and this guy. Okay. (Marilia).

(Marilia): Thank you very much Robin. I just would like to take advantage of my position here as a newcomer not to Internet governance but to ICANN to ask some basic questions to you. By the way, thank you very much for organizing this (unintelligible).

And my question relates very much with what was said before regarding the point of the underlying justification of the new (unintelligible) of having the Whois information up there at the (unintelligible). And, you know, the base information that we have is that the Whois is useful first of all for UDRP and intellectual property purposes.

And I'd like to ask (Cathy) if with your particular experience you find this is really relevant and especially with the government sessions that you're having here on the proxy and privacy services and also because of law enforcement reasons.

And I wonder if there is no correlation here with the - I mean if you have a contract with your ISP your information is going to be, you know, held and kept protected unless you have a court order or unless you have lawful requests from law enforcement.

So why is that not like the Whois system? And sometimes I wonder why the Whois system really exists and if there shouldn't be any other way like a bureau that lawful requests are set to this place or this body. This body would then give information to the one that is requesting the information - the contact information.

The question that I have is that there are some policies here in ICANN that get approved and that they go against basic rights like the right to privacy and then we start to patch, you know, the damage and try to make it, you know, as less harmful as possible but then it's a very damaging policy.

And I would like just to make a reference to what (Stephanie) has said about developing countries. For me it's very hard to understand first of all that you have to - nowadays the system that you have to pay for proxy and privacy now that you have some privacy regarding the data that's used in Whois. For me it's very hard to understand and accept that you have to pay to exercise the right.

And if you think about the price of Internet access in developing countries then you have just layers and layers of services that you have to pay for. Right. The Internet is already very expensive.

And then if you want to have a domain you have to pay for it and the prices vary a lot. And then if you want to have your privacy protected then you have to pay for it for a service. I mean this is - this makes no sense to me but then maybe you can comment about that.

(Cathy): A number of excellent points. Is Steve Metalitz still in the room? Steve, this is one you and I should both answer because Steve and I have sat across the table from each other since 1998 on this issue.

And I've raised the same - if you look at UDRP for example, which is the uniform dispute resolution policy. This is domain name disputes where someone's alleging basically a trademark infringement or a trademark use - use of the domain name in bad faith by a trademark owner.

And I don't know why you have to reveal someone's existence. You can look at the domain name. You can look at the uses of the domain name particularly if there's a Web site without revealing who it is behind the domain name. You could still transfer it or cancel it without knowing who's behind it.

So I've never quite understood that why you have to reveal the person. Steve would probably have a very different view on that, which you're welcome to share Steve if you want to.

But one of the questions we've debated all along is is mere allegation enough. Just because someone alleges trademark infringement or alleges fraud or misuse is that enough to reveal the data whether it's in the Whois database or particularly whether it's in a proxy privacy service or whether it's in this new centralized database that the Expert Working Group is seeing.

This is something we're debating in the Proxy Privacy Working Group right - we'll be debating it shortly. When do you reveal the underlying data? And there are very, very different views in the multi stakeholder world here.

Robin Gross: Thank you (Cathy). Okay. So next in my queue is (Lee). You're in too - you're in as well. (Lee), please. You have the floor.

(Lee): Thank you. Thank you Robin and thank you very much. Anxious to be here. I've already addressed some of you in the NCUC from the Council of Europe and Inter Governmental organization with 47 countries. And I'm - we're also an observer to the GAC.

So I've just come from the GAC. I do net communique business and it looks like they might take note of the reports, which is being done by two experts - independent experts. It's not a negotiated position adopted by 47 countries. That has to be made clear.

But nevertheless it's a report which brings together some of the human rights issues in ICANN's procedures and policies. And I think it - I guess some of you have already received it. But it's - it was submitted to the GAC a week ago. Many haven't yet read it. There are some concerns so it may need to be updated a little bit.

But still the point of that thing is that this is on the radar of the GAC. So the question I guess that you're discussing here in Chapter 3 on Whois and

RAAs and the state of protection of privacy are sort of now in the radar of the GAC as well.

So, you know, it's quite clear this report with or without comments received - I'm sure there'll be lots of comments received and an update possibly will go into ICANN 51 and there will be more discussion in the GAC but also elsewhere. So I expect maybe in the GAC cross community discussion perhaps in the future - that's my feeling. I don't know.

So this report is - it talks about many things but for the purposes of what you're talking about now, I think (unintelligible) I'm sure you already talked about (expert tension) and judgment and the case of the courts and necessity and proportionality and all the things that we know and love in the (sort of) privacy. So there's no point in going into that.

But it does mention all of those things in the right order. And I think it's quite compelling reading although it doesn't go into too much detail. It's very well sourced and grounded. So I think it's a good - it's a good basis on which to start to discuss. Certainly won't satisfy our expertise here but still for government it's quite a good start.

So that's who we are and it talks - it brings back into consideration public interest. It's very - it refers to the high level panel of ICANN, the report and also NETMundial of course. And I think - what I would like to say it's a lever for discussion in ICANN 51. It's a lever to access discussion with governments particularly the GAC.

And I hope and I expect that we can also discussion this in the IGF as a next step. And so I think this work - this report and your work combined -- it should be combined -- will have a life together.

I mean it talks about the U.N. It talks about the (ICCPR). It talks about - it refers a lot to the DPS and the work of the Article 29 Working Group. So it's

actually quite a broad and holistic approach to the question of Whois at one particular level. So, you know, I can (send out) the report to you of course and we can - it's out for comments. So thank you.

Robin Gross: Thank you (Lee) and I would encourage everyone to take a look at that report and read that report the Council of Europe has put out. Okay. So in the next - in the queue next is (Chris Parsons).

(Chris Parsons): So thank you. I'm a newcomer to ICANN so I apologize if any of this is incredibly basic. If it's very basic I'm just really missing something. I wanted to start by pointing to - and I know that I haven't heard talked about the whole time I've been here - the whole week and I've been involved in probably more discussions about Whois than I ever thought I ever have.

The first thing is we are working on an assumption and I don't know that it's a good assumption. It's that the individual who registers a domain - so I have a domain, (Christopher.Parsons.com) and I registered it.

Now I did. But there's an awful lot of people who come to people like me and say hey, I want a domain. And then that person fills that information in and you never hear about that person, what they write, they have a domain, they're done, I have not contact with them.

So when we're talking about (unintelligible) and sort of if someone realizes that they're not risks, which thinks about trust all to being with. Let's pretend it works.

That assumes that the person can do nothing about setting up a domain in the first place and doesn't have enough knowledge after they've created a Web site to then go oh hey, there's all kinds of my information sitting on the Web somewhere and that needs to change now. Well let me just suggest that this is a belief that does not stand up to reality. The first point.

The second is I actually take the comments of the rule of law and (strongly) rule of law states very seriously. But I do sort of like just want to complicate it a little bit. And so here I apologize. I'm from Canada so you got all these Canadianisms from all the Canadians that are here.

But let me just share one recent experience. So there's an individual from Scotland Yard who contacted our federal police here at CMP. And Scotland Yard was subscriber information or basic information from a Canadian company.

They did not go through (Amlot) process. It was a call hey can you get this from this company. Company gets called by RCMP and they are subjected to repeated yelling matches. We need this information. Children are going to die if we don't have this, so on and so forth.

This company refused. But there is a process for getting that kind of data. And LEA and the U.K. went to another LEA in Canada when there was a horrible treacherous long process. The (Amlot) process is terrible. They could have gone through it and they chose not to.

So I do want to flag that. But what happened isn't necessarily illegal under Canadian law but it does underscore the ability of law enforcement to contact other jurisdictions to try and get information that might be more difficult if they were to go through more robust channels if you can all them that.

The third thing I wanted to point out is going back to (Milton) actually. Going back to the very first thing he said about the Whois, you know, this is what was technically there to do. Good summary. I liked it.

At the end of the discussion that we had yesterday from the Expert Working Group, the question that was framed by, as memory serves is, is the proposed Expert Working Group Whois better than what we have now.

And let me just say that anyone that accepts that framing is already - you're going to be hard pressed to say no. Because you can probably imagine some way is better.

So it seems to me that the framing is generally given the minimal technical requirements the Whois needs to provide - I think that's - personally I prefer (Milton)'s this is the (unintelligible).

But I think that has to be decided. Better is not a good understanding. Is it appropriate? Is it correct? Is it technically necessary? And if it isn't, maybe that's where the discussion happens.

But I've been in this conversation with Whois all weekend or I guess all week rather. And I can't get my head wrapped around how it will ever happen. And so I'm actually asking as a real question is this a white whale?

I mean we can think about data protection. That's hard. But I think there's an easier place to look. If we're talking about synchronized data, as my colleagues from (Syria) has pointed out, that data will have to sit somewhere.

So is it going to be a situation where it's going to be in Europe? Maybe we can create data protection standards in Europe so hurrah. But are other jurisdictions going to be happy with that? Or maybe we move it to China. And is the U.S. going to be happy with that?

It seems like there's also this geopolitical concern that doesn't tend to be raised in the conversations. The governments are going to want to control it whether it's significant or not just from a political optics perspective.

In the U.S. this has obviously attracted attention from the Republicans. So is this - I'm asking this because I don't know. It's not a loaded question or anything like that. Is - how much of this is a white whale or how much of this is an actual live real we have to worry about this? Haven't asked because I

had limited time, limited resources and actually I know where I should be spending them actually. Thank you.

Robin Gross: Thank you. (Stephanie), you wanted to respond to that?

Stephanie Perrin: I'm going to try and be brief because I know our colleagues here have been waiting to speak for some time. But my memory is bad and I've already forgotten the question over here that I haven't responded to.

So I agree that the deceptively simple question is it better, is it not is almost false advertising on top of 166 page very dense, very politically complex, very technically complex, very policy complex document. So you can go either way, yes, no. And so it doesn't help you.

Is this implementable? Certainly parts of it are implementable. The - and we have proposed that the pieces stay together not because we're trying to slide this through the GNSO without the proper processes but you don't get the verified data without the privacy as far as I'm concerned.

And so many - there are so many balances it's, as I said earlier, it's feud like, you know. Somewhere the trumpets have to get picked up again, you know, weeks later.

And so putting this together is going to be quite complex and it's - I'm not quite sure that ICANN has the maturity level to manage that. But boy, I bet there's going to be an urge to try because the system right now is kind of broken.

And I think - we didn't go into why it's broken or how it's broken or just because I don't think anybody felt they had to justify how broken Whois is right now. As far as I'm concerned, privacy is broken and so I'm delighted to see the Council of Europe report coming at a good time and the opinions from the EU coming at a good time.

And so it's a good time -- I sound like Martha Stewart here -- to try to do something about privacy at ICANN. Even if it's only a baby step up to the next level, it would be an improvement. So does that answer your question sort of?

And there are people who want this thing to work and they all join the working groups. And ICANN's challenge will be calibrating all of that making sure it stays balanced.

Robin Gross: Thank you. Next we've got a comment from a remote participant and we've got our gentleman here.

Man: Thank you. I'd just like to generally - just generally summarize the things in discussion in the remote chat now that is focused on the issue of the technological limits of some of this and how, you know, all systems are, you know, presumably hackable somehow and that is of course - the only way to prevent that is of course is not collecting the data.

The specific question was from (Casper) and was specific as a question for (Stephanie) and he said surely longing for data protection compliance could never become the (radar net) for keeping personal data that was not otherwise lawful to print it.

Robin Gross: Okay. I'm sorry. (Stephanie), you're looking like maybe you want to respond or something.

Man: You want to repeat that?

Stephanie Perrin: I didn't quite hear. Surely something.

Man: Surely longing for data protection compliance could never become the (radar net) for keeping personal data that was not otherwise lawful to protest.

Stephanie Perrin: Agreed. How about that?

Robin Gross: Okay. So next we've got Pranesh. Please go ahead. And then the gentleman immediately next to him.

Pranesh Prakash: Thank you. For the record this is Pranesh Prakash. I just wanted to pick up some - respond to (Gus)' question about rule of law that had earlier been raised by (John Labresy). And note that one activist dissident is another official's (feeder) and another right holder's terrorist. Okay.

So and this is applicable not just in weak rule of countries but also in strong rule of countries that the moment information is collected, it can and will be accessed by law enforcement agencies as long as they know who to reach out to. They're the ones who'll be (down) the law and regardless of what is stated in ICANN policy, that is what will happen.

So the only way to - of preventing that I see is either not collecting the information at all in the first place, which might be a problem for the link and technical purposes or to mitigate that to some extent if it is collected for technical and the link reasons then not making it known who holds that information.

So because as long as that information is known, law enforcement agencies can go out and get it from those people. And yes. So - and that's much more difficult to actually do than to say.

Robin Gross: Okay. Thank you. Sir, would you like to go next?

(Patish Van): (Patish Van). This rule of law causes extremely (laudable). And I think some of the European states and (sit in the) United States holds on to defense rules of law (surely) and that's logical.

However, rule of law is most problematic because most, including the United States, it's totally one thing whether this rule of law is actually affordable. That's the difficulty that a lot of states are under that. Is this rule of law actually - can you really afford this?

And we've learned in the recent past that actually some of the states - most sort of are (unintelligible) as far as the rule of law is concerned actually use other methods to get around it.

They get another state to take on the role of breaking the privacy of their target within their own state. They overcome the rule of law issue by doing that.

So there is a real problem that even weak states obviously do not have rule of law and of course other states like China and Russia actually does not have rule of law in the way we understand rule of law.

But even they have disclaimed that they operate under rule of law. And I think especially for United States visitors - but I think often you take rule of law as being a very strong principle because you apply those principles to your own citizens and your own country.

But when it comes to applying these very principles when you are tested you begin to use other (plots). In fact the space no longer functions under the rule of law. So you introduce something called the (Gitmo). So you actually place them in a terrorist (way), no rule of law. So the rule of law principle doesn't apply anymore.

What I'm saying is that this is the problem we have that we have been tested about the ideas about rule of law, about human rights. But the notion of privacy simply because these are often taken as, if you like, you know, it's something that we say; we say we have got rule of law.

But we've never been tested on that by the players. So when we test and we find actually that we have tremendous difficulty in applying those principles because we have suddenly come across something called good guys and bad guys.

How do you apply who is a good guy and who is a bad guy? This - I'm putting it philosophically because I think you need to understand especially in United States. I think because you have very strong principles which you apply to your own citizens.

So for example, you have gun laws. Every citizen is entitled to have a gun and lots of guns. You know, this is a guiding principle of the United States. This is something that you apply.

I'm asking you this that in fact what is happening in Europe and is still happening in many other places - I think you need to understand this. That we are going to work in gated environments, which for example Germany, a country which is one of the most democratic countries in the world - in fact, the privacy laws in Germany are incredibly strong. In fact they're not comparable to the privacy laws we have in U.K.

But the U.K. has been particularly lazy of...

Robin Gross: Can you wrap this up? We've got a few people waiting in the queue.

(Patish Van): But I think it's important for you to understand this because I think people are taking for granted the idea of rule of law and not understood the principles about good guys and bad guys. And I think we're being tested on that.

I'm not sure I am on these things. But I'm asking you that you need to be aware that there is not a single safe player in the world anymore.

Robin Gross: Okay. Thank you very much. I need to move on in the queue. We had the gentleman in the end her...

((Crosstalk))

Robin Gross: ...very long time.

(Patish Van): One more point.

((Crosstalk))

Robin Gross: We're running out of time and so we need to move on.

(Patish Van): Let me just put one especially before I go, which is that we are in a multi (unintelligible) information environment. We're not longer in a singular sort of linear environment if it's one language or two languages. And two more...

((Crosstalk))

Man: All understood by everyone in the room.

Robin Gross: Okay. Thank you very much. We're moving on to the man who's...

(Frank Tellen): Thank you very much and I'll try to be brief. (Frank Tellen) for the record. And my first ICANN meeting. And I'm learning a lot. One of the things I value greatly is hearing all the various views and truly getting a sort of multi stakeholder process and I think it's working well.

But I want to point out two things. One in the way of comment. I'm very interested to read the report. I see some of the responses to the report, which I had a chance to read through. But some of the potential privacy benefits that are included in the report if there's a way to summarize those - I don't know if there's an executive summary that does that.

But trying to articulate that in some kind of a very brief fashion so people can point to some of the key advisory points that are made that are going to really be privacy benefits.

And then also I think it's important, you know, this is truly a multi stakeholder process that represents all points of view. And I think it's important to remember that all constituencies who utilize the ecosystem that we operate within have legitimate points to raise and also need to be considered.

So form the standpoint of understanding the benefits of the Whois system and understanding where it works, there's not question there are legitimate issues about privacy concerns, legitimate issues about, you know, inaccuracies from the database.

But when it comes to actually being able to use Whois to, you know, try to curtail illegal activity or try to use it in the intent that it should have been formed for I think that that's what we have to get back to in some of this discussion.

And we have to make sure that it's a system that actually works for those who need that kind of benefit. You know, in the U.S. we know that rule of law means that sometimes it's not just a criminal prosecution against somebody who's engaged in criminal activity. It's up to the individual to perhaps engage in a civil activity. And sometimes information needs to be accessed.

So I think law enforcement does need legitimate tools to stop truly, you know, bad criminal behavior that's happening in the Internet space. And I also think that there are cases where we saw this gentleman earlier talking about his daughter.

You know, I wonder whether or not if something had happened that was a sort of a different type of crime in the online environment and Whois was the tool to try to prevent that, he might not, you know, look to that as a resource.

So I'd simply point out it has to be effective, it has to be one that works for everybody who really does believe in its purpose. Thank you.

Robin Gross: Thank you very much. I've got two people left in the queue here. I'm sorry. I don't remember your name.

(Mona): It's (Mona).

Robin Gross: Thank you.

(Mona): Thank you.

Robin Gross: And then...

(Mona): Actually I just wanted to ask a question that - about why do we have to reveal the identity. Why don't you - why don't we take the site or whatever - no. I think that the issue is about legal security because he who controls the data cannot be transformed into an authority - a legal authority when he is not.

I mean we have to avoid making these people in control of the Internet or of the data or whatever as judges. So if it's for our own safety. Nevertheless I may think that maybe in this question we should consider what is happening in the banking sector like the case of banking sector (unintelligible).

The banks can reveal the data upon proof of reasonable permission or reasonable, whatever. I cannot translate ((Foreign Language Spoken 2:28:09)), so.

Woman: When they really can prove that they have a reason to do this.

(Mona): Exactly. Thank you. So - and I want to add another idea. Because today we were at a session where they were talking about ICANN responsibilities - public responsibilities.

So actually ICANN is running the most important infrastructure or resources in the world, which is the Internet. And when talking about public responsibility it seems that they are very aware of what they are doing and they (are retaining) the most important thing in the world that makes the economy and everything.

And it means that they are acting like government somewhere because the traditional role of the government is to be - to administer, to manage and everything the rights, the resources, the rights, the interest - the public interest. So why not?

And as the professor here -- I don't remember the name -- said, if the code is the rule then ICANN has the obligation of taking or putting some rules to protect privacy because if at the legal level we don't have the solution, they have the obligation of protecting all of us. Thank you.

Robin Gross: Thank you very much. Yes, the lady down here. You are - been waiting patiently. And then Volker.

(Julia Powell): Thank you. (Julia Powell) here. I think that I would particularly commend the opinion of the European data protection supervisor on the commission communication on Internet policy and governance, which was issued in Brussels on Monday the 23rd of June as a very illuminating study on a lot of these data protection and privacy issues.

I have found it quite unconvincing and still remain to be convinced on a compelling case for centralized or synchronized RDS. It seems to me that the - in the 156 pages report, which I haven't read in detail but I have read

through, the primary foundation is sort of facilitates administration and it has cost benefits.

But I would question what costs have been taken into account in terms of the privacy implications. In particular one of the purposes that needs to be made explicit and isn't necessary in proportionate to collect in a centralized fashion.

I think that taking into account the data protection implications particularly when you're managing sensitive data has very significant cost and has significant legal exposure for ICANN as an organization. And if that was taken into account perhaps it would consider very strongly whether it should centralize. Thanks.

Woman: Thanks. Let me jump in ahead of all and say please join the working group.

Robin Gross: Thank you. Volker.

Volker Greimann: Two separate and completely independent points. First of all I am very happy to see that there's a lot of European data protection officials in this room today interested in participating in ICANN. And I would hope that they or someone on their staff would consider joining the GNSO working groups dealing with the evolution of Whois and either as actively participating members or resident experts who can lend their advice to us or questions when they arise.

And the second point is I agree completely with what most of the people have said in the room. Data collection at least in Europe can only happen for legitimate purpose. Such purposes cannot be later - that the data may later be used for law enforcement or (unintelligible) right to protection (Phase 2) must be useful for a legitimate purpose at the time of collection. So that can only be technical or business purposes.

An example how this - how legislation in different areas but which could be considered similar as an example - it could be taken as an example in Germany for example, the filming of traffic by cameras see who is driving too fast, i.e., filming everyone and then seeing who was to fast is illegal. You can only film based on cases.

So if you have a measurement of a certain car you can use it - you can film that car for evidence. So if you already know that there's a - that there's a violation ongoing then you can take a picture and use that. You cannot film just on suspicion.

And the other one is that German courts have recent - repeatedly held that the retention of meta - communications meta data by several communications companies is illegal in Germany, violates the constitution and I see that would be very similar to Whois data collection for law enforcement purposes or right to protection purposes.

So claiming that Whois fulfills these purposes abuses what Whois actually is. And that's a technical and business purpose.

Robin Gross: Thank you very much. So let's move on to our final topic, which is next steps and action items. And I want to turn the floor over to Avri Doria to moderate this part of the discussion. Avri.

Avri Doria: Thanks you. Not that there's much time left. But I think it is important to walk out of here with some idea of how to keep this going and how not that could be just a one time event.

And certainly certain was said about people getting more involved about - but I think it's more than just finding people to participate in our working groups, which can be labor intensive. It's also getting suggestions. Yes, see. Labor intensive makes you tired.

It's also how we can get to you for help for those of us that are participating. And so basically looking for suggestions on how to start with this as a resource and build on it. And so we have what, maybe 15 minutes of idea collection because all I can - you know, it easy to say what Volker said to come here and help on the working groups.

I know most of you can't do that. Come here and get some of our staff to work on the working groups. Maybe you can do that. But we're still going to be here working on these working groups and we're constantly needing help, needing resources, needing quotes, needing document pointers that - okay.

We have two or three people here that are very policy and privacy policy knowledgeable. Then we have a bunch of people here that are just policy hacks like me that work on problems and hand wave and we always need help. That's why they asked me to do this one because I always need help.

So please who's got suggestions of how we can, you know, basically reach out to you? What ways - what best ways can we keep this discussion going and take it further. Take it to your colleagues that we weren't able to convince to come here. Please. First - yes.

Man: Well the obvious suggestion if you want to finally get to the end of PDPs and working groups on Whois is turn it off. Shut the whole thing down. Twelve years we've been out hearing about what should and shouldn't be in Whois. Maybe it's (haystack).

In the 90s it was important to know the technical contact for something was because there were only 20 people who had name service. That's 20 million people now. And it's not generally the registrant who even needs to be contacted about things like that. Either put it back to its original purpose or just turn the whole thing off.

Avri Doria: Okay. Thank you. That was one good suggestion. I'm going to give you the floor but I'm only going to give you two minutes and I am going to shut you down. Please.

(Patish Van): I was going to say it's important that (base) players are involved (and so let) civil society elements and that in fact it should be a global effort in fact including (base) players and others who are not necessarily people like us. It might be bad guys, bad states.

I think this needs a global effort to protect this great knowledge base we have called the Internet for our own future well being. The idea that information is something that all of us should have access to, the whole world; that we should have open access to it; that means all the players working together.

Avri Doria: Can you give me one concrete suggestion of something we could do? Shutting it down as great. I don't know if we can pull that off but great idea. Does anybody have concrete suggestions? Please.

Woman: I just wanted to understand exactly what you ask for. I'm sorry.

((Crosstalk))

Avri Doria: That's quite all right. I talk too fast in English and - I'm basically looking for ways you can help us. And as obviously being here and being in the working groups is good. But how can you help us even when you're not here? How can we reach out to you? Can we create a method? Yes. I have (Stephanie) and (I'll come back).

Stephanie Perrin: I think it might help to sort of sketch out the kinds of activities that we're going to be engaged in. So this report will go - it's gone to the Board at ICANN. Then it will be sent along to the GNSO, which is basically - how would you describe that Avri? You sit on it. Policy committee?

Avri Doria: It's a policy - yes. It's a policy committee.

Stephanie Perrin: Jolly good. At that point they will decide what to do with it. Do we strike one working group, two working groups, 15 working groups? Do you decide at the GNSO level that we like this, this, this but not that? That activity will go on. And folks like Avri will be on that and the business community and everybody's representative. So there'll be another...

((Crosstalk))

Stephanie Perrin: ...visible punch out because the documents are on the Web. You can watch remotely from wherever you are and you can send advice to Avri for instance.

Avri Doria: So is there a way we can build something where we can notify you when there's something that we need reviewed, that we need comments on? Can that happen? Please?

Man: If I may. We - in the opinion that was published on Monday by the EPS we also referred to the last part of the discussion of the multi stakeholder model to (unintelligible) options.

The commission just to give credit to their communication already noticed that there is a problem for example for civil society NGOs to participate in ICANN just because they cannot hire 5 or 50 people doing nothing else but to run the two working groups and meetings and representing the organizations (thing).

We - the commissions asked that more stringent application of remote participation could be a way out but I think all that are here today know that is not replacing being here today to remotely participate. And we made this point and certainly appeal to this organization's staff run programs to (invest into that).

As regards the participation of data protection authorities, we recognize that in substance certainly privacy and data protection commissioners can make important contributions to the process. However, only on the basis that this is covered by their mandate and that they are given the resources for that purpose.

Quite frankly the European taxpayers represented by the Council and the European parliament does not consider that to also staff members travel so many weeks per year to places like San Francisco, Honolulu and others to represent data protection interest. That's not - just not the level of (unintelligible) that we operate on.

And that's probably even more the case speaking under (Ian)'s control for all the (unintelligible) counterpart and that's why we are not currently in a position to fully engage in that.

But Internet model like a resident expert where it doesn't necessarily require physical relocation but being in the background answering on requests or giving assessments of draft documents in the process, that's of course much less resource consuming and can also be done on a different timeframe. So I think this kind of model should be explored. Thank you.

Man: (Unintelligible).

Avri Doria: One of the things Volker pointed out to me and then I'll come right to you is that most of the work of working groups is done on the phone. So people don't have to travel for that. They just have to give an hour every week or two to a phone call to be on one of our working groups.

Man: Oh, I think the last time you were asked the requirement of considerably beyond one hour per week.

Avri Doria: That's only on the phone part. It's however much time you put in prep...

((Crosstalk))

Man: ...should be realistic about logistics but some kind of advisory support relationship would be feasible. But we really kind of direct in terms of what it if you want to help with, what issue you want advice with. We don't want to (stand up) and try and solve all your problems because you've got a lot of them and it's - you've been doing it for a long time.

Avri Doria: But they're all our problems.

Man: But they're really direct in terms of which aspects of system design or law or whatever it is you need help with. And then we're in a much better position to use our limited resources in an effective way.

Avri Doria: Thank you. You're (unintelligible).

Woman: Thank you. Actually I'm - I think that it could be a good idea if we can have - if we can use the social media to connect and to comment on this document or maybe other ideas. We can take that document - I didn't see it, excuse me, if it cannot be done you can decide.

But I think that if we can - it's hard to do all the document and to comment on it. We can take it by paragraph or by part and we can collect the idea about the comments and work on it.

Another thing we can maybe work on knowing was - and getting in touch with are the groups that are working on issue related or that could be interested by this privacy.

Also personally I can also advise to make maybe - I don't know. Those who can do it (a Sunday night), whatever around this document. I will consider

doing this during the event I talk to you about where we are going to discuss the creation of a commission for (informatics) and (events around the net).

So it is really so dependent on how much we are involved and how much we do care. I'm not with the shutting down. I am with Whois. (Let me) stay it's the same as they are.

I am - because this information we do need it also for security and for (unintelligible). But I am with the recommendation, with rules and with limits. And most of all we have to avoid any illegal abusers of this instrument. And we can benefit maybe from the moment from this - what is happening about accountability and responsibility of the ICANN, this transition. Thank you.

Avri Doria: Yes. We're definitely going to have to work on that. Okay. Got only a few minutes left and I do - I have (Stephanie). Did I have anyone else - and the gentleman and that'll be the last and then I'll say something very quickly here. Please.

Woman: We have a meeting in LA in October. And I think that we could have a very big event and really draw attention to this. I mean just really plan it and make it 3000. And I think that there's this - there's no issue unfortunately because I think there's some more important issues. But there's no issue that really people feel stronger about at this point in time. And I think it could be a very crucial important thing to organize around.

Avri Doria: Thank you. (Stephanie).

Stephanie Perrin: I just wanted to see if people were interested. Most people don't need another list serve. But would they want - would they participate in a say a call updating on all the various activities say once a month for an hour? And the folks who are active at ICANN could tell you what's going on. Because I know it's very hard to keep up and it's one thing for ICANN to have all the records

up there on the Web but you got to read them, right. It's easier to listen to a call while you're working.

Avri Doria: So monthly calls one thing. And we could organize it. Please. Who had your hand up? Yes. You did. Didn't you? I though you did.

(Jeff Sassoon): I thought it was somebody else before me. (Jeff Sassoon) for the record. Well I think privacy rights is a fundamental human right that is also a cultural issue. It's - this is very much reflected in the variations of the privacy laws around the world.

And well I mean I may be wrong - I hope I'm wrong. But I'm not seeing any - I mean I seem to be the only Asian or person from actually around, you know, in this room. I mean even in - on the table. And or, you know, so I hope, you know, to answer your question about what can make it better.

I think, you know, if it include people (unintelligible) because I think we have (curious) variations in privacy laws even within Asian countries. And a lot of us - a lot of countries barely having their brand new privacy law enacted in the past 12 months. So I think this is crucial.

Avri Doria: Thank you. Okay. So basically - okay.

Man: Sorry. But before we start signing up to extended participation, I think what's become clear is there's a lot of concern about any form of database being developed without incredibly strong safeguards.

And you know what. This sounds a lot like (Stephanie)'s dissenting report. And the issues around consent and what not. Why don't - is there going to be a next step there? Like is there going to be somebody to address the points that (Stephanie) has made.

Otherwise if we do have another call, we're going to be repeating these things time and again. I'd far more refer a report back about how that (unintelligible) person integrated or not and then we can engage.

Avri Doria: Okay. Report. I don't expect that her report will be integrated. I expect that it will be appended and it's only if we keep talking about it and we keep putting it in people's faces that anything will happen because what they're going to do -- my prediction -- is thank you very much. We let you append it to the appendix. We've been good. You made your report. Now let's move on.

This is ICANN. We have to keep putting it in front of people. So, you know, not asking you for continued involvement. Many of us will do continued involvement because it's what we do whether anybody's paying us for it or not.

But, you know, so that - but we have to keep putting it in front of people. So anyhow, what I've got is we're not going to do lists. We're going to try and do monthly calls on the issue for a while and see if we can attract people.

I think (Stephanie) had already said people should read the EWG report and other reports and send in comments. Sending in comments. Anytime anything is coming out of here, things can have issues reports, impact reports. So there are documents. So we can through some sort of, you know, social media make sure that people are informed.

If people don't want to pay attention to the fire hose that is the ICANN information stream about everything, we can try to narrow down that fire hose to just the privacy related issues, which is probably not quite as wide as the whole fire hose and try and get - what matters is people comment.

What you said about Asia is critical. What matters is people commenting from all around the world, not just from one or two regions. So getting those

comments in, getting more events going and now the time is up and I turn it over to Rafik to close it.

Rafik Dammak: (Unintelligible). Thanks. Well, it was (unintelligible) of three hours. Yes. I'm not complaining Avri. I'm really happy that we got people to stay with us to talk about all the issues and we hope to continue to send you updates and to brief you what is happening and how you can help us in concrete way.

So I'm not going to keep you more. Thank you everybody for joining us and hopefully see you soon. Thanks.

Robin Gross: Thank you. And if I can quickly also add a big thank you in particular to the data protection officers for coming today. This was really a treat for us to have the opportunity to meet with you and speak with you. Thank you very much.

Woman: And please leave us your cards if you'd like to stay in touch because we would love to be in touch.

Avri Doria: We do have a sign up sheet with hopefully email address on it.

((Crosstalk))

Avri Doria: Which will not be circulated.

((Crosstalk))

Man: Avri.

Avri Doria: Oh, we will send mail to those lists.

Man: Avri. We did data collection so we'll get the information on...

((Crosstalk))

END