

**ICANN Transcription - Marrakech
NCSG Human Rights Meeting
Wednesday, 9 March 2016 0900 UTC**

Note: The following is the output of transcribing from an audio recording. 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.

Also found on page: <http://gns0.icann.org/en/group-activities/calendar>

Stephanie Perrin: Okay so folks, we seem to be a very small but dedicated crowd this morning. So please come up and join us at the table. The folks who are speaking are up here, so don't worry we won't put you on the spot. Grab a chair closer. It's kind of a big room really. And we'll start in a minute as soon as we...

Okay is everybody reasonably ready?

Kathy Kleiman: ...actually put up a real Whois slide.

Stephanie Perrin: Good. Wonderful. That's good. None of the rest of us have slides. Okay. (Unintelligible) Hello everybody. I apologize for being a little late starting. We're still waiting for one of our speakers. But let me just introduce who's at this table here and who will be speaking.

On my left I have Kathy Kleiman, who will be telling us the history of Whois struggles over the years. My name is Stephanie Perrin. Kathy and I are both with the Non-Commercial Users Constituency. On my right, I have (Sophie Klosney) from the Council of Europe, and Peter Kimpian, also from the

Council of Europe and the Hungarian Data Protection Agency. So - and they'll be telling us - giving us a bit of background on Europe and their views on some of the things that are happening here at ICANN.

So without any further ado, we do have remote participation. I don't - is that yes? We have a couple of people online. So I'll be counting on staff to give me a wiggle when somebody has a question in the remote. And I guess any time now, have you started the recording? I should have given you a signal. Sorry. Okay. Okay very good.

I see the agenda up on the board behind me. My job I think is to just give sort of an orientation on where we are on all things privacy that are happening at ICANN. Without putting him on the spot, I'd like to identify David Cake there. Wave your hand, David. David is the - one of the co-chairs of the recently formed PDP on RDS -- help me out, David.

David Cake: Next Generation Registry Data Services, I think. But currently the PDP to decide whether we should replace Whois, the Whois system, we're already replacing the Whois protocol, and if so with what.

Stephanie Perrin: Right. And I must say I struggle with the name all the time so I call it Who 2, but the name has not caught on satisfactorily I think. Anyway.

David Cake: I think the next generation bit has a charming sort of Star Trek ring about it.

Stephanie Perrin: Right. Kathy has suggested perhaps it would be good to go around the table just very quickly if people would like to identify themselves and their interest here.

Kathy Kleiman: But in the interest of privacy, you don't have to.

Stephanie Perrin: Yes.

Kathy Kleiman: So, Kathy Kleiman the co-founder of the Non-Commercial Users Constituency and spent way too much time over the last 15 years on Whois, but I'll tell you about that later.

(Vincent): (Vincent) (unintelligible), University of Vienna, somewhat of an academic observer.

Tatiana Tropina: Tatiana Tropina, Max Planck Institute in Germany and a non-commercial user constituency here at ICANN.

(Aidan Thurdland): Hi. (Aidan Thurdland), member of the NCUC.

(Barbara Middleman): Hi. I'm (Barbara Middleman). I'm a relative newcomer to ICANN, non-technical person, and my interest is largely having to do with privacy in medical and biomedical applications.

(Mark Siden): I'm (Mark Siden) from the SSAC. This year I'm on the NomCom and also the membership committee for the SSAC, and we are actually trying to find a privacy engineer to participate in SSAC activities.

Maria Farrell: Maria Farrell, Interconnect Communications. I'm a member of the NCUC.

(Stacy Walsh): (Stacy Walsh), Interconnect Communications, member of NCUC, and I'm on the RDS PDP on the Human Rights Working Group.

David Cake: David Cake, Electronic Frontiers, Australia.

Woman: (Unintelligible).

Man: (Unintelligible) I'm a judge in Belgium in the commercial courts. Thank you.

Woman: (Unintelligible) I'm from Lebanon, professor of law, but mainly head of NGO. We're active in cyber security and actually we're a project on creating a commercial agency for personal data protection in Lebanon.

Man: (Unintelligible) from Jordan. I'm a judicial assistant at Jordan Minister of Justice and IP student in IP law in Jordan. Thank you.

Man: Hi my name is (unintelligible) I'm from Morocco Next Generation. I'm a telecommunication engineer and I'd be interested in human rights issues for present and civil society in Morocco.

(Motico Ayzela): Good morning. My name is (Motico Ayzela). I'm with the Institute for Human Rights in Business.

(Bastien Hostings): My name is (Bastien Hostings). I work for the Amsterdam Internet Exchange but I'm here on behalf of the Dutch Internet Society Chapter and At Large structure.

Stefania Milan: Stefania Milan, University of Amsterdam and GNSO councilor of the Non-Commercial Stakeholder Group.

(Nielson Hoover): (Nielsen Hoover). I'm with Article 19 and I'm chairing the Cross-Community Working Party on ICANN Social and Corporate Responsibility to Respect Human Rights.

John Selby: John Selby, Macquarie University. I'm doing a research project on the intersection between international trade law and Internet governance, and Whois is one of the first issues which is emerging there.

Peter Kimpian: Peter Kimpian from (Aim), originally from the data protection of Hungary and member of the TDP, which is a advisory committee to the (unintelligible), which is a data protection convention of the Council of Europe and we'll be talking about this later in more detail.

(Sophie Klosney): And (Sophie Klosney) from the Council of Europe in Strasbourg, and I'll be telling you more about our work later.

Stephanie Perrin: Okay thank you very much. Okay briefly, how many here have been following closely the privacy work that has been going on at ICANN? Okay. So I apologize for boring you but I'm going to give a brief update for those who haven't on this - the initiatives that we've recently had.

There was a very large PDP that went on for policy develop process that went on for a year and a half on the issue of whether or not - or rather, what accreditation issues we had in terms of the privacy proxy services accreditation project. There had a recommendation from the board I believe to accredit privacy proxy services which have been operating for many years now without any kind of official rules.

So the determination was made that privacy proxy services should be subject to some kind of accreditation and this group was struck to examine the issues. The report was passed by the GNSO. I actually believe there may a mention of the PPSAI report in the GAC communiqué. It was a long - that would be the GAC communiqué that is coming this week. It was a long and fairly fractious discussion. One of the issues that we had some tension over was whether privacy proxy services should be available only to individuals or also to commercial entities, small groups, NGOs, in other words non-individuals.

And we decided in favor of allowing it. I must say that we had - there was a petition that went on during the call for comments period, and we go how many, Kathy, was it finally?

Kathy Kleiman: We got one petition with 10,000 signatures and numerous comments, as well as 15,000 other comments. I know because I read through most of them.

Stephanie Perrin: Right. And thank you for doing that. So that was a record in ICANN's history in terms of the number of comments we got. So that more or less settled the dispute on whether or not privacy proxy services should be available to everyone.

So that recently closed. We also had an implementation committee of volunteers looking at trying to improve the implementation of the law ending policy on conflicts with law. And if you're not aware - sorry? If you're not aware of this policy, it basically tells registrars that in the event that they determine that their Whois requirements are in violation of local data protection law, they should bring a binding order indicating that that's the case that they are violating the law to ICANN and ICANN will give them a waiver from the legislation. Now - from the Whois requirements.

There's a separate process that is not under this policy for a waiver from data retention requirements which are also illegal under some laws. And the data protection commissioners have been writing ICANN repeatedly saying, particularly for Europe, all of our data protection agencies agree that this is in violation of our data protection law so give them all a waiver. And ICANN has not recognized that letter.

So there's quite a bit of frustration on the part of the registrars because they have to go out and seek this authorization from the data protection commissioners. Data protection commissioners normally don't give opinions on that before you break the law. So they were in a classic catch-22, if you are familiar with that expression, and there was quite a bit of frustration. We had quite a few registrars on the group.

Nevertheless, the policy continues and I don't think we solved the improvement question, improvement to the triggers, which was our task. So the next question is what do we do about that policy? That would be up to the GNSO to decide to alter that policy.

So that - you will find if you look on the ICANN website that there is an area all things Whois and a list of these projects. I'm not going to go into the more technical ones except to mention that there is a call for comments out right now on the RDAP implementation. The RDAP is the Registration Data Access Protocol.

And several years -- well not several years -- but a couple of years ago when the EWG finished its work, that's the Expert Working Group that was commissioned basically to look at the Whois and make recommendation, we did make a recommendation -- I was on that group -- that there be tiered access, in other words that instead of everybody getting access to Whois without authenticating themselves or identifying themselves that it should be tiered and, you know, that some elements should be public and then underneath that, you would have to identify yourself and provide adequate purpose and reason for getting the data.

In order to do that, you need a new protocol. And the RDAP protocol does facilitate that because it has differentiated access. That - so this is a necessary technical improvement to allow some of the policy requirements. Sadly the policy requirements have yet to be determined, and quite frankly, the new Who 2 has only just started. And Chuck Gomes, who is the chair of it, was joking the other day that it would only take us three months. My guess is five years. I shouldn't say that because I'd love to have any of you join it if you'd like to.

David Cake: You're terrifying me, Stephanie.

Stephanie Perrin: It's probably somewhere in between three months and five years. I see David has his light on.

David Cake: I just said you're terrifying me with this five years. But I just wanted to clarify something about the RDAP implementation just in light of your comment. So RDAP is a replacement for the Whois protocol. It has both pros and cons

from a privacy point of view. Certainly it's more secure. But you mentioned the differentiated access or tiered access. That is not going to be implemented in the current RDAP implementation, which they're doing now, because that would be a major policy change.

And there's actually probably still a few policy implications of what they're doing now, you know, the GDD is sort of flipping through when they should really have put it to some sort of process. But they are doing that differentiated access on the current RDAP implementation. It certainly is the case that the EWG recommended it and the Next Gen RDS may also end up recommending it, at which point they probably will implement differentiated access, but they're not doing it yet. But the RDAP protocol allows for it, where Whois does not.

Stephanie Perrin: Thanks, David. Anybody who would like to put their comments in and recommend that ICANN recommend that implementers construct their systems so that they can do it as cheaply as possible, we'd love to have you do that. Thanks.

I'm going to now turn the mic over to Kathy Kleiman who's going to give us a history of previous work on Whois, so that'll help us understand what's going on with this rather large PDP that's just started.

Kathy Kleiman: It occurred to me in my introduction that I forgot to do the promotion (unintelligible). So. There's an echo. (Miriam), I just sent you a note on that. Can we put up that slide a little later? Can we go back to the agenda slide? We'll get around to this.

Okay. So by day, I'm at a firm called Fletcher, Heald & Hildreth, the U.S.'s oldest telecommunications firm, and I run the Internet Law and Policy practice. And so I'm going to be devil's advocate for a second here and tell you what I've heard here for 15 years, which is that domain names are important pieces of information and people use them on the Internet to post

all sorts of information that's illegal: counterfeits, illegal activity, defamation, fraud.

And so it's very important to be able to track who is the domain name registrant. And ICANN inherited a system that had a system - it inherited a directory services, we call it the Whois, but it had a lot of information in it. Can everybody hear me if the microphone's not directly in front? In that okay?

So we had a lot of information in it. So I went back to the old techies to ask where that information came from. So national - and how this Whois developed. And what I was told by (Scott Bradner), who was Harvard IT, I don't know if he's retired yet, but Harvard Information Technology for a million years. Is he still there?

Man: (Unintelligible)

Kathy Kleiman: In two months really? And in his honor, I wear sandals all the time. And so (Scott) said that it goes back to the NSF days when it was a closed network and a trusted network and if you wanted - he was running Harvard.edu, and if the guy that ran mit.ed - there was a problem with the T1 line down Massachusetts Avenue between Harvard and MIT and they wanted to know who to talk to, they looked up in this Whois and it was (Scott)'s information. It was his name, it was his business address at his Harvard IT office, it was his business phone numbers, we didn't have cell phones then, and it was a fax number.

And that was -- and his e-mail. And normally they sent e-mail but occasionally picked up the phone and called each other, and I guess sometimes they had lunch, you know, and figured out where the office address was. That's the model that scaled into a global database for about 400 million people. Every speaker on the Internet who uses a domain name now has to put their name, address, phone number, e-mail, you are excused from putting your fax number in now.

And that's what scaled really without looking at very closely. Except we did try. And I should say my background includes I interned with what became the Electronic Privacy Information Center in the United States early on, and years and years ago I was also an intern at the Israeli Ministry of Databases (unintelligible). And so I was exposed to data protection structured that don't exist in the United States, those that were in the European Union and that's many, many different ways of looking at things.

But the Whois is - well actually let's look at the record. (Miriam), can we look at the record now? Let's take a look at what a Whois record is because we spent all of our time talking about a few fields which have to do with data that identifies people. But most of it's something completely different.

We're going to page through the whole thing and then go back up to the top. So this is only part of it, and we'll keep going down. And I've highlighted it. The highlight is mine. So this is a sample Whois record of Amnesty International. So they're amnesty.org. They've got a domain name ID which is unique. They've got - the really important thing is who's the registrar, who's the one responsible for putting this up in the database, kind of who can take it down if there's a technical problem.

So the registrar is there. The updated - I'm going to kind of go through. We have an updated date and a creation date. Actually these create infinite amounts of spam because coming close to the expiration date, registrants will get a lot of information that says you have to update, you're going to lose your domain name, and often it's not from their registrar, it's from somebody else. And that's creating a lot of problems with spam and mis-re-registration and people getting credit card data.

So we have the expiration date, we've got the registrar, which is Network Solutions here, and an ID number. Something new through the Registrar Accreditation Agreement of 2013, there is a registrar abuse contact. You'll

notice that's not personal information. They've created an e-mail address and phone number so that whoever's sitting at the desk can be contacted.

In this case, Amnesty International has put in special protection, client transfer prohibited. So you can't transfer it -- not easily, because there's a lot of hijacking that goes on among domain names. And you see that there is - we see the registrant name, so they're identified as Amnesty International, the street, the city, the state, the postal code, the country. In this case no phone number's been entered. That's going to change. There's a real push for accuracy and completeness among this data.

(Miriam), can we page down? There is a fax number, interestingly. And of course a registrant e-mail address, which is actually really important. So they have - they've created a DNS admin at amnesty.org to be contacted if there are any problems, and that makes sense. And that way, if someone's on vacation someone else can answer the e-mail through the administrative - the general administrative box.

Notice now there's - we, in addition to registrant, we now have administrative name, organization, street, city. And in this case Amnesty, as so many noncommercial organizations and so many individuals, has just repeated the data from the registrant. But if you go down a little further there's a third contact, which is technical. And sometimes you'll see the same data for registrant, admin and tech. But in this case they've said that if there's any technical problems, go to Network Solutions and they'll solve it, which makes sense so you're going to the registrar to handle technical problems.

And then at the very bottom, you have what you really need on this which is the name server, where do you find this domain name in the Internet universe, in the (TCPIP) universe where would you go to actually get the website, get the information, the e-mail, the list serves associated with this domain name. And in this case they have four name servers, which probably indicates they get a lot of traffic.

Can we go back up to the top? Thanks, (Miriam). And let me just give you a pause. What if this were Charlie Hebdo? We're identifying the location of an organization. And that's creating infinite numbers of problems. Twenty years ago I started seeing these problems coming through, harassment, stalking, some related to the DNS, some not.

So harassment, somebody's got a really cool domain name, somebody else wants it. They're going to send - they send all sorts of letters. Cease and desist letter. You have a generic word, a really big company wants it, a lot of cease and desist letters will past. I've seen individuals, small businesses, small organizations for no good reason under trademark law threatened with trouble damages, jail, all sorts of things.

I once went up again a billion dollar company, who had found my registrant through the Whois, and told them that if they didn't stop their crazy claims I was taking them on the Tonight Show and we were going to ridicule them nationally, and they pulled out very quickly.

But what's happening, you know, it's one thing to threaten to try to get a cool, neat domain name that you otherwise are not entitled to, but, you know, real people are threatened here, journalists, bloggers, home-based businesses, small businesses. This is - this home address, this address that often winds up being home or identifying where an organization is that's controversial is very upsetting.

So since the beginning of time, the beginning of Internet ICANN time, we've been trying to pull back and we've had Whois task forces. And what you're going to find, and not around people at this table but if we had the full ICANN table, the first thing you'd find is that most of the people in this organization want more information in the Whois, they want more identification of that information, they want it to be more accurate. Whereas I want to pull most of it out or at least the stuff that I've highlighted.

So let me tell you, instead of going through kind of long history of ICANN fighting this, what I'm going to do is focus on the Whois review team and the final report that we created. We met for 18 months where a requirement under the affirmation of commitments, which is part of the deal that the Department of Commerce gave with ICANN when they gave ICANN more independence, I don't know, five or six years ago now, maybe a little longer.

And so we were a group of law enforcement and government and noncommercial and intellectual property, and we met for 18 months looking at the Whois record, looking at Whois uses, talking. And we came up with a set of findings. I'm just going to go through it briefly with you. One is that Whois should be a strategic priority, that ICANN should stop messing around with it in lots of different corners and try to figure out what to do with it.

Two is that there should be a single Whois policy. It turns out that Whois was actually buried in registry agreements and registrar agreement. And to really understand what we were doing about this directory database, it was buried in all sorts of different places, we said pull it out of the closet, let people know really everything that affects Whois.

Outreach. We said, you know, there are a lot of people who don't want to - who don't follow ICANN's kind of convoluted discussions who might be interested, like data protection people. And so we said if there's a proceeding, let's go out of our way to make sure. Through ICANN and its staff let's go out of our way to make sure that outreach reaches people who would care about this one proceeding among all of ICANN's other proceedings.

Data accuracy. They got that through. A lot of people want whatever winds up in this database to be accurate. Proxy and privacy services. If you can't - this is something the market created. Does everybody know what proxy privacy services is? I'll just summarize it briefly.

It's when you go to something like Domains by Proxy and you - so when I register a domain name with GoDaddy they say would you like to pay extra, \$10 a year extra for privacy service? And I say yes. And it means that they put their Domains by Proxy, which is kind of a co-owned company, their name, their address, and their phone number in the database so I don't put my home address in. There's always a move within ICANN to ban proxy and privacy services. We just created a process for accrediting them, but there's always a move to ban them and it will never go away.

(Nielsen Hoover): I have a question because I've seen different implementation about this under different TLDs and also difference between ccTLDs on how this can be done and I've also seen free services and paid services. And so is this - so my question would be, A, is the user of privacy proxy standardized and is there a difference between gTLDs, ccTLDs in implementation or just in RAA, or where does the difference stem from?

Kathy Kleiman: Okay. So privacy and proxy have only recently been like recognized as actually existing and now they're accredited through the gTLDs. But there's no standardization. Some, depending on - and country codes are totally different. ICANN does not regulate country. It does not do any policy with country codes. It coordinates among the country codes but country code are not, unless they've chosen to sign a contract with ICANN, which few have, they're not bound by ICANN for their policy. So whatever they're doing with Whois is their job. Some are publishing the whole directory service, some are publishing nothing.

Australia, at least the last time I checked, if you went to Microsoft.com, they would not give you the corporate address. They would confirm that Microsoft was registered, Microsoft.com.au, but they wouldn't give you the corporate address. They said they don't need to.

So - but in the gTLDs were different. All generics are regulated by contract and - but still, among the different privacy and proxy services they're their

own implementations, the one thing ICANN will make mandatory is that they have to respond now because a bunch of them weren't. But I've talked with European registrars who also offer privacy services who say they don't believe under law they can charge for it. I assure you in the United States they believe they can charge for it. But let me turn it over to Stephanie.

Stephanie Perrin: Yes just -- Stephanie Perrin for the record -- I just wanted to jump in here and say it's not something we've made a whole lot of noise about but at least in Canada the data protection law is very clear. You have to tell people what their rights are and state your policy. And ICANN in the 2013 RAA has all kinds of rules about registrars, what they have to do that are basically competition between registrars' base I would say in terms of motivation.

But there's no requirement to tell individuals about their data protection rights. Now the registrars themselves apply their own law. The RAA says you have to tell people that you have proxy services if you run them and how much they cost. But one of my frustrations is it makes a big difference whether you're getting a .ca or a .com in Canada, and nobody tells you that the country code has a much better privacy policy than the other gTLDs. In fact the average user doesn't know what a gTLD is or a ccTLD, and nor should they in my view, you know. Life's complicated enough. Thanks.

(Nielsen Hoover): Sorry to break the flow a bit, but I have a question to the Council of Europe's expertise a bit on this. Is there any chance we could perhaps push for enabling a privacy proxy by default?

Man: Well this is a difficult question. We've been also assessing this new document on privacy proxy services but we understood that this is a fruit of a compromise already. There are of course certain additions which has - which could be also made, but we will be looking at it in the future how to improve this. For now I think this has been already accepted as it is, or it will be soon accepted.

(Nielsen Hoover): From the ICANN document I understand, but from a legal standpoint, like European privacy protection?

Stephanie Perrin: Please remember to state your name for the record. Yes thanks.

(Sophie Klosney): Privacy by design and privacy by default are definitely principles that European data protection laws are trying to promote and implement, so that's certainly something at the European level could be - yes could be pushed for by European data protection law.

Man: However being said that, I would also emphasize the right of the data subject I think that would be the most important thing to depart from, so what are the data subjects, which chooses or which not. So I think both have to - it can be open. And of course privacy by default is one of our major priorities as privacy by design. However, the choice of data subject will overrule anything in my view.

(Nielsen Hoover): (Nielsen Hoover) for the record. Thank you for that great and informing answer and I think this comes back to Stephanie's answer of the importance of informed consent that if we want to work on informed consent, then I think we really need to work with the registries and the registrars on the signup forms, because there is very little except for I agree with terms of agreement, which is I think the biggest lie every day told on the Internet because no one actually reads and agrees.

Kathy Kleiman: You can't work with the registrars on that. They're bound by contract to do just what they're doing. I mean they can't opt out. They can't give you more options. They're bound by contract. ICANN makes them collect that data. And so I just wanted to share -- and I'm almost done -- that the Whois review team came to a startling conclusion, it was startling for ICANN anyway, that all types of registrants actually want privacy and don't want to put their data in that open 24-hour accessible, you know, 24/7 accessible record.

And I'll just read quickly, individuals would prefer not to have their personal data published on the Internet as part of the Whois record. Organizations, religious, political, ethnic minorities or those sharing controversial moral or sexual information are concerned. And companies, even companies want privacy and protection from this kind of publication for upcoming mergers, new product or service names, new movie names and other types of product launches.

And because we didn't get it right, and this is the history ICANN, because we came up with too much privacy, immediately after Stephanie was drafted to be on the Expert Working Group because privacy is a hydra in ICANN. You cut off one head and two grow. And so I'm glad you guys are all here. That's the history of Whois at ICANN.

Stephanie Perrin: Okay. Stephanie Perrin again. Thanks very much, Kathy. Any questions on this before move on? Yes?

Man: (Unintelligible) from Jordan. I want to ask Miss Kleiman if I got my point - your point, you said that the name of the streets, the name of the city cannot be registered. Actually in my country because - as a developing country, these things have been taken into consideration by registrars. So I think that ICANN cannot comment in the future, except in a process that for developing countries to take these things into consideration.

Moreover I want to ask who has the right to object that user registration of domain names they're using. If someone registers the name of a street, does the government have the right to object the registrar or the interested party is anyone of their community? Thank you.

Kathy Kleiman: Could you give me an example, kind of a quick example of what you're...?

Man: Yes. If someone registered the name of a street, who has the right to object to this registration to submit a application to object to this registration.

Kathy Kleiman: The street address is wrong?

Man: Yes.

Kathy Kleiman: If the street address wrong. So instead of putting in my home address for a new home-based business, I put in 555 Main Street. Right now you can go to ICANN Compliance and it's possible they'll take that domain name down. It's possible they won't, it's a little inconsistent, but it's possible they will.

Man: Thank you.

Stephanie Perrin: Yes, (Mark)?

(Mark): It seems like a lot of the privacy concerns hint around doing business with the public so that entities that take money from the public and could defraud might be required to have less privacy or more easily pierceable privacy in fraud cases. And for me, that seems quite reasonable.

Your Charlie Hebdo example is a perfect one because they take money from the public, but, as you could see, they might have benefitted from some privacy. Although as it turns out of course their Whois record was not used to find their office and shoot them up. So, you know, you can't solve every problem in society by putting privacy in Whois.

Kathy Kleiman: For what it's worth, I run a nonprofit called the (Unintelligible) Programmer's Project. I'm dedicated to telling the story of women in the early history of computing. There were lots of them and we don't know about them. And we do take money, we take donations, but they're all through PayPal and another - a group called Docs in Progress. So should we lose my privacy because we do collect money but it's through other sources -- and most small businesses and others are working through PayPal.

So what we found as we debated this over many, many years is that it becomes more and more complicated the farther down we go. It's not as easy do you take money, because often you're not taking it directly, you're going through. And that's why PayPal and others are wonderful. So very complicated but a good point and it comes out often should we ban any kind of privacy for commercial entities and keep it for noncommercial. And again, the finding of the Whois review team is the commercial companies want it to, want privacy.

Again, if you're merging, if two companies are merging you're actually, at least in the United States since there's security laws, not allowed to reveal that merger until a certain time. So even though you got the domain names, you're all lined up, you can't tell, you know, the market has to find out all at once. And people were finding things out by seeing Whois registering certain domain names. So there's all sorts of reasons, but it gets complicated because of course you do want to find out who's behind somebody, you know, an e-commerce site that's fraudulent.

Stephanie Perrin: Stephanie Perrin for the record. One of the things that I'm a little bit rabid about, quite frankly, as a former government person, retired now, governments can regulate e-commerce. ICANN has a very limited remit. I would like to keep a very, very bright line between what ICANN has the authority to regulate, because let's not kid ourselves. If you cannot sell a domain name unless you sign on to the ICANN contract, then whatever is in that contract is regulation by any other name. It's regulation through contract.

And we do not want ICANN to start looking into the uses of domain names and deciding this one's good and that one's bad. And keeping that bright line is extremely difficult particularly with the new gTLDs where they're putting on social conditions in order to get such and such a name, a top level domain. So this is going to be one of the challenges I think in the upcoming Whois review, which you should join by the way, (Mark).

Kathy Kleiman: Because we're going to do it all over again.

Stephanie Perrin: Yes please?

Man: Yes thank you. (Unintelligible) from Morocco Next Gen. I'd like to raise a question about the privacy that we're talking about. Actually all the privacy issues that I heard if I understood well are concerning protecting from hijacking or from privacy or things like that. But I would like to know we are here in Africa, we are in Morocco so it's not like the west and it's other situations that we have here, other problems that we have in this region that are not the problems that you might have in London or in other places.

My question is that privacy should not only protect people from those issues, like theft or cyber crime or things like that, but privacy in my opinion, and I think other people share it with me, is that sometimes you have to protect people and citizens from their own government, you know. When you write an address it might be someone is doing some kind of activism or someone in some other position movement. And when the government has the address, it becomes easier for them to harass them or to make some things for them.

I know that this is political issue because it's also a matter of sovereignty and I ask a lot of questions here in this ICANN, which is my first one, but (unintelligible) and a lot of people just answer me this out of scope or ICANN doesn't work with that.

So I'm just wondering that - how you deal with that because I know that you would say that government is sovereign in its country but you're all people of human rights so how can you deal with that? I mean government should be sovereign but at the same time government cannot do things that are not allowed under international laws. So that was my question. And I just wanted to focus on the region because we are here in this region and you have an opportunity to talk about London and west in other meetings that are in the other region. Thank you.

Stephanie Perrin: Stephanie Perrin for the record. Thank you so much for that intervention. We'd love to have you join NCUC or join civil society here. But I'm passing the microphone for (Sophie Klosney) to answer that question.

(Sophie Klosney): Yes thank you. Because the question is actually leading to what the Council of Europe is doing. So maybe to start with just a broader explanation of what the Council of Europe is because it's not clear for Europeans so I can imagine it's even less clear outside of Europe.

So we're an international organization, so it's a regional organization, based in France in Strasbourg, so nothing to do with the European Union in Brussels. Even if the European Union also has the council of the European Union, so the mixing of names makes it very difficult. Unlike the EU in Brussels we have 47 countries, so we already geographically spread really completely at the east. We have Russia, we have Turkey for instance. Those are countries that make big difference in terms of EU Council of Europe.

Also our identity's completely different. To start with, after Second World War European states decided to create stronger bounds between the states. One direction was economic ties at the EU, the other one is the human rights identity, democracy and rule of law organization. That's the Council of Europe. And we have the European Code of Human Rights in Strasbourg, which is a unique judicial institution.

Our member states, so it's 47 countries, have all ratified the European Convention on Human Rights and can be taken to the court by individuals for violations of their rights, and this is about violations by states, so that's clear. So this is our Article 8 of the convention on the right to privacy. But we also in the late 70s starting working on the convention on data protection, specifically on data protection.

This convention is 30 years old now, so it's an old instrument. We're modernizing it. What is very interesting is that this convention was already thought as a global instrument. So it's not limited to European countries. Any country in the world can exceed to this convention.

There are a number of conventions in the Council of Europe that are like that and I want -- and I'm sorry for the privacy-sensitive souls that are here -- I want to mention our cyber crime convention, which is a good example that I would like to point out because the USA have become party to that convention.

So we can have United States becoming party to conventions of the Council of Europe. I wonder why cyber crime had more interest than our data protection convention, but this is really something in your countries you need to push for your government to come to the Council of Europe and say we want to ratify.

And actually Morocco has been invited to join the convention. Hopefully, as they will be holding in this same center the data protection conference this year, the annual event, they promised that by then they would be parties to the convention. Not everything is ideal in the Moroccan legislation. We have pointed it out in our opinion and in terms of scope of application to police, for instance. That's something we have to review.

But so what is fundamental with convention 108 is that it has your horizontal scope. It applies to public sector, law enforcement and also private sector. So here a definition of the work of ICANN, law enforcement access to the data is something that can be protected by the principles we have in the convention.

I want to mention other countries to show you that there is a momentum for convention run rates, extending outside Europe. We have (Morocco), who I mentioned, (unintelligible) invited. Now (Capoverta) just requested. Iroquois is already a party. It was the first on European country.

So please, in your countries, push for this convention. It is the only instrument in the field that can protect individuals worldwide, I mean legally binding instruments.

Why the role of the Council of Europe is important and I think in the discussion and in the work. It's an intergovernmental organization, so here intersecting of ICANN, our first entry point was the GAC. We are observers in the GAC because we are an intergovernmental organization. Even if we work in a multi-stakeholder way too, involving our discussion, all interested parties.

We focused in ICANN in feeding in the work of the GAC as observers. So I am a newcomer to ICANN. So I'm new to ICANN, which doesn't mean that ICANN is a new to me because if I can also come back to what we have already done.

The committee of convention run rates, which is basically all the representatives. At the moment it's 47 countries that come to Strasbourg to speak about data protection and the convention.

All those delegations in this committee already in 2012 responded to a request by NCDC by Robin Gross at the time underlining the privacy concerns we had with (them). But indeed, lectures was not necessary or effective.

So we decided to come to the meetings, feed a bit more effectively in the work. And (Dieter) will tell you in detail what we are doing. But also more recently, and I'm glad that (Monica) is there, the Council of Europe facilitated a report on basically ICANN policies and human rights.

I think it was really an important report. It led to further visiting of the need to do this work. So (Monica) was (costering) the report with (Thomas Schneider), who's currently the chair of the GAC.

There is a specific chapter in this report on privacy and data protection issues, so I invite you to read it. It's interesting to (Monica) to see that your recommendations, you're doing generally the list of points to see the progress.

And I see there is progress. For instance, the mention of human rights in the bylaws. That's something that can be acknowledged. So things are moving.

I just want to maybe also give you the broader picture about Council of Europe and ICANN, so not solely about data protection because we are a human rights organization. So we're also working on other human rights like freedom of expression. My colleagues are dealing with this topic.

And we have 47 countries that adopted last year's declaration on ICANN human rights and the rule of law. It's important because it means that those 47 countries have committed to a position. And I will read just one of the paragraphs which I think is very relevant.

Internet users should be able to exercise human rights and turn them into freedoms without being subjected to unlawful, unnecessary or disproportionate interference. This right should prevail over the general terms and conditions of service of private sector Internet companies and the technical mandates of specialized entities such as ICANN.

So 47 - yes, this is available online. Forty-seven countries that actually are represented in the GAC have committed to this position. And what is also interesting is that they have mandated the Secretariat to assist ICANN and its communities basically to ensure that human rights and rule of law are referred and considered in ICANN.

So the Council of Europe is really there to assist the communities to achieve that. I'm ready to respond to any questions that I think that will give you further information about completely the work we're carrying. Thank you.

Man: Yes thank you very much. So I will start with (them), if you allow me, with some basic questions. So what is ICANN's dealing with its primaries IP address and the NS address and all related data?

So if you go a little bit further and we put it in a human rights context, or at least in a legal context, does the IP address have any rights already? I would say not as far as I know. Humans and persons have rights, but not IP address and the NSs addresses.

However, we have to be - we have to start to be familiar or to get accustomed to the treatment of IP addresses as persons. Yesterday I heard a very interesting and for me strange intervention from a speaker.

He's saying that you are all IP addresses in the room. That you. I didn't know that. And at least I have three IP addresses carrying with me, but okay, never mind.

So this is let's say a trend. I would also recall you or invite you to read, it's a white paper prepared by Cisco about Internet of things, which is \$4.6 trillion business. So it's obvious that in the future you will be having a lot of IP addresses to be born and processed.

And ICANN definitely will have a role in all this. So what kind of rights IP addresses or this related issues have? So what has been rightly pointed out by (Sophie) is the one issue of the cyber criminality, which is the IP addresses can be a target of it and data protection and privacy.

So Council of Europe have - this is the only international institution that has convention in both of these issues -- cyber criminality and data protection. So this is how we are. We connected at first place to ICANN and to this fair.

And now I will, if you'll allow me, go up a little bit further in detail. But for that I will have to switch to data protection, again. I'm sorry. There's no interpretation for this. Please stop me if you don't understand anything or I would be glad to answer your questions later on.

So for us ICANN is, as I tried to in my introduction point out is a global data controller. It's - it was generating a network of data process or if not data controller themselves. So this is an interesting question also.

And a data controller who has extensive relation also with law enforcement community, international law enforcement word I would say like this. And I have noted it is just - I noted that there is nobody from law enforcement committee present here at this session, which is - which I find, it's sorry for this.

And to go further on about, or with the data protection and privacy considerations. So European institutions have already pointed out some generate data protection and privacy issues, which can be associated or which can be analyzed in ICANN's work.

It was mainly the (unintelligible) working party, which is the European Union data protection body and the Berlin group. And those concerns were about the purpose limitation, data minimization, access to data, proportionality, data accuracy, finality and data retention type of issues.

So these concerns were very general. I mean it didn't go very much into details. So what we have decided, well not we, but the Council of Europe at first place by the declaration (Sophie) referred to by the Council of Ministers.

And after that following this, the TPD, the committee for the commission run rate to go further on details on these issues and on other issues which come to light during our work or our cooperation.

So since Dublin we have decided to participate in working group. So we have - we are member of the working group (PDP) on (RDS). And also we are member of the cross-committee working party on human rights.

Of course, ICANN and the functions of ICANN are very new to us. And we are also learning the process. However, we are committed to work on - in this working group and deliver our expertise in that.

We have already spotted some policies for our privacy and data protections can be at stake. According to us, these are the new gTLD policies, the Whois too, this (RDS) working party, the privacy proxy services, the (AA)s, the Whois low conflict, the (fake) Whois and the public safety issues and the (drives) to GAC about public safety.

Where I can only reiterate that 47 member of GAC have strong commitment towards privacy and data protection and more generally to human rights. Also that can be of interest of the public - the discussion about public interest, what is it?

And I can tell you this is a very hard topic. It's - even in the European Union we have (really bad times to define) what is a public interest, especially customer protection and of course competition can be issues where data protection privacy can play a role.

So our plan in the future is to participate in ICANN meetings and in between meetings activities like working parties activities by an expert. For a moment it's only me. But maybe in the future we can be or there will be some other experts also from Council of Europe. Our main goal is to channel, as I said, our expertise on data protection and privacy issues due to ICANN PDPs.

As the conclusion, I can say that we are of the perception that ICANN is at the turning point. We clearly saw that a lot of its constituencies and persons are willing to have a momentum in ICANN in order to become a more than responsible and global organization with respect to human rights.

And I think in that we can work together. We can catch you efforts and burden also. We are here for you, for all the constituencies, registries, registrars and also law enforcement because it's very important to speak about these issues because there is (accurate) threat around the world.

And - but it has to be done - data processing has to be done according to very well recognized principles that we really want to help you to implement in ICANN. So basically that would be my perception and my vision of the actual work and the future work. So thank you very much.

Stephanie Perrin: Thanks very much (Pieter). Stephanie Perrin speaking for the record. I'd like to remind everybody to state their name for the transcript because this is going out to remote participants and there will be a transcript afterwards. So it's really helpful to have your name there to know whose speaking.

Over on the left-hand side there's questions. Mark first then and then we'll go down the row there.

Mark Seiden: Mark Seiden for the record. So asking what privacy rights and IP address has is very similar to a long asked question, what privacy rights does a telephone number have? We have a lot of history about that. It's very similar.

A paradox agree, one of the technical changes that's happened in the last few years that has increased the privacy rights, or the actual privacy of IP addresses is something called carrier grade NAT.

Right now carriers, because of the shortage of IPV4 addresses, are mapping their private address space into individual IPV4 addresses. And the logging that many websites do, which is purely IP address and not the source port number will indicate any of hundreds of people - possibly hundreds of people who are using/sharing the same IPV4 address.

Similarly, corporate proxies have found gateways to the same thing. So there is quite a portion in the technical community to, if you want to have meaningful logs, you have to actually record the source port number as well.

And the details of the way carrier grade NAT is being implemented means that the logging requirements are extremely onerous on the carriers to associate what outgoing port number corresponds with what customer. So they're trying to avoid doing that completely. They can comply with law, produce all their logs and it doesn't reveal who the customer is. It's an interesting technical development.

Man: If I can just very quickly react to that. Yes, it's (an outcome), but being so that the privacy is not something that is really meant to, okay I want to hide from the world and do as I wish or do anything I want.

Privacy and data protection has very well defined principles and rules which are stemming from those principles which goes for necessity. A proportion or finality of data processing. And that balance has to be strong about all - every inch of data processing activities in order to find out whether it's legal, whether it's serving the purpose actually.

But privacy is a very important human right. But it (unintelligible) you shouldn't allow to - for, you know, to be - hide from your duties or your obligations and responsibility.

(Stacy Walsh): Hi, (Stacy Walsh) for the record. Thank you for your comments. You picked up on something that I've been thinking about the last couple days is that

there are now law enforcement officials here around the table today, at this table, right.

Yesterday I was at the registrar and law enforcement panel, which was actually very civilized and interesting. And I think that maybe it's up to us to go out and invite them specifically to meetings such as this.

And maybe the next ICANN we should have a human rights and law enforcement or privacy and law enforcement panel, which would bring these parties to the table and get us talking.

Woman: Thanks. That's an excellent idea and we'll take that back and see if we can get enough time for that because I think probably a hour and a half wouldn't do it.

Woman: Thank you, (Exfona). I would like first of all to see - say that I'm so happy to hear that you is very educated. And...

((Crosstalk))

Woman: Yes, yes, yes. Excuse me. I was writing about it, so excuse me. I get confused. Okay. So because actually as you can see already in this room, there is no such understanding of the meaning of privacy and their right of privacy.

In the actual society, privacy is eroded with technology. And we do need to protect this erosion to happen again with what is going on in the domain name system here.

So first of all, privacy is not only a human right. It is a protector of many other human rights. You are not seeing that importance maybe now, but you will be seeing it when it will touch you and touch your rights and your private life.

Even if from our - from American system, the legal system, the American one, in the States there is a right said to be the right to be left alone. So even if you have a priority for the freedom of expression, do not forget that you have also to protect personal or private life of people.

If you don't do this, then excuse me, we are put like (nate) before the hard word. And it is not good, not only for our private life, for our business also. For all of our concerns, profession and everything else.

So what I wanted to talk about, excuse me, I have to say this about privacy. Look a little bit up about this, the right to be forgotten. It is an extension of - it's a natural development of the right to privacy.

You see, it is a need - we need privacy. We need to protect our privacy. I'm not talking as legal or jurists, I'm talking a citizen. In this information society where I am exposed all the time, we do need protection.

What I wanted to say before hearing the room is I'm so glad to see that you are educated because if you look at the GAC or at other meeting, you will see translation, you will see what other.

Well here, since at each session I don't see translation, which means many, many people who don't know - who are not English speaker cannot participate effectively. So maybe we have to ask ICANN to engage in her role as core because corporations has a social role here. So they have the responsibility of ensuring better participation in these meetings.

And about the law enforcement, I think that maybe they have other meeting, but believe me, they are interesting - interested in these issues. And they have to be. If we can - I don't know what we can do to make all the other constituencies in (unintelligible).

And each one in this ICANN corporation understand that if they don't engage in protecting privacy in the context of human rights, then they will be creating problems for many, many use - millions of users - I said of Internet users.
Thank you.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. I would just like to say that I agree with you totally about the translation issue. But please don't hesitate, there are many languages around the table. ((Foreign Language Spoken))

With respect to this issue about trying to, you know, the old expression in English, you can lead a horse to water, but you can't make them drink. We will certainly try to set up a more cohesive law enforcement and privacy panel the next time to get people in the room.

But ICANN has managed to not respond to the data commissioners since 1998. And I think it's been a very good technique. There have been many, many interventions, letters, even opinions of the Article 29 group, which is a committee of the European community, not the Council of Europe.

But it's kind of like water off a duck's back. So I'm not optimistic that we're going to have 500 people in the room. But we'll give it a go and see what we can do.

I know (Kathy)'s in the queue and has a question. With respect to this broader problem of getting basically privacy and human rights embedded into ICANN's procedures and processes. Ironically often the security and stability advisory committee, the SSAC have better reports to lean on than some of the others. SSAC54 and 55, they're asking the same basic questions, what is the purpose of Whois? As the privacy commissioners have been asking for the last 17 years.

So we - the problem is getting the theoretical issues of, and I don't mean theoretical in a sort of meaningless sense of the word. I mean the broader concepts of human rights integrated at the technical level at ICANN. That's a huge challenge.

And the purpose of this meeting today was to bring you up on some of the working groups where we're actually trying to interpret what human rights means in the context of things like the IP address and the protocols. The broader discussion that (Neils) was referring to is definitely happening at the high level in terms of human rights.

And we're then now trying to get it applied at various levels. So okay, over to (Kathy).

(Kathy): Okay if you wanted to - I'm going to change the subject if you wanted to respond. Okay, I'm going to play devil's advocate. The United States, ICANN is a US Corporation. But there are a lot of US companies involved. Data is valuable. And we're collecting it. And we're using it. And it's legal. What's the problem?

Woman: We've only got five minutes left.

Man: Right, okay. So with all you said, nothing is illegal. But I'm afraid that you haven't said a lot of things. So it's how you are processing the data or how you intend to sell it and how you can profit off because to put it very bluntly, I don't think, me as a data subject, have the all or necessary information about all the processes you are doing with my data. This is one thing.

The other thing is that I haven't been given the opportunity to decide in every each of the data processing activities exact sequences because there are a lot of. And what I'm always advocating for is to cut this down and cut it in pieces and see legally what is feasible and what is not feasible, which leads to human rights and which leads not to human rights.

And I'm afraid the US also acknowledged many times the importance of the universal declaration of human rights. And even if they are not part of yet this convention of 108. But there is a huge privacy prudence in the US also, which is evolving.

We can see that I think it's rushing to (a court), which is the new case. It's evolving in the US. You can see to privacy shield. It's something which was unforeseen before. And so there are things which are in change. And the best way for this is dialogue to better understand the two coins of the same coin.

And at the end, what is the best asset of a company nowadays is the credibility and the fairness and the how you call it, the overall ethical vision of the company. It's not anymore like that. And it's includes the respect for human rights, including privacy.

So you will be much - you are getting much more business if you are complying what we are saying, I'm sure.

Woman: Yes, just to compliment. I don't think that from a European perspective we can say it's legal. That's the question of the applicable law and of transporter (unintelligible). And this is clear that under European law there are a number of issues that are of real concern in data protection law. So that's what we need to look at.

(Monica): (Monica) for the record. I just wanted to confirm with (Sophie). Well true, but maybe slightly more direct than (Pieter) was. True, you - ICANN collects the data. ICANN uses the data, sells the data, all is legal. What's the problem?

Well I'm sorry, but that is a problem in more - that is a problem in more than half of the world, I guess. Indeed ICANN is a USA-based corporation. But operates on a global level as it proudly announces everywhere it can. So I think we have to be more assertive in that. This is not legal. This is not okay.

Stephanie Perrin: Stephanie Perrin, I just wanted to add that more than the Europeans have data protection law, according to Grant Greenley's latest article and book, Asian Privacy Law, there's 109 last count. So up here first please.

John Selby: John Selby for the record. We're seeing a huge amount of efforts being put in amongst a wide range of stakeholders here at ICANN to develop and advance Whois policy.

I'll draw people's attention to the transpacific partnership, a recent trade agreement that's being negotiated in Chapter 18 to 19 chapter. And it says at Item 28-1B, countries will have for their CCTLD's online public access to a reliable and accurate database of contact information concerning domain name registrants.

So a policy is being developed outside entirely of this space, instructing what will be done in Whois. And that's a concern. This is the start. There's a number of other agreements coming down the pipeline. And it's likely we'll see more and more of this.

So huge amounts of efforts go on here. And certain stakeholders who are not in this room, consumedly end run around them and get rules put in place which will cascade and nullify a lot of this work. Your thoughts.

Stephanie Perrin: Stephanie Perrin again, and I'm hogging the mic. But I do feel I have to respond to that. The problem with trade treaties is that governments then have to implement them.

They then will have to go home and violate their own data protection laws to put that in place. Now I haven't looked at the precise wording, but if it is as you described, contact information. Contact information can be an email that says abuse at digital discretion.za, in my case.

If they have spelled out cell phone number, legal contact with cell phone number and all of the things that were the recommendations of the data elements in the NWG report, we have a far bigger problem. So do you know what it says?

John Selby: I'm reading it here. It says reliable and accurate database of contact information concerning domain name registrants.

Stephanie Perrin: That's fine because the privacy proxy registration data will be reliable and accurate. It will just not be publically (displayed) to everybody.

Woman: Country codes, they don't necessarily have privacy...

((Crosstalk))

John Selby: And it says reliable and accurate - at the moment in this agreement. Reliable and accurate database of information about the registrant. So it doesn't necessarily say that you can use a proxy service because that would not be reliable and accurate about the registrant.

Stephanie Perrin: No, actually that's one of the purposes of accreditation of privacy proxy services so that we know who the service provider is. And they become the registrant. The person who has hired them to get the domain name becomes the beneficial registrant.

Woman: Okay just a quick response. The time we cut the head of the (hider) off and three heads grew. We have to follow wherever there are negotiating issues that involve domain names. We've got to be there with a multi-stakeholder approach that includes privacy, otherwise we're going to lose, as you pointed out.

(Monica): I just want to - (Monica) for the record - that it's not just Whois. Quite recently electronic frontier foundation also noted the same about UDRP, although we will have a formal review process pending.

But sort of in disagreement it says that this has to be the case it is, and it will stay like this. So it's quite confusing. The moment we balanced UDRP in 1999, which we did, input information for registrants, a much worse version was put into bilateral treaties right away.

(Devan Cain): Yes, (Devan Cain) speaking. The - yes, there have been things for quite a while. But TPP section on Internet governance, I mean it's got several other sections that I think are equally terrible on, you know, copyright and so forth. But particular the section on Internet governance is just dreadful.

It essentially says here are these things that develop by multi-stakeholder models. Let's cherry pick some things we like and then pose them as treaties, which means they're unchangeable, which means that they, you know, should the multi-stakeholder decide as we, you know, may well with Whois the - we went down the wrong path.

But the, you know, this bad - relatively bad policies get, you know, stuck on. And Stephanie, I'm afraid I think you are wrong on the issue about proxy privacy accreditation and so forth because these are CCTLDs. They do not have to follow GNSO policy.

Stephanie Perrin: Yes. Sorry about that, yes. And many of them ban privacy proxy services. So yes...

((Crosstalk))

(Devan Cain): (All my head) there and perhaps, I mean I know the dispute resolution procedure in many of them are different for very good reasons. For example, you know, they may require, you know, their dispute resolution procedure

may be different because it's not entirely about trademarks because they use, you know, business and registration services for the local nation or something, which is perfectly sensible.

It's a terrible idea. But it - more than just being a bunch of terrible ideas, it's implemented in the worst possible way. This is the anti-multi-stakeholder model. It's the, you know, most stakeholders are completely excluded, up to and including elected government officials are not allowed to see the draft text here until it's nearly done.

And the - and to add it's totally top down and, you know, every other thing that's wrong. The one thing I do want to mention here is the initiative by the (FF German Malcolm) of the EFF to identify this issue about essentially turning trade treaties into what we call policy laundry.

You take your bad policies that didn't get up in a, you know, a multi-stakeholder open model. And then you slip them through the back way by this secretive, you know, lobbyist run process.

And, you know, they come out looking good, you say. You know, we spent years in negotiation. Yes, you spent years in negotiation where only, you know, trade ministers - trade ministry and business lobbyists were ever allowed to get anywhere near the process, excluding even all matter of elected government officials.

Stephanie Perrin: I think we have strayed into the area of international global governance. And while it's fascinating and a bit discouraging to those of us who are pouring time into ICANN because you're quite right. But let's maybe get the questions that were at the back.

((Crosstalk))

(Devan Cain): An outcomes process.

Stephanie Perrin: Yes. If you could remember to state your name and come to the microphone please. Maybe if we had a queue at the mic that would help speed things up.

(Hela Fermoda): (Hela Fermoda) from Ethiopia. ICANN is incorporated. And these does not have a compression data protection law, at least comparable to the UN standard, European standard. So can you brief us (unintelligible) this fact to the issues we are discussing right now. Thank you.

Stephanie Perrin: Could you repeat the last half of that (couldage). We got the part that the United States doesn't have comprehensive data protection law. California is actually the best state. But what was your question?

(Hela Fermoda): Okay, the fact that the US doesn't have comprehensive data protection law, at least comparable to the European standard does have an effect to the data protection and privacy issues we are talking about now.

So can you elaborate these issues? Are we this (non-extensive) list law is affecting the ICANN.

Woman: Yes so earlier on we gave the example of data retention, for instance. That's in European law, data protection law, you can only keep the data as long as it's necessary to proxy on the purpose. And then you need to delete the data.

And there is this notion of proportionality in keeping the data. And here it was felt that the data retention obligations are basically in violation of this principle. So that's under European law.

And so in order to sort out this problem, what was said to the registries was you need to request for a waiver of this obligation. But this is not the way to do because I'm just mentioning one aspect of data protection law, but there are a number of other data protection aspects that are of concern.

And the registrants, so if I take French one for instance, subject to French law, has to satisfy and respect that law. But then following some of the obligations put on the registry by the ICANN framework is conflicting with that. So I think it puts them in a difficult situation.

That's really for local - if you look locally. And then there is the question of transported data (fills), which is also in Europe very, very strict. And I'm not speaking about the Council of Europe there. I'm speaking about the EU.

They cannot export data outside EU or adequate countries when it's not really clearly a regulated. So I have to admit, I've not looked at the case of ICANN, if there is any contract that had been signed between them or not. But this is also an issue.

Stephanie Perrin: Yes please.

(Afran): Hi. This is (Afran) for the record, (unintelligible) from access now. And I'm glad to see that this discussion has evolved from the land and paper to the way it is right now.

I just wanted to get the clarity about - because sorry I walked in late, but as you said earlier, the introduction between these stream of work and the human rights - the main human rights discussion that's happening with the GAC. Like are you guys interacting?

Second, about the data retention and data protection, it's good that that was raised about the conflicts about that. And as I mentioned two years - one year ago, almost two years, I would like to see this discussion moved beyond this space because about the data retention, very great provisions about that (ability) conflicts in the African convention on data protection.

Getting those people in this room, the AUC, (unintelligible) and (Alice) to be a good idea to move this discussion beyond that. The original people who are in this discussion right from the beginning. Thank you very much.

Woman: Just a ques - can I actually because earlier (Pieter) mentioned that he Council of Europe is a new organization having both a cybercrime and a data protection instrument. It's not the case because the African Union has a text that covers both aspects.

Except I think the difference between our instruments is that yours is solely for the members of the African Union. Has this text entered (InfoForce) yet?

Man: So far five countries are verified. So we're reaching for 10 more. And then it's being enforced. So as this process goes on, because I mean processes like if the African Administer talks about the Kenyon Bill coming into force, South Africa is in the same (garner). So it's a precedent that's ongoing. And it's good to engage right from the beginning and not come at the end once it does come into force. Thank you.

Woman: Okay thank you. And then about the links between the works in the various four, I think...

((Crosstalk))

Woman: But as I said at the beginning for instance, our work, we're pushing it also in the GAC as observers. But then between communities and (us) I think we'll be able to respond.

(Niels): This is (Niels) for the records. And I can confirm that - the excellent work that's being undertaken by - in the PDP on Whois is being relayed to Sub-Group 5 of the cross-community working party on human rights.

And the work on the cross-community working party on human rights and that is also relayed to the GAC working group on human rights and international law. We even had a joint session yesterday. So I think there is ample coordination and collaboration between all the groups to also bring this forward, not only in the PDP processes, but also in the Work Stream 2.

Stephanie Perrin: Yes, and Stephanie again. I'm afraid we're going to have to cut this off because apparently somebody else is coming into the room and we're already over time.

I do apologize. If you're interested in continuing discussion on how you can contribute to either the HR or the privacy work at the ground level, please come and talk to us. We'll be hanging around outside. But I guess we have to clear the room for everybody else.

So thank you very much for your attention today. It was most appreciated. And we'll follow up for the next meeting. Thank you.

END