ICANN
Transcription ICANN63 Barcelona
GNSO – NCSG – Can formal standards simplify 3rd party access to registration data?
Session 1
Sunday, 21 October 2018 at 13:30 CEST

Note: 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.

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page:
https://gnso.icann.org/en/group-activities/calendar

Stephanie Perrin: Okay I guess well we better get started. Thank you everybody for coming. My name is Stephanie Perrin and I'm with the Noncommercial Stakeholders Group. On my left is Farzeneh Badii, the Chair of the Noncommercial Stakeholders Group. On my right is Milton Mueller same, not the chair, Non-Commercial Stakeholders, Ayden Ferdeline and who will be our moderator for today, Andrew Clement from the University of Toronto Whois the Principal Investigator on the research project that is occasioned this workshop today and beside him (Brenda McPhail) who is invited as part of the research project to present civil society views from Canada.

Just a little word of an introduction from me first. This is a joint production today of the Noncommercial Stakeholders Group and the University of Toronto research project. We're very grateful for the opportunity to come and talk with ICANN folks who have the deep experience obviously of giving access to personal data, personal registrant data on what kinds of issues and difficulties they run into and whether or not standards would be useful. So I think that's enough out of me and I will just ask Andrew to maybe introduce the research project a bit and why the Privacy Commissioner of Canada funded us.

Andrew Clement: (Unintelligible) Stephanie and to all of you for coming to this and I'm especially grateful to Stephanie because I had the pleasure and honor of supervising her doctoral research over the last many years, yes call it last. But it was a very fine piece of work that examined the history of the debates within ICANN over who has access to Whois. And it's - I think it's interesting that it's the 20th anniversary and that anniversary coincides now with the bringing in the among other things the GDPR that – the General Data Protection Regulation in Europe which has in many ways underscored Stephanie's arguments about the importance of bringing access to Whois data in line with data protection requirements and laws particularly here but elsewhere. And we're very interested in that in Canada.

And so this project that we've engaged in - and I should make it clear that this project is in effect led by Stephanie and not myself although I'm the name on it for academic reasons, but is aimed at trying to develop ways in which those who have legitimate access to Whois data can gain that access as an alternative to the current, which I understand is the current regime which is basically that all the data is open which is quite a remarkable thing from the point of view of data protection authorities given that personal information should be under the control of the individual themselves. So it's our attempt to find ways of somewhat balancing the need for access of third-party access. And there certainly are legitimate needs for third-party access to Whois data but and also and respecting the rights of the individual domain holders. And so we really appreciate the opportunity to present some of this work and mainly to consult with those in the ICANN community who are familiar with these issues and to hear from you what are the issues that we can - what we should be taking into consideration. And this will lay the groundwork for the next stage of the project which will be to actually formulate some principles and other bases for the certification of, you know, those who have legitimate access to that data so that it can be get what they need and also respects the data protection requirement. So but this is a very early stage and we very much appreciate you coming and we look forward to hearing what you have

the say and giving us robust advice and hopefully you'll be hearing from us again as we further develop those proposals so thank you. (Unintelligible).

Stephanie Perrin: Thanks very much. And now Farzi would you like to…

Man: Thank you.

Farzeneh Badii: Thank you Stephanie. My name is Farzeneh Badii. And I am the Chair of Non-commercial Stakeholder group for those three days then Stephanie will be the chair. But we are at Noncommercial Stakeholder Group we have a set of values that includes freedom of expression, privacy protection and also human rights in general that we are trying to infuse these values in ICANN policies regarding domain name system.

So it is very important for us that the domain name registrant's data that is existing in Whois is redacted and also accessed by accountable users. So you keep hearing around today and this whole week about access to Whois and how access to personal information of domain name registrants should be provided to legitimate users. But what we are not hearing is how we actually can hold those data users accountable when they have access to sensitive data. So we are not necessarily against granting access but we think that should be accountable. And Stephanie's project starts this conversation which is very important to us and proud to host us. Stephanie, go ahead.

Andrew Clement: We'd like to keep this session today as interactive as possible. So we're going to try to keep presentations and interventions as short as we can. And at any time if you'd like to ask a question please raise your hand and when appropriate we'll come to you. But aside from that I think we can begin with the next item on our agenda which is with you Stephanie.

Stephanie Perrin: Thanks very much. I would also just like to introduce Maryam Bakoshi who is supporting us down at that end of the table. And Mariam if you could give me

a nudge if there are questions online because of course people are following this remotely. So it's a little hard to multitask and keep an eye on everybody particularly because I'm going to be pulling up my slides. So could we put my slides up there, said she hopefully.

In the meantime I'll talk just a little bit. This is a very small research project. It's certainly not bundles of money. The Office of the Privacy Commissioner of Canada has a Grants and Contributions program maxing at I believe half $1 million at the moment and research institutes and civil society, other actors put in bids for small amounts of money to study particular topics that are on the privacy commissions agenda. Now I can't say that standards was on his agenda this year but there is the problem of third-party access to subscriber data is fairly well-known. We hear most about it in the arguments over access to ISP data usually.

Whois is a less well-known problem out there. I know it's a big topic here but not so much in the real world. But that is the reason that I think they've shown interest in this topic and so have the Berlin group. That is the group of data commissioners that study telecommunication and IT issues. So do I push the slides or do you? So next slide please. Oh wonderful thank you. Watch me mess this up. There we are.

So basically I have gone over Item 1 which is the UT research proposal. We had originally suggested that we study first Whois and then ISP data. This is in the Canadian context so if you look at our background documents you'll see a lot about Canada. It is well-known it's a global problem though so it's just that this is a Canadian Commissioner, it has that Canadian content. But unfortunately we don't have enough money to do the ISPs this year so that will be next year. Should this be successful next year we will apply again if there's interest. If nobody wants than the - we're not going to continue doing the academic routine of developing something nobody wants.

The next item would be the framework in the GDPR, just a couple of words about that, the existing data protection and security standards in the ISO stream and that what questions do we need to be thinking about as we go through the day? So I think I've covered the University of Toronto proposal. And these are the outputs that will be coming soon. There will be should be a Web site up shortly, a bibliography of relevant standards work and any risk analysis that we can find, further consultation with the standards bodies. That will be as soon as we have the results of this workshop and we show whether there's interest or not. Standards bodies for those who are not aware of how they operate they are funded by the participants basically. So if organizations are interested then they participate and bring the funding. If there's no interest, there's no standard. Elliot is here. Did you want to stay a few words at some point Elliot or not? Okay think about it. Let me know if you do okay?

Man: He's so shy.

Stephanie Perrin: I know he's usually very shy and I'm sorry to focus on it. Okay so we will be talking to the standard folks. There's quite a few standards out there already so I don't, I'm not convinced at this point that we need development but that's for discussion. And then there will be a summary report in spring of 2018. And Ayden I'm counting on you to give me the nudge if I'm talking too long, something's not moving. Okay there we are, whoops. Now it's moving.

Framework within the GDPR for standards is Article 43. And I'm not going to read you the whole thing but basically they GDPR contained specification for standards. The data protection commissioners that are organized first in the Article 29 working party and then later in the European Data Protection Board, as soon as the GDPR passed they became the European Data Protection Board. They wanted to participate in the standards process. And in fact they have written to ISO asking them to make public ISO 17065 which is a management standard because standards cost a lot of money and the privacy commissioners would like to see that distributed. I don't see a

response yet. I will be checking to see whether the ISO's going to give it away but I doubt it.

So basically this - the reasons why the data protection supervisors want the standards is basically how on Earth would they manage to do oversight of all organizations and wants for data breach? They can't. So they're looking for industry standards to come up to levels that they can recognize. There are of course attendant issues that come along with that. The DPAs are looking for assurance of privacy management practices are being met. They want predictable security standards that are recognized by industry as being appropriate. They want assurance of identity management. And that means if I send in a request to access Joe Blow's data how do they know who I am? How do they know whether I am as authenticated as an individual that has the right to get that data? Say I'm working for a security company or the police.

So that kind of - that's what I mean by identity management. There's a whole certification process there. And they want freedom from pressure to audit practices on a regular basis. They need to offload some of that and therefore standards is a way of doing that and to do enforcement without constant intervention.

There are questions ensuing out of this certification process in terms of liability. So if you are a data controller and you rely on a data processor who has been certified as meeting certain standards, management standards, and has been accredited what happens when something goes wrong? Who's liable? Is it the inspector or the auditor? Is it the in other words a certifier or is it the company, the first company and second company? That's - these are questions that will doubtless be sorted out in time.

There we are. Now in terms of what privacy standards exist, I am leaning very heavily on the work of (Kai Randenberg) who teaches at (Goethe-Institute) in Frankfurt and who has been the convener of some of these

standards under ISO JTC1. So ISO JTC1 one is - that's the Joint Technical Committee where most of this work takes place. And SC 27 is the IT group that has done most of it in Working Group 1 and 5, mostly five. So these are in the identity management and privacy technologies stream.

And that link at the bottom is to really quite a comprehensive presentation that (Kia) made to (Similac) back in the fall. So it's a reasonably up to date. Sadly we are competing in this ICANN meeting with the biggest privacy conference of the year which is in Brussels. And it is the big launch, a GDPR one. So I was - I had a hard time getting anybody to come from the community to this workshop. But we will be I think hearing from some of the data protection authorities and the folks that have been working on standards later during the life of this research project. But that's a pretty interesting link. And I knew this would happen. I stole one of his slides which gives a very high level outline. And I don't have time to go in all of them but it maps out the particular ISO standards that are relevant. And if you can read it's – there's the general framework standards at the top. And the largest section in the middle is the management standards. And there is one for the privacy impact assessment and one, a more general one for privacy management. Then there's a new one 27002 that is coming from Working Group 1 on privacy management. And raise your hand if you're finding this a little too thick with the standards. If you're not – you - yes. Oh I'm sorry.

I'll be brief then I move on. But I've included on the next slide a further reading. So you can go to the (DIN) Web site and download the freely available standards and a list of the relevant standards. We will be putting all of this up on our Web site as soon as he gets going so and the possible applications of the different standards because each one does a different thing. Now I think that's enough for me. I'm probably over time.

Ayden Ferdeline: You actually, this is Ayden. You're actually not out of time Stephanie. We're ahead of schedule.

Stephanie Perrin: I'm proud of myself.

Ayden Ferdeline: So we have more time for questions.

Stephanie Perrin: Wonderful.

Ayden Ferdeline: I'll just note initially if you were struggling to see the slide before it is an Adobe Connect so you're able to download the slide deck into you know, to zoom in.

Stephanie Perrin: Right.

Ayden Ferdeline: And with that said were there any questions for Stephanie regarding why privacy standards exists, why they might be the solution to some of the…

((Crosstalk))

Stephanie Perrin: Or I'd be happy to talk about some of these standards in more detail but that will probably put some people to sleep right after lunch. I mean basically you're looking at standards for accreditation, what does it take to accredit someone. There are standards for the management practices obviously. So if you are certified to an ISO management standard then you are meeting that standard of management practices. And that is really particularly relevant with privacy because there's so many things you have to do -- retention schedules, records management -- you know, all of those things. Yes?

Collin Kurre: Hi there, Collin Kurre and for the record. I'm actually not very familiar with ISO standards or their development. But my question would be - so that's some homework for me. But my question would be is there kind of any, is there any type of historic articulation between ICANN and ISO standards? Like has there been any kind of feedback in the past or are we trying to kind of have a new level of not coordination but kind of interactions between these different standard setting bodies?

Stephanie Perrin: I certainly don't think they've done anything in the data protection area. I mean there might be ISO standards. No? Elliot's shaking his head. Apparently not which is shocking in anyways because for those who are familiar with say government security I mean we rely on ISO standards for a lot of that security management.

Collin Kurre: Didn't know I (Unintelligible). Hi, it just another clarification question. So if the ISO is involved in setting security standards there is – are you saying that there hasn't been - really I don't know if there's somebody from SSAC here, if there hasn't been any kind of articulation between those two standard-setting bodies, SSAC and ISO?

Stephanie Perrin: There will be people from SSAC here. A lot of the SSAC people participate at the IETF. And I didn't talk about IETF or IEEE but this whole concept of privacy by design has struck a chord with many of the standard-setting bodies. So IEEE I'm sitting on a standard-setting exercise there where they're trying to deal with things like talking Barbie's, you know, these communicating yes that's a real problem. ISO I believe has one of those standards at the bottom of that long fine print chart deals with wireless devices.

Collin Kurre: Yes.

Stephanie Perrin: So but I don't think they've hit the talking toys yet but no, their arrival standards groups and they sometimes there will be two standards going in different groups at the same time. But I don't see ICANN playing. If anybody has anything to add on that I'm happy to hear it.

Ayden Ferdeline: So we have a small queue forming. Milton did you have a questions? No, then Elliot please.

Martin Mueller: Yes hi thanks. You know, I think that I want to tie two points together. You know, it's my understanding that under the GDPR this concept of accredited

bodies is a little bit narrower than we can use for our purposes. It's very specific. But I find both that and ISO standards to be something that we can use as persuasive but not conclusive. And I, you know, I really would encourage the community not to look at those as full solutions but as, you know, things that have, you know, elements that can be extremely useful. You know, for better or worse I believe when it comes to dealing with tiered access and dealing with all accreditation issues we're kind of stuck on our own out on a bit of an island. And I think that it's important, you know, whether we're talking about ISO or whether we're talking about IETF that we remember that the I stands for international and that this is global and those are fundamentally different creatures. Again that doesn't mean that they're, you know, completely at odds with each other but it does mean that they have different considerations and different stakeholders. And so, you know, I really want us to be recognizing explicitly that, you know, we can use those just as persuasive or suggestive. You know we're kind of, you know, what we do here, you know, I won't even say, you know, for better or worse because I think it's, you know harder, you know, we're going to have to be doing on our own.

Stephanie Perrin: (Unintelligible).

Ayden Ferdeline: There was one question in the chat room, Steve DelBianco who was just asking if there was in NCSG position on the proposed RDAP profile. I'm not sure if you want to take that now or maybe we can…

Stephanie Perrin: Okay.

Farzeneh Badii: Farzeneh Badii speaking. In response to Steve this is, we are only hosting the session. This is our about a project that Stephanie has and NCSG does not at the moment - has not formulated any kind of position that talks about accreditation or access. We are not talking about NCSG position here. We just thought that you should start the conversation and then later on when we go to ICANN policy and we are trying to talk about access later on then we

can see whether we can use some of the results of the discussions that are happening around the community in that (Unintelligible).

Stephanie Perrin: I think - this is Stephanie for the record. I think Steve was inquiring about our position on RDAP though. And we do have a comment ready at the table do we not?

Farzeneh Badii: Yes. On RDAP we do have a position but this is just I'm just making it clear that this is not the session to talk about NCSG. We want to talk about what you are doing Stephanie and the standards (Unintelligible). And so but Steve I can tell you what our position is for sure later and we have a public comment that you can - wait, yes thank you.

Ayden Ferdeline: So and Milton please?

Martin Mueller: So building on Elliot's comment can you specify the relevance of these particular standards to the ongoing Whois process? For example the issue of accreditation as I understand it is something that relates to having a - an access system in which if you are accredited in a certain way you get access to certain kinds of information. Some of these ISO standards that you're talking about and these are much more general standards dealing with security and privacy. So how do they relate to what we're doing here?

Stephanie Perrin: In terms of accreditation we are going to have to follow some protocols as to who we allow to have access to, for instance cybercrime researcher, cybercrime professionals. What do you have to know before you are considered to be a cybercrime recipient of data? What to do diligence does the organization that you work for have to go through before your accredited? And there is a accreditation standard that talks about process there in terms of what you have to go through. You would also have to meet the management standards in that organization before the data would be transferred to you. So right now we have cybercrime researchers sitting in pods in companies. You know, Elliot's probably got one in his company. Mark

(Unintelligible)– in fact I'm going to slaughter your name Mark is going to talk about what Microsoft does.

All of these pods need to meet certain standards so that I can could say yes that's of bona fide person engaged in cybercrime and not a member of a mob that is doing identity theft. And don't laugh, it's happened. And so that's what we're looking for that kind of accountability. And it shouldn't be a problem for a bona fide operations and the other ones don't show up at ICANN so we're good. Does that answer your question?

Martin Mueller: In particular how would it to relate to the board's proposal even though they don't want to call it a proposal to make GAC responsible for certain aspects of accreditation?

Stephanie Perrin: Stephanie Perrin for the record. Do you really want me to answer that? Well I would love to see GAC have to be accredited in terms of the process that they're going through to designate people that would be recipients of data and I'd love to see the management practices as to how they're managing. And this – I'm a former government bureaucrat myself and I know how bad things could be in government so I'd like to see them meet the kind of security standards that we're looking for here. So but I don't think that's what ICANN is proposing in terms of its model. We haven't heard anything about that. I could be - stand to be corrected.

Man: Yes sorry my - just to clarify and so my understanding is as much is you, as the registers like Elliot will say if you – if I receive a request I want you to answer all these questions to make sure it's a fully legal request. Now normally one of the ways this often works with securities issues -- and there's a lot of security things as you say -- you know in industry you would tend to say, well are you ISO 27,001 certified? You are good, security is good. We don't need to know the details but you're, you know, that's the standard and you're investigating whether we have a, basically a standard that answers the other questions that registrars and so on would ask and say okay are you –

have you got a process to show that you are - ask that the purpose you are asking that the data is valid that it is appropriately directed and all these other things. And you, you know, your company or your whatever would say yes I have met the certification so I'm easily able to answer these requests in a standardized, you know, I'm able to certify in a standardized way that yes a registrant can give me the data or not, have to get it in detail of that exactly.

Stephanie Perrin: Right. Ideally Stephanie Perrin for the record. You know, you cite 27,001 and that that 27,002 is the privacy management standard that would hopefully be the one you would say for the privacy management practices, because right now you'd have to go in there, read their policies if they have any check, you know, it's a big job. It's a big job, so once you certify not such a big job.

Man: Well I'd clarify that that, how we would (Unintelligible) this thing.

(Leslie): This is (Leslie) from Tucows. So for most of these ISO standards as I understand it as sort of a self-certification and so anyone can say why yes I am ISO 28,640 certified without actually having to prove that. And that's a concern for me. If we have a standard that's great. At least I can say are you ISO XYZ certified? But I would prefer more than just a self-certification just because I know how that works.

Stephanie Perrin: Yes Stephanie Perrin for the record. One of the reasons that in Canada we developed a privacy standard with the CSA that was accepted as a quality management ISO quality series 9000, so we have a quality management standard which you can then register and have it certified by an independent ISO auditor and a few Canadian companies have done that. We thought it was the answer to the international problem where, you know, we did this in the 90s when the United States was refusing to pass a data protection law and the Europeans were going ahead.

We're now 30 years later and we still have an impasse there. So I'm not working in government anymore but I still think it's a great idea because if you

like self-certification has limits and we're going to find out what those limits are in this discussion of liability that I touched on earlier because you're going to have to have agreements under GDPR approaching liability. If you're relying on a self-certification to 27001 or 2, you know, how are you going to figure out the liability there?

(Leslie): I just want to say that there are very good reasons for self-certification that I'm not against certification across the board, just there are some concerns. Thank you.

Ayden Ferdeline: Just doing a time check I think we should move on to the next item on our agenda now.

Stephanie Perrin: Okay.

Ayden Ferdeline: But we will have opportunities later to revisit some of these conversations. So next up we had Theo who's going to be discussing the problems the registrars face when dealing with requests or access to registrant data.

Theo Geurts: Thank you Ayden. My name is Theo Geurts. I'm a real-time registrar or registrar in the Netherlands. We started out in 1999 with the ccTLDs and in 2004 we became ICANN accredited and we currently have like 2-1/2 million domain names on our platform. When Stephanie asked me to speak to you today I was wondering what I was going to say here because I'm going to put the question forward here how big is the problem when it comes to the amount of requests because when I was thinking about I was going back to 2011 one of the first ccTLDs announced that they were going to redact personal data. In fact they we're going not direct - not redact it, they were going to remove the data. So every time there was a Whois query it wouldn't return any personal data.

And we were a little bit worried back then. I mean in 2011 we had somewhat of a similar debate like we have now within ICANN, not on the huge level as it

is within ICANN but still we had concerns and I remember the day clearly that the first day the registry started to no longer display the data we had extra support people to make sure that we could handle the massive amount of requests that we'd be - would be getting. It happened, I sent back the support people two hours later because the phone didn't ring, no emails came in. It was quick a time. There was not much going on.

So over the years we've seen the process of CT ccTLD operators starting to no longer display the personal data notice. I've seen it a couple of times. I mean it's a repeated process and every time the result was the same -- very, very limited requests came in.

So back in April this year we started to redact the Whois for the gTLDs, same result, not much happened barely any request. Up till this day minus a certain requester we got like seven requests till now. So we like 150 days in now with a redacted Whois and I got like seven requests which is sort of following the trend and the results from the geo TLD group which was released earlier last week.

The geo TLD like .Berlin, .Paris they've been monitoring the requests since the 25th of May. And what these people have been observing on a registry level was they got like 50 requests till October 4 and 25 of them were legitimate. So again how big is the problem?

Also when we are looking at the ccTLD level one can observe that registries themselves set up partnership with companies like NetCraft to monitoring abusive domain names. And these ccTLDs have evolved into very effective program to detect abuse on a ccTLD level. I mean the uptime is for abuse domains is very low because these registries have managed to make sure that everybody is very, very responsive.

So when we look at abuse levels in Europe for Europeans ccTLDs the uptime is low for abuse because all the actors involved know what to do. When the

requests come in we already know it's a trusted requester. So we basically don't have to figure out anything ourselves.

So as a registrar and especially being a wholesale registrar when it comes to requests from third-party actors we can't do much with the requests at all because our resellers deem us as the data control, data processor and themselves as a data controller. As such we have all these data processing agreements in place and basically I can't do anything with the data the resellers provider us except to register a domain name. So as there are requests coming in I am contractually obliged to tell the requester please go to our reseller, fix the problem there. We can't give you the data because that would be in violation of the data processing agreement we have under the GDPR with the data controller.

If I'm looking at domain name disputes when it comes to trademarks of course over the years in Europe we already have a large experience with those issues when it comes to trademarks. And basically that process is still being executed today with the gTLDs. I mean as – so as a UDRP, we look at the request, who is the plaintiff? We do a little bit more of a - at least I'm doing it I'm documenting who the requester is or the plaintiff in this case, how old are the trademarks? I want to make sure that everything is not fishy or anything, that we are not to disclose any data on accident due to a trademark holder who basically wants to get a data for whatever purpose they have. So we do a little bit more due diligence than in the past. But still when I'm looking at the UDRP levels at the moment they reflect the same numbers as last year. So I think when we are looking at trademarks issues, life goes on, it's not much of a problem.

When I look at compliance we of course we're getting requests from ICANN compliance when there is a complaint. So far the process is we haven't had a set process so we are still trying to figure out on a case by case basis how much data are we going to give ICANN compliance. Redacting a lot of information goes a long way. I must say that dealing with ICANN compliance

it is a very copacetic engagement. And from that far - point of view I do not have any complaints.

We still need to learn and basically we still need to get further into the details and get more standard processes there because currently we are winging it and you want to have a set process. I don't think I'm going to give you a lot of time back because that is basically what I wanted to tell you people here in the room about my experience so far with third-party requesters. Thank you.

Ayden Ferdeline: Thank you very much for that Theo. Were there any questions for Theo and Collin, go ahead please.

Collin Kurre: Hi there. Thank you for the presentation. So you mentioned that you that internal you guys have been implementing more measures of due diligence in processing third-party requests. I wonder if those steps had been institutionalized yet within your organization? And then I wonder if there had been any kind of convergence across either registrars or registrars and registries to develop some sort of well standards for lack of a better word, for due diligence and processing third-party requests?

Theo Geurts: That's a lot of questions. When I look at my internal process when you are dealing with the GDPR you have to document a lot. So basically when we get these requests in I'm documenting them and I don't have a set process for it yet. I think we're still trying to figure that one out but I again under the GDPR you have to document everything and anything because at some point you have to demonstrate compliance at some level. We don't know what that level's going to be. We never had an audit by the data protection authority yet. It will come.

So we don't know actually how that's going to work. But basically I think if you start documenting the requests and how you handle the requests, what steps were involved, I think you're good way and good spot on demonstrating compliance on the GDPR.

Now the later part of your question about registrars and registries setting up standards I'm of course within the Registry Stakeholder Group we are looking at it and we are trying to develop something. We are not very far with it though I think that Elliot or maybe (Reg) can talk a little bit more about it because Tucows has been providing us the registrars with how they do it. I think Elliot did a session in Panama also explaining a couple of things that Tucows is doing which is of course very handy for the rest of the registrar community.

Elliot Noss: Yes I think that I sadly want to pop up a level on that because, you know, Theo talked about lack of volume and that is very much what we're seeing again outside of (Optitext) acting on or reporting to act on behalf of Facebook. We're seeing extremely low volume. And, you know, I wish there were some more members of the IP community here for this dialogue. And, you know, and I'm sympathetic to excellent and I'm sympathetic to - I said more so - and, you know…

((Crosstalk))

Elliot Noss: Yes and I'm sympathetic very much so to the, you know, the lack of standardization. But we're not, you know, the bad news at this point is, you know, we're falling I think certainly in terms of the policy process in terms of what we've been talking about at ICANN meetings going back to Copenhagen. So, you know, what is it four meetings and five meetings and, you know, we're still talking, you know, sort of at each other about, you know, the right to access as opposed to dealing with the work of access. And so, you know, we're seeing low complaint volumes, were seeing very, very simple things be a struggle like demonstrating authority to make the request, like, you know, simply providing the allegation, you know, the - around the wrong doing in the domain name.

And I really feel like, you know, until we - and two or three more - I should note that we set a correspondence to date to the ICANN correspondence file that went up this morning in that correspondence is an appendix which, you know, lays out sort of the simple and I really mean first orders simple requirement that we have to provide access. We did, you know, we included that appendix because we want there to be some form of public record at this point so that we can all as a community start iterating on it.

But, you know, I really think that, you know, what we've got to be doing at this point is dealing with that very simple level. You know, so much of what you're talking about Stephanie or, you know, Collin and when you're talking about standards across registrars, you know, we're not dealing with the simplest elements of this yet.

You know, we can get agreement on – and when I say agreement there's not even an intent to agree. There's not even, you know, a debate about things like, you know, what form should reported authority take? You know, what, you know, so much of this is done by third parties and, you know, how do we sort through that. Very, very simple things, what form should the allegation of infringement take?

You know, the – we can't be getting to these more complicated and important issues until we deal with the things at the highest level. And there are - and again, I'm deeply sympathetic to this, there are a lot of registrars at this point that are just not responding or are, you know, sort of dealing with it in a relatively cursory fashion.

You know, we don't like that. We think that, that, you know, we think that, that should not be the case. But there's no, you know, I think we've got a what I – I guess to sort of summarize that point is like we've got to get into the work. You know, we have to move from I don't want to say stop - we have to move from – I'm not going to say stop. We have to move from, you know, third parties have valid rights. You know, registrants have valid rights to getting

into the nuts and bolts of the work if we're really going to be dealing with these issues.

And I think it's very important to know that, you know, I don't know that we have at this point again because volumes are low – and (Reg), you know, please correct me if I'm wrong here, you know, where people or requesters are jumping through these very simple, you know, elements of the request. They're getting the data and they're getting it in a timely fashion.

And so, you know, I think that then, you know, we can move on to things and this was something we discussed last ICANN meeting, you know, to allow the IPC and the law enforcement community who come to these meetings to start communicating those very simple standards out to their relative communities. You know, I think that we're very eager and willing to do that inside of the registrar community. We have to rely on, you know, the IPC to communicate to the IP community and the law enforcement interests that are here to communicate out to the law enforcement community. We can't do that. And we can't be expected to do that. And so again it's an, you know, and urging to kind of get to the work and I'd love to yield to my friend over here.

Stephanie Perrin: If I could just respond to that Elliot you are preaching to the choir. You're looking at a sucker who's sitting on the EPDP. And I must confess we did all the work to put in this standards proposal to the privacy commissioner way back I guess it was January wasn't it? And the EPDP had not started. And I had no idea that we would be just pushing the same wretched rock off the same hill because I was a privacy officer in 1984. I know some people weren't born then. Too bad, you missed it.

But back in 1984 when the privacy act was passed in Canada there was a manual that went with it. And with that there were forms. And you didn't give data to a law enforcement officer unless they filled the forms, showed you the badge, gave the, you know, rank and serve a number and why, you know, within reasonable grounds depending on what kind of criminal activity it was

or what kind of regulatory authority they had what they wanted it for. That's 1984 people and that's a one pager form. And we don't have that here.

I'm not trying to overcomplicate this by coming up with an ISO standard but I'm trying to shoehorn from what's out there in terms of much deeper management practices which would have these forms as part of, you know, as part of the management practices. Anyway that's enough out of me.

Ayden Ferdeline: Thanks Stephanie. We have a small queue Mark followed by Alex.

Mark Svancarek: Mark Svancarek from Microsoft. Oh we're allowed to move these microphones?

Stephanie Perrin: I am.

Mark Svancarek: Yes.

Stephanie Perrin: I'm doing…

((Crosstalk))

Mark Svancarek: We were in another meeting where we were not allowed because of the cameras.

Stephanie Perrin: (Unintelligible).

Mark Svancarek: Yes okay.

Man: Apparently not allowed…

Mark Svancarek: Yes some interesting comments on the volumes. I think if you're running a good operation you're going to see lower volumes of requests. Like, you know, if you have good processes and you're blocking obvious infringements

coming in, if you're doing even a tiny amount of verification like, you know, imagine how many times we find someone who's registration is registered to Microsoft Corporation, 1 Microsoft Way 425-882-8080, you know, clearly our identity while any sort of remedial verification would've caught that right?

So if you're running a good shop you're going to see less right? I mean that – I think that is – it makes sense. Another thing though which is interesting we asked our cybercrime guys when you ask for data are you having trouble getting it? And they said, "We can ask for data? We have recourse, really? We thought we were just screwed."

And Theo I don't think the information on how to get data from you is actually even on your Web site. I'm not sure it is. So that is another thing where we really did standardization, say here's how you do it. In the new RDAP protocols we've been talking about having a remarks field where we could put, you know, if data is redacted here's how you request it, have that in a field and that would go a long way towards, you know, unblocking people who don't know how to do it. And I don't know if it will actually change the statistics at all. Again if you have good practices you should see fewer violations.

Ayden Ferdeline: I'll let Theo respond because you were named?

Theo Geurts: That's actually a very good point there Mark. We do not have that on our Web site and up till now I never had the idea to put it up on our Web site because apparently everybody can't find it because I get the most silly requests sometimes which makes me wonder like how on earth did you even get to me because you're not a customer at our – at real-time registrar. You're a customer at your hosting provider which is your – our reseller. You don't pay us money so how do you actually end up with Whois abuse contact?

And of course over the years with many of the, I mean since we are in Europe so accustomed to having several large ccTLD registries no longer publishing that personal information It's sort of, you know, when I look at it

from a law enforcement practice if I see how fast did cops in Poland can make a request to the Dutch police and ended up like an hour later on my desk and it's all vetted and it's all being processed and I'm going like wow, we can actually do it, it can be done.

So yes so from a law enforcement perspective I haven't done that on my Web site but it's a good point. I maybe should point - put it up and put it in a form and see how many requests we actually get through that form. So thank you very much.

Ayden Ferdeline: Alex you're next. Thanks.

Alex Deacon: Thanks, Alex speaking. I like this conversation that's - I think it's a good one to have and I especially like what Elliot said is like if we, you know, we should tackle the easy things first. And, you know, there's a lot of hold low-hanging fruit I think that would really help a lot, everyone registries registrars and those who need access or who would like to be able to request access to data through whatever process.

And actually Mark actually asked the question that I was going to because Theo I also looked at your Web site while you were chatting and I realized there wasn't a way - there was no instructions on how to best request this data. I mean I know enough to do a Whois on Port 43 and I saw your abuse contact and I assume that's where you get most of these. But this may be one of the low-hanging fruit that we could work on at least, you know, is there a standard or is there a Web form or is -- whatever it is -- I don't really care what it is -- where people can request access to this data? And of course it has to be done in a way that is, you know, intelligent and supported, it has all the details that is required to allow you to then analyze it, do the balancing test, make all the determinations that you need to make and then decide whether data could be sent or not.

And so that seems to be one of the many things I think we could do and I think that would be helpful. So I'm glad to hear that Theo is considering adding this to his Web page because that's the startup. Thanks.

Theo Geurts: Thank you Alex and we're definitely going to put it up now. It's in high demand.

((Crosstalk))

Theo Geurts: But we could also put it out in the Whois out like try this. So maybe that's a two track part there. To build up on what Alex just mentioned and it always puzzles me a little bit when I see sometimes a lot of requests coming in, for instance a whole rail - wholesale registrar we don't provide any hosting. So it's somewhat amazing how to when you actually open up the abuse box in the morning when you're getting your coffee and you go like wow, all these complaints and I can't do anything with it because I don't hosting. So all these requests to remove content again basically do not anything with it. And it seems like we have some educational partner also to make sure that we also streamline those kinds of requests.

And going back a little bit to law enforcement my experience is at least with the Dutch police when I find they are having issues with content they don't knock on our doors. They go directly to the hosting company. And that is - that part is twofold in the Netherlands for the Dutch police.

Most of them know that most of the information which is usual for them is with the hosting provider. Usually there's payment records there, IP addresses et cetera, et cetera. Also and we have a code of conduct within the Netherlands for hosting companies. And that code of conduct is adhered by most of the hosting companies into that service providers.

And if there is a legal content like say for terrorism or whatever you can file a complaint so in a really easy fashion with the content provider and you will

have results like within an hour and illegal content like child porn, et cetera, it will be removed within an hour. It goes really, really fast because everybody adheres to the code of conduct and understands that if we want to have - be offering fast Internet, reliable Internet if we want to keep that up we need to be proactive as hosting companies. Thanks.

Ayden Ferdeline: We have a queue of Elliot followed by…

((Crosstalk))

Ayden Ferdeline: Okay we'll pause.

Rick Wilhelm: Yes very briefly on that, Rick Wilhelm. Just very briefly on that point, that's content this is about domain names...

Man: Whois.

Rick Wilhelm: …and Whois. So that we're not in the business - ICANN is not in the business of content, just to draw a really sharp line on that for everybody. Not to say that what hosting companies do or should or should not do but we're about domain names, not about content.

Ayden Ferdeline: Thanks Elliot?

Elliot Noss: Yes I think that, so my original comment I do want to, you know, say briefly, you know, on Rick's, that that is overwhelmingly true or I wish it were true. There are two places where I think we have to recognize that there sort of, you know, slight mitigation of that. The first is that it is still the case that a chunk of what comes in through the queue and has to be processed is about content. And so, you know, that's just, you know, the ugly truth.

And the second is that, you know, I do think we are now moving to a world particularly in this global environment where there are no national standards

or very rarely national standards where and, you know, and that distinction can't quite be as bright a yellow line as it has been in the past. You know, I hate opening that door even a crack but the reality is that, you know, if we want to be good Internet citizens, you know, and given that the Whois has gone dark and that's the reality, the Whois has gone dark, you know, I think that the, you know, I think about it as, you know, when all of the data was public, you know, the permeable membrane could be a lot thicker on this question.

And now that Whois has gone dark in all of this information is not public there is some first order very high level, you know, penetration of that membrane that I think if we're going to be responsible members of the Internet community in this world we, you know, we have to acknowledge does exist. So I don't want to, you know, contravene the religion. I just think there is a reality in it that is different with Whois dark.

And, you know, I'm very, you know, I like, you know, both Alex and Mark, you know, sort of wanting to get to the work here. And I – so I want to be real specific care, you know, we point out a correspondence. It's right now the top link on the ICANN correspondent file so go there quickly before somebody else puts a letter in. There's an appendix, you know, there that you guys can shoot at now.

You know, there is a kind of a, you know, it's all we have publicly know but it's there, it's available, you know, we would love feedback on it. And, you know, the reality is that if we, you know, it could be just the three of us, you know, or the three organizations do real work on that and bless it and get comfortable with it, it will become de facto and important piece of work. So the more eyes on it, the more work on it, the more weight it gets and the greater ability we all get to, you know, kind of sort of join arms, you know, with to deal with people who are being unreasonable in the current context.

Ayden Ferdeline: Thanks Elliot. Were there any reactions or final comments or should we save five minutes and go on to the next agenda item Stephanie?

Stephanie Perrin: I think that's a great idea.

Ayden Ferdeline: Perfect. And next we have (Richard) who will be talking to us about VeriSign's implementation of RDAP.

Rick Wilhelm Very good, I'm Rick Wilhelm on VeriSign and we can flip the slides.

Stephanie Perrin: Perhaps a word for newcomers that RDAP is Registration Data Access Protocol right?

Rick Wilhelm: Very good. And I will attempt to keep the acronyms to a minimum. Feel free to make whatever gestures are necessary to hold me to that. We – here we go. Maybe they can zoom because my vision is terrible, too much time staring at computer screens at all ages in my life of which there are many. There we go, not quite that bad. It's like the big E when we go to the eye doctor.

All right, yes I can read that one the big E. Okay so at a - and you can maybe zoom it down a little bit and you can flip to the next slide. There we go, that's pretty close. And we can flip past this slide. This is a little agenda. I get – oh that was a good one.

Man: (Unintelligible).

Rick Wilhelm: We broke Acrobat. Okay there we go. There we go. Oh meeting, they've given me the clicker, hath no fury.

Okay so VeriSign has been involved in RDAP since before it was called RDAP, Registration Data Access Protocol. We've been our – my colleague Scott Hollenbeck who was originally the presenter for this one so I'm

reasonable facsimile of Scott he authored a bunch, authored or co-authored a bunch of RFCs. I don't have the numbers memorized although someone in this room probably does that they describe RDAP.

And RDAP is a replacement for Whois. And it's design because Whois never really had solid standards around it with a lot of interoperability. RDAP in and of itself takes and replaces Whois with that – with a technology stack that is – uses HTTPS as - which is sort of the - one of the core protocols of the Web and is – has its form its responses provided back in JSON.

And what that is, is a format that is much more standardized and parsable by modern software whereas Whois is much more free-form and on text based lines. We're not going to go into the details of RDAP here in this. This is just more a little bit about our pilot and such.

Just a quick plug before we get too far into this, there's a discussion tomorrow 10:30 in the morning so your coffee will have soaked in by then, 10:30 to Noon understanding RDAP and its role it can play in RDDS policy. And it's a panel style so hopefully it will be pretty engaging. The fabulous (Marcus V.) is going to be on that panel so that'll guarantee to make it be a good draw.

And yes the cape, we might get the hat and maybe even the magic wand. We're hopeful for that. So that should be good. And that'll kind of cover a bunch of things there.

So VeriSign has been running a pilot -- you can read the slides -- since back in 2015. We'll talk a little bit more about this. We cover a bunch of the TLDs that we operate in here, .cc, .tv, com, net and also .career. And we include a bunch of different features in there because all those TLDs have various different features. So let's see if I can get the clicker to work here.

What's up with that? So if I hit it again that's interesting. So it doesn't like the title slides. Maybe that's a bit of AI that Adobe has put into the Acrobat reader or a hint or maybe my PF has been hacked. Okay.

Woman: Yes.

Rick Wilhelm: So one of the things we're going to talk a little bit about is federated authentication here. So this is something that we've added to the – to think we'll call it experimental feature. And basically what this is, is it leverages single sign-on technology. And there's a diagram in the next slide that we'll show here and we – it uses open ID to establish and communicate between an identity provider and a client. And it's a way that will, it provides a standardized way to gain with a third-party to do a login mechanism between an RDAP client and a RDAP server using a third-party to do the authentication.

So why is this important? This means that if you had a RDAP that you could have a login mechanism at different RDAP and use it at multiple RDAP providers sort of in the same way right now you might have a login at let's say Google. And you can use that to authenticate at multiple places across the web the same way you do you might use your Twitter login and login multiple places. Your Facebook will login that sort of thing.

So it – or what this means is not necessarily that the community might be looking to one of those out for mentioned entities to be doing RDAP authentication and authorization but rather that it would be possible to stand up and operate a separate entity that could do that sort of thing. Some of the terminology here those - anybody that's been involved in identity things it's recognizes some of the terminology here. Identity provider you see that and sometimes capitalized. You see things I think we have relying party up here, you sometimes see that capitalized.

Let me flip to the next slide and in a second here and that we've got an Internet draft at the bottom. You don't really – if you just Google Hollenbeck (Reg X) open ID or whatever search engine is your favorite, Mark you can – you'll be able to pull that out. I'm sure Bing would pull it out very fast, very fast. Other people probably use (.govgo).

Let's see if I can - now we'll see if the picture - here we go, the picture works. Okay nameless faceless RDAP client. So the way that this sort of thing works is the same way that it kind of works when you would use let's say Twitter to sign into another site. So way back at the beginning of time you're registered with an identity provider. And in this case it wouldn't necessarily be one of those things but some sort of an RDAP identity provider.

And you would set up your login password there, some sort of a trusted entity. And then at some point you decide to go to your favorite registrar or reseller or something like that or registry and you say I want to be able to get access to this protected resource. And then what the server says is it would issue a, some sort of a redirect over and this is where it gets into the open ID kind of thing, sends you over to the identity provider, some pop-up window magic happens and you send back, it sends you a window, you type in your credentials. Your credentials do not go to the RDAP server. That's a good thing right as we all know. And then the after the authentication goes forth we don't have the lines on there in the - I wonder if the pointer works?

Any guesses as to which one is the pointer? Maybe the red one. Yes hopefully I won't put out your eye Alex. Yes maybe put on your welding goggles. You do bring welding goggles to ICANN meetings, that's important, always important lots of bright lights here.

So between the RDAP client and the identity provider we don't show the traversal or the password but it does not go through the RDAP server. And then the identity provider sends it back to the relying party, here's what the

client has said you can see and say about here's what kind of claims have been sent back and forth. Any questions about any of this? Yes?

Stephanie Perrin: So this would fully enable synonymous or anonymous querying as long as the identity provider authenticates that individual as being entitled to it, yes, no, because we certainly hear from law enforcement in particular that they need anonymous search capability for certain types of investigations?

Rick Wilhelm: I don't think that it's - so when we get into law enforcement and anonymity and the sort of things that they're looking for this probably is not satisfying that sort of a how many ambiguous pronoun references can I go? The open ID is probably not where they're headed with that sort of thing. Go – Elliot please go ahead.

Elliot Noss: Yes I mean I do believe that it could work here. So think about it like this. You know, and I mean there's dialogue around an element of this. Imagine, you know, for us Stephanie and this is something, you know, I have puts about the FBI and the RCMP now for over ten years. You know, you should authenticate the relevant parties in your jurisdiction. And so, you know, I don't know the chief of police in (Kamloops) is but if the RCMP says they're okay then that's fine with me and I don't need to know them. I'm glad to see (Benedict), you know, has a view on this.

You know, I – from our perspective, you know, there are what would I say trusted parties that in this context we would be delegating, you know, some identity authority two. I think that, that is an exception not a rule. I think that it's likely, you know, it makes a lot of sense to me on its face in some law enforcement contexts and virtually no others. But, you know, I do think it still could accommodate.

Stephanie Perrin: Just before may I contest that I've already talked to (Tor), people are familiar with (Tor) the anonymous browsing to Roger Dingledine who tells me that Ian Goldberg, Dr. Ian Goldberg at University of Waterloo who's a pretty

prominent cryptographer and privacy enhancing technologies designer they have a system for anonymous querying.

I presume -- I'm not a techie -- I presume that would bolt-on on top of this so that they would come in authenticate anonymous but they split that this is the magic of the Ian Goldberg querying system as it splits the query into so many little bits and then reassembles it. I don't know how that would work with RDAP.

Elliot Noss: I'd like to chat with him. That would be a good cup of coffee.

Stephanie Perrin: Yes.

Elliot Noss: Even if it's a bad cup of coffee that would be a good cup of coffee.

Stephanie Perrin: I believe Ian has a paper out and there's a project that folks are working on in Canada on this so…

Man 1: You know there are real cops here right? And I don't mean drinking coffee in the corridor. So Elliot yes you're quite right and there is definitely a problem around authorization and the who gets to have access. But and don't get me wrong that's an almost (fractually) complicated problem. And but that's actually not the problem. It doesn't - so if you say yes okay RCMP gets to decide who has access yes…

Elliot Noss: In Canada, that was contextual.

Man 1: Yes absolutely.

Elliot Noss: Yes.

Man 1: And that's a complicated problem. But that's not the same problem as the on the anonymization problem. And my understanding is that somebody -- and

I'm looking at (Patrick) here who really understands this stuff -- somebody has to know who you are. And that might be but that might be a situation where cops feel happy to trust an authentication provider the point being that they can give provider token and then pass to a registry or registrar so that that access is tokenized. That's my understanding. So Rick is that correct?

Rick Wilhelm: The - and well I should tell you about, the things that I've been having sidebar discussions with law enforcement on are where somebody in law enforcement is authenticating law-enforcement folks and then handing those things, those queries off as authenticating queries with the identity of the querier already stripped.

And so the query comes across that I won't say anonymous but because it still maintains the context of coming from law enforcement but does not and frequently won't even have the – will have some - won't even necessarily have the context but from within law enforcement because it will be from within a big bucket of law enforcement so you don't necessarily know that it's coming from, you know, whatever, you know, specific law enforcement agency right?

Man: I think the general question here is I hear questions about how do the authentication Federation protocol works were in this case open IDs and news. There are others which work slightly different. But the important thing is the role of the identity provider and then the RDAP provider are two different entities okay?

Something that I do not remember which I think you also ask about implicitly is who is taking care of decision of the role of that authenticated entity? Is it the RDAP server or is it the identity provider? And I don't remember and I tried to start to read the RCs and would see a gentleman that seem to know that but just one second. Okay yes, yes. So and that is another thing to look into.

But I think when people say that they would like to have anonymous access and I'm even less a cop than (Benedict) even though I work with him just like most people in this room, there's also a difference between disclosing who you are, what role you have but also that you are querying about a certain object at all might be problematic enough. So the traceability of the fact that there are queries might be bad enough.

So whenever any of you start to have discussion on what real requirements for example law enforcement have and because of that what sensitivity the query logs have in the RDAP server and because of that what requirements are on the provider of the RDAP server like VeriSign in this case you need to really dig into what is really meant by the role, identity, authentication, traceability and not just sort of hand waving and say anonymous. Thank you.

Stephanie Perrin: If I can just respond to (Patrick) -- Stephanie parent for the record -- I'm neither a cop or a geek. And the conversation that I had with Roger and with Ian Goldberg was way back in May. But I think that's the beauty. So you get the token. The token is not associated in time with any of the queries. And then you use the Goldberg fractal dispersion of the query so that you have no way of knowing who's looking for what. Now I don't know how the RDAP server is going to feel about that or treat it but that's basically the technique.

Rick Wilhelm: Go ahead Mark.

Mark Svancarek: Mark Svancarek. I don't think we should get too far into implementation right now. I mean we haven't even decided on what the off method will be let alone the authorization method. So we don't want to get too far ahead of ourselves. In general I dislike anonymization. By that I mean anonymous access. I don't like anonymous access.

So what we have in who is today is some, you know, somebody shows up on a port and gets some stuff right? And in this model somebody somewhere along the chain is going to know who that person is and what sort of rights

they have. And so I think about it in the similar way to we have an IRM system that we sell at Microsoft. We use it very heavily inside the company.

And information, so it's like DRM, Digital Rights Management. This is information rights management. What the distinction is that DRM, the rights are delegated by publisher and IRM the rights are delegated by someone in administrative capability. And so we can assign rights on whatever level of granularity. So a person an organization usually what we do is we create what we call a security group and entry to the security group is moderated. And then when you're in the security group your granted certain rights to certain resources whether that's a folder on a SharePoint site or even an individual document. That's the level of granularity is an individual document. So I wouldn't use the word anonymous but at the level of a security group for instance you might not know what that security group is. As long as you trust where that security group was created you can make it work.

Ayden Ferdeline: There's a small queue forming now. We have Elliot, a gentleman in the back followed by (Reg).

Rick Wilhelm: So I want to resist Mark's urging not to get into implementation because we don't get to talk about it enough and I think (Patrick) raised two, you know, important points that I want to just put into the room just so we can start, you know, shooting with live bullets here. You know, (Patrick) said, you know, as a point, you know, and I don't know who the RDAPs over here, you know, is.

And I think here, you know, from our perspective as a, you know, registrar with, you know, tens of millions of customer relationships, you know, we under GDPR we think that we're the RDAP server. And so, you know, I do think that, that is the right implementation frame.

And then, you know, forget I think it was Rick who said who was talking about, you know, the well sometimes law enforcement doesn't, you know, want to disclose what they're looking for. And I think there that's a great

example of where again we have to start getting down to implementation. And, you know, there I would distinguish between, you know, this is a matter of life and limb, you know, this is a serious criminal matter or this is a commercial matter because a significant portion of our law enforcement queries are about commercial matters.

Yes they are commercial matters that under statute, you know, are law so one can say they're breaking the law. But they should have a different weight in this context, you know, between matters of life and limb because that allows that, you know, that as a party responsible for privacy, you know, we would place a different weight on those two matters.

And we would want to know that we were speak, you know, have the ability to sort through them. None of this by the way is what we - I shouldn't say none of this is what we want to be doing but sadly, you know, this is, you know, kind of the world we're living in. And so, you know, these are exactly the specifics that I'd love us to be getting to sooner rather than later. Thanks.

(Michele Camaroff): Thank you very much. My name is (Michele Camaroff) and I (Unintelligible) from Moscow from Russia from (Unintelligible) University has core economics and quite interested in this topic. And I just wanted to pull in several let's say issues. First of all we are talking about not jus, you know, registrars but actually more or less different companies dealing with the personal data right? And so we should think about some unified approaches to let's say privacy protection.

And second, I really like, you know, the idea which was proposed here about federated authentication an idea of those information rights management system which was proposed by Microsoft because we are talking about anyway users or, you know, human beings, let's say civil rights granting access to particular personal data to let's say (Unintelligible) or I don't know, a (Unintelligible) server or federal tax service whatever right, so one database right?

And then we are talking about third parties either getting let's say permission to get a pointer to a particular types of personal data like, you know, names, your name what you have for e-commerce for instance right? And the question is that we're interested in what, in protecting, you know, some third parties. We're interested in knowing who actually got access and when to particular types of personal data or be interested in fully automated mechanism when we have, you know, user granting access to, you know, and feeling let's say initial database of future personal data and then just picking, you know, which types of data could be shared with e-commerce or with particular, you know, companies or not.

So I mean this is an extremely, an interesting in extremely up to date topic which should be discussed more or less on implementation level because we don't have time waiting few more years when actually, you know, we will think about our kids and their data being stored somewhere right? So that's yes thank you.

Ayden Ferdeline: Thanks for your comments. Next in the queue we have (Reg) followed by Alex and then we might check in to see if there are any more slides that need to be presented. Thanks.

(Reg): So this is entirely possibly something that we need to take off-line but I want to know more about the IRM because I think that that's a pretty excellent idea and way of framing this. But it seems to me that since with DRM the rights holder gets to decide who has access to their rights. Then similarly with IRM, the rights holder the person or entity whose information it is would have that right. But again this is probably far afield from where we are right now.

Man: I'm happy to go after at the end of Rick's presentation. That's fine.

Rick Wilhelm: Okay thank you. The one thing I will say just to kind of wrap this apparently very rich slide up is that this is, this model here was not really a specially

targeted towards law enforcement type access but more targeted to other types of appropriate access. The other thing around this is that the - in the RDAP pilot working group we're very much and even these days more strongly now that the EPDP Working Group is getting going we're walking around wearing T-shirts that say mechanism not policy.

And so we're very strongly focusing on not doing – where implementation capability and the policy that the – we're all about the how and not about the what to say it a third different way. So let me kind of keep going. We have a hard stop at quarter past, is that correct? And our hard stops here, our hard stops in Barcelona I believe right?

Okay so this is a list of the federated authentication. This is all open source stuff. You can - you'll be able to see these in the slides and whatnot. So this is some - an experimental feature that we're working on called - which we call object tagging. The name is – might be a bit confusing. Here's sort of a little bit more explanation about what it means. When we say entity handles that's a synonym for contact objects as opposed to hosts or domains.

And here is the challenge, when we say query bootstrapping what that means is that if you have an object hand – if you have a contact ID and you just get hold of it and without any contact, without any context on the contact handle you don't know from whence it came. And so therefore you don't know where to go query to find more data about it. If you get a domain name right like benedict.com you know what registry to go hit to -- as he walked out of the room -- that - if that was all it took wow, got to remember, note to self, right?

I like (Benedict). Is he – since this is on the record. The – so you know when you get that domain name where to go query about that right? Similarly with a host object you know where to go query about it. If you're just get a contact ID you don't know where to go. So this contact taking entity is we've written an object, we've written an idea about this. When I say we have course that

means Scott Hollenbeck and you can see the URL there about how to do this tagging. And it's really just a naming convention right?

You register the suffixes with IANA, you adopt it as convention and away you go. Therefore you can – any time you get a hold of one of these contact IDs in the wild you know where you'd go to do it. You could register dash RTR and then you'd know to go find it at Theo's place -- that sort of a thing. I'm not trying to get you to leave so you can stay.

Okay and here's – we've got another experimental feature here around regular expression search. Basic regular basic expression, basic searching in RDAP is not very good. That's very much a purpose right? Right now basic search is only asterisk based batching the trailing characters. That's very much on purpose so as to not put implementation burden on the implementers because searching is anybody who's done searching knows gets very complicated very quickly. You could even make a business off of search or so I've read.

We've done work in CC and TV. These are two ccTLDs for which VeriSign is the registry operator. They are both thin domains and TLDs. And we've done the core RDAP for those. You can read the – I'm going to go a little bit faster so we can get to some Q&A before we go. We've done that.

Clicking, this must be another – oh this is a brilliant user interface design. Only Alex can appreciate it here. Can you ooh and ah for me? It's just the rest of you will have to wait until the slides are posted. We paid the engineers literally three or four cans of Diet Coke to be able to develop this. Then we've got – we did a RDAP pilot for common net. It's a thin TLD. We did core things there.

(Unintelligible) you can see that. Let's see we did .career. This is a thick TLD. We also did object tagging. We did also the federated client identification here. And we did and integration. I'm not going to have – be able to – we did

integration using (Viaginy) for that - the UI won't work. So we did implement the federated authentication using the open ID with a little blue diagram and stuff. That worked great thanks to (Mark Blanchette) up in (Viaginy).

We captured data on our - and captured and published data on our gTLD domain volume. Our – this graph if you can't see it very easily it just starts in October 2017. This current data capture goes up through May 2018. I didn't bother to recapture the graph. The ramp that you see that's total domain queries. And then we've got name server and entity queries.

The ramp that you see in January through early May corresponds exactly through the spring term at a particular university. Somebody found us and did a project banging against our server which was kind of interesting which we were very happy for the traffic because it kept us honest. And it kept the team that I had – that we had developing the prototype it kept them very responsible and made sure because they couldn't ever say that no one is using us. So it was actually really good because it did help make them feel like they were providing a service.

See, okay a couple of quick observations here and then we'll have a few minutes for questions. Protocol test suites, (Mark Blanchette) of (Viaginy) is working on a protocol test suite. This is really helpful. You can see the GitHub URL there. This works for anybody that's working on - in RDAP so that's very positive. The core features of RDAP are working well and we've been working on adding experimental stuff.

I didn't mention it but it deserves mention that we needed to after we got the thing running we needed to do changes after the temporary specification was developed and published. So our – we had like folks in the real world our pilot had to scramble in May in response to the temporary specification. And so we brought ours, our implementation in line with that.

I think there's a little bit – we're going to be doing some open-source work. And then we didn't cover it here very much but with the RDAP also has a referral model where it leverages the 301 capabilities in HTTPS to allow a registry to refer queries down to a registrar and such. And so I think we've got about six minutes left. I know Alex had a question then we can take any others. So…

Alex Deacon: Thanks Rick. Yes I think that's great. And I think it's important work that VeriSign is doing here because, you know, it shows that there's a path forward. I think there's a few comments I wanted to make and I'm glad I wrote them down because I thought about them a lot (Unintelligible). You know, we've talked or you talked a lot about federation. I think the ability to support federation is important.

Users need the ability to use a single credential, an accredited credential if you will across the RDAP servers. But at the same time the servers also need to be able to support credentials from multiple accredited credential issuers. So these are two kind of important concepts of federation that I believe will be required in the future here.

A third piece of technology which was mentioned -- and I won't go into the details here -- is the authorization part which is separate from the authentication and that's important. The draft that you referenced here, the One ID Connect draft I think, profile of Open ID Connect draft by Scott Hollenbeck is really good and I think will solve a lot of issues moving forward. But I will note that the current RDAP profile does not mandate support for this which I understand from the timing-wise timing point of view is probably make sense but I think it's a missed opportunity. So I'm not too sure what the plan is in the RDAP profile group to address that but I think there needs to be we need to be on a path to get that draft approved and properly profiled.

And then I'm glad lastly glad you talked about open source. That is a - that's a key part of this and my - I appreciate that VeriSign is going to be putting

some of this out for people to use. And hopefully we can get some crowd source, you know, according going to make improvements as things move forward. Thanks.

Ayden Ferdeline: So we have time for one more question before our coffee break. Elliot please?

Elliot Noss: I just wanted to Alex's point the two of them maybe have clarification on and maybe it's more asking for clarification on the second. And the first, you know, we as registrars are certainly having discussions about federating authentication, you know, I think it's very efficient to do it. I would deeply understand it, you know, from your side.

And my guess is that at least that or the hope is maybe at least at a volume level if not, you know, by number of registrars that a significant portion of the volume will get captured, you know, as we're rolling out here relatively efficiently and quickly. And, you know, when you were talking about authorization that worried me a bit. So let me tell you the worry and then you tell me if that's what you are trying to say.

You know, I think that no matter what different registrars will have different standards around, you know, what people are entitled to and why I think that's unavoidable just given the range of national laws and the a range of approaches. And so I - were you looking for standardization there or was it something a little different?

Man: Well I'm - the way (Olaf) works again without getting into the detail is that it allows you to convey actual beards about yourself and to things that you want to request and allows requesters to convey details that registrars may need to make their decision. And so we need a standard way of conveying that data and that's part of the authorization token. It's a sign token that says here are the things about me and providing them to you to be able to make your decision and Rick.

Elliot Noss: Yes I've got. So that's input, it's not output.

Man: Yes.

Elliot Noss: Yes completely agree and understand and agree.

Rick Wilhelm: Just let me sharpen that a little bit. A standard way of communicating that which is authorized saying nothing about how that decision gets made.

Man: We if I could restate that as a standard way of communicating what is asked to be authorized which is separate. Okay because it's I guess that's where I'm – I think we all agree so that's great.

Ayden Ferdeline: Great and with that said we are going to pause now. One the recording as to stop because of the length of our meeting we've reached the limit for Adobe Connect. So it's going to – so I'm told apparently. So we have time for a coffee break. We will reconvene in 30 minutes time. And please do come back afterwards we're going to be hearing from Mark as to how Microsoft uses privacy standards. We are going to have the perspectives of a number of security researchers and also civil society perspectives as well. Thanks.

Stephanie Perrin: Thank you so much. That was a great session. You all come back now in a half an hour or even sooner if you like.

END