BEIJING – Next Generation - gTLD Directory Services
Monday, April 08, 2013 – 11:00 to 12:15
ICANN – Beijing, People's Republic of China

Ladies and gentlemen, would you be kind enough to come forward and take your seats so that you can participate in the next program. For those of you in the back of the room, would you please take seats so that there is more quiet? Hello? The children -- the young people in the back of the audience, could you please be seated? We would appreciate it very much. Thank you.

Once again, ladies and gentlemen, please take your seats. We'd like to get this program started. Thank you. All right. We're ready to start our program. The next generation gTLD directory services.

JEAN-FRANCOIS BARIL: Let's get started. Good morning and very warm welcome to the next generation data directory session that we have today. My name is Jean-Francois Baril, and I'm very pleased and I would say even very honored to be the facilitator for this expert working group. This session today should serve basically two main purposes of usually one to update the ICANN community on our progress as a working group. The second one is even more important, and it is to collect your input and insights on critical issues that is we are currently working on. As such, we have built the following agenda for this session. First, a rapid introduction and background on the origin and purpose of this working group. Then a structured dialogue with the community. And then wrapping up and proposing the next step looking forward.

So why are we here today as a working group? If you remember, last October Fadi Chehade announced a very ambitious plan for addressing one of ICANN's most controversial issues but at the same time very strategic, WHOIS. Despite many years of passionate debate, maybe I should say (indiscernible) -- and encouraged or so by the WHOIS review team report, it was recognized that WHOIS could not be easily fixed. Instead Fadi suggested that a fresh and clean slate approach would be much more efficient and effective, especially looking forward to the new -- in the context of the new gTLD and the Internet of tomorrow. ICANN board announced last December the creation of this Expert Working Group with a strategic direction to help redefine the purpose and provision of the gTLD registration data. If we are well articulated, transparent obviously and logical, it is our expectation that GNSO will take our input/output seriously. It is also our expectation that this blueprint will help as a foundation for GNSO to create a new global policy for gTLD directory services.

Now, this EWG incredible team, as you can see we are very packed on the stage. So it's really like a team. We are 15 members, including Steve Crocker and Chris Disspain, also serving as board liaison and in addition we have the chance to have five precious ICANN staff. As you can see, very diverse team coming from business and non-business backgrounds, from the five different continents, strong core technical expertise covering all spectrum of different cases, like IP, trademark, data protection and privacy, law enforcement, and of course registrars and registries. But above all, and at the risk to embarrass their humility, they all come with very strong leadership skills as well.

Our mode of operation, well, we are now basically six weeks in our job and operating via weekly teleconferences and so far three face-to-face meetings, LA, London, and obviously these days Beijing. We have been conducting a comprehensive review of issues surrounding the requirements for gTLD Registration Data Directory Services. But we have also found very relevant to understand various use cases while challenging the current logical flow around these different processes. And always having in mind the strategic questions of what, who, where, how, and when. All of that in the best interest of the overall ICANN community.

Nevertheless, we have to be very humble and admit that despite very intense work and effort, we are still in the exploration, reviewing, challenging phase. But at the same time, I strongly believe that we are coming to a very good and solid common understanding as well.

As Beijing represents a unique opportunity for the EWG to capture the tremendous heart and brain power that exists in this ICANN community, we would like now to invite all of you to a very open dialogue. Even so at this stage direct input will be more useful, we think, to us than just questions. Six of our members here have volunteered to lead six of the most relevant issues that we are currently examining. So now let me make a first disclaimer. Each of the presenters will speak in the name of the overall Expert Working Group and not in their own name. I think this is important also to understand. So for each of the six topics we will have two minutes as an introduction, eight minutes to collect your input. In addition, we have prepared an extra ten minutes for you to have the chance to express your extra thoughts which we will not be able to fit in the above structure. And in case this is not going to be

sufficient, we have also prepared an e-mail address for you to post your input and questions. Now, Chris here, sitting on the floor, has accepted -- almost sitting on the floor, has accepted the difficult challenge to be the moderator but I know very well that he really, really enjoys it. So Chris, the floor is yours.

CHRIS DISSPAIN: Thank you. Thank you, Jean-Francois. Good morning, everyone. Very quickly before we start, I just wanted to do a couple of logistical bits. So the first speaker is going to be Rod, I think, yeah, and it's going to be usage requirements. So he's going to do two minutes. We've got two microphones in the usual places, for those of you who are used to this. Please come to the microphone. We only have a small amount of time. I appreciate that there will be lots of people who want to say things, but if you could keep your comments short, we're really, really interested in your comments and they're going to be addressed as a specific question following Rod's particular presentation. Then we'll move on to the next one, the next one, the next one. We do have a ten-minute timer which will go off at the end of ten minutes, and we would like to try to get through it. Don't forget there's ten minutes at the end to sweep up. So with that, Rod, over to you.

ROD RASMUSSEN: Thank you, Chris. And good morning, everybody. Glad to be here. As Jean-Francois was mentioning earlier, one of the ways we're tackling this very large issue is to look at the problem holistically, take a look from all angles, from everybody who is involved, try and figure out why, when, where, how, et cetera, that people need to get access to domain

registration data, the purpose for it, and understand that from a -- a fairly balanced perspective and have divided the work up into several -- examining several use cases. And this drives usage requirements, which will then drive what we need to develop from both a systemic perspective as well as feeding into potential policy recommendations and policy questions.

So this really just involves going through all the various angles, looking at the uses, identifying the -- you know, kind of the areas where people are doing things today and where we might want to be able to take things tomorrow. And classifying the various people, processes, systems, et cetera, that are using this kind of information and what they're using it for. So that's a very brief introduction as to what we're doing. We have a discussion question around just the whole perspective around collecting, storing, and provisioning of this data. Is this necessary, why is it necessary? And thinking of this from your usage perspective, what are the uses you have for this kind of data and what do you need it for.

CHRIS DISSPAIN: Thanks, Rod. So ten years this has been going on. Wouldn't it just be easier to abandon the whole thing? Do we really need WHOIS, do we need to collect the data and store it? Obviously not. We could probably move on, if that's the case. In fact, why don't we just cancel the whole -- right. Should have known. Ray. Steve, go ahead.

STEVE METALITZ: Thank you. Steve Metalitz, a member of the intellectual property constituency. I want to thank the expert group, first of all, for all the time and effort they are putting into this and I think it's going to make -- I hope it will make a very important contribution to resolving some long-standing problems.

I just wanted to say on this issue of why collection storage and provision of the data is necessary to -- I'm sure you've already heard from among your members about how this is being used in business, how it's being used in order to enforce intellectual property rights, how the data is used for law enforcement purposes, how the data is used for technical purposes as well, but I hope you'll also bear in mind that one of the important aspects of access to this data is for -- to use a phrase that's become very trite within ICANN but I think you will find may have been first used in this context with regard to WHOIS, accountability and transparency. And people who use the Internet, the consumers, the families, the parents, have a real need to know who they are dealing with online. They need to know that for their business transactions, economic transactions, also for how their children use the Internet. So it's important to keep those individual consumers in mind as well as the business uses and the technical uses and so forth. So one question you might ask yourself is, what are the categories of people who shouldn't have access to information about WHOIS registering?

CHRIS DISSPAIN: We're coming to -- that is one of our slides, Steve. So thank you. Ray and then Amadeu.

RAY PLZAK: Thank you, Chris. All kudos and thanks assumed so I'll proceed. Yes, you need to collect it and you need to collect it just from the beginning perspective identifying who is a successful applicant and who the people are that you would need to do business with just to maintain the operation of the gTLD. And you're going to have a section later on storage and provision I'd like to change the thrust of that just slightly in that what the output of this system really is is a series of reports from a database. And so what you're really looking at is how you would shape that. And it starts to allude to some of the things that Steve was talking about. And so that in the end all of the information you collect may not be available to everyone and it may be available in -- in compartmentalized type things, depending upon the nature of the person that is -- needs to access the data. And I'll -- you're going to do that later, but I just wanted to put that out there right now.

CHRIS DISSPAIN: Thanks.

RAY PLZAK: So the why I think is really self-explanatory. And the real question is, what are you going to collect? And whether or not some of that is the things that are later reported can actually be generated by computation or amalgamation.

CHRIS DISSPAIN: Thank you. Amadeu.

AMADEU ABRIL I ABRIL: Okay. Does it work? Hold on. Try again. La, la, la, la.

CHRIS DISSPAIN: Well done.

AMADEU ABRIL I ABRIL: That was my comment. Well, kit couldn't be much farther than that, unfortunately. No, the question is that, from my perspective, recollection of storage or not are the controversial parts. And we may discuss whether facts in the 21st century makes any sense or not. But even if it doesn't, is not controversial, it's not something that we'll raise (indiscernible). I think we'll all agree that quality, high quality registration data, upgrade registration data is necessary to be collected from the registrant, necessary to store that. And even I think most of us agree that should be accessible to at very least some accredited parties. So I think the real challenge is on whether we should grant access to some verified parties or some categories or we should give access to everybody through universal publication. But quite frankly, I would recommend the group not to spend too much energy into collection and storage part because there's some technical issues that should be improved but it's not the crush of the problem here.

CHRIS DISSPAIN: Okay. Thank you. I mean, there are some questions around storage in respect to how you store it and which we're going to come to a bit later on. Ms. Kleiman.

KATHRYN KLEIMAN: I find myself disagreeing with Amadeu. This is troubling. I'm Kathy Kleiman. And I do think we should talk about collection and storage and what we're collecting and why we're collecting it. I went back to some of the old techies years ago and I said why do we have these particular data elements and what data was in there. And they looked at me, it goes back to the NSF net days apparently and this was the business data, MIT, IT, I think I was talking to Scott Bradford at the time, so it was Harvard IT. It was his business office and he was the technical contact for any problems. So I'm truly, truly hoping that you're going to be looking at the data elements, the collection of the data and why. Why we're collecting it, for what purpose. I think all these issues are open to you. I'm glad you're looking at it. I'd like to hear more about what you're thinking on that.

CHRIS DISSPAIN: I'd like to hear more about what you think.

KATHRYN KLEIMAN: Well, I'm concerned about accountability and transparency as the standard for registered data. Because I think of the Internet, the way I used to use it in 1982 when there was no commercial speech online. There was no commercial speech, personal, political. I still do a lot of non-commercial speech as does non-commercial users constituency. And accountability and transparency is not the standard for speech. In fact, many countries protect the rights of minorities, of dissidents. Even of parents and mothers to say things without putting their address on it. Thanks.

CHRIS DISSPAIN: Thanks, Kathy. Ray, you wanted to respond to something Kathy said and then the gentleman over there, we'll come to you in a second.

RAY PLZAK: First of all, I have a question. Are you actually going to have a session -- question on collection itself or is this the --

CHRIS DISSPAIN: Yes, we have a -- yes, we do. Carry on.

RAY PLZAK: Okay. The -- so part of the answer to the collection question is actually involved in what you're going to be reporting in the provision question and that also goes back to requirements that are negotiated in regards to requirements of, for example, law enforcement, being able to get some kind of information, you mean otherwise collect it. Also, the conduct and the operation of the gTLD, for example, and point of contact. Those are requirements that are generated by other things in that system. And so by the pure act of registration you wouldn't necessarily collect that.

CHRIS DISSPAIN: Okay.

RAY PLZAK: So you have to answer those two things together.

CHRIS DISSPAIN: I understand. Sir, if you could just introduce yourself.

RUBENS KUHL: Rubens Kuhl. I have a suggestion for the work group to consider. There is some levels of provisioning of registration data that would be useful for users that such provision could be into the DNS system as well. One example would be -- (buzzer).

CHRIS DISSPAIN: Carry on, sir. Carry on.

RUBENS KUHL: One example would be a user that doesn't want to do business with domains that are hidden on the proxy, under proxy, proxy registration data that such a flag could be published into the DNS so the user's browser could then select, oh, this guy is hidden behind a proxy, this guy is not. So there are some users of provisioning of registration data that could be used in realtime by the users. So we shouldn't not only focus on WHOIS as something to look at and after the fact but something to look at while we are browsing the Internet. That's what I would like you to consider.

CHRIS DISSPAIN: Thank you very much. Thank you. So we're going to move on to the next one now. And who's running that one?

SUSAN KAWAGUCHI: I am, Susan. So we're also looking at the data requirements. Registrant classification was a hot topic. We're looking at the uses of domain names and does that change what people have a right to in the information displayed for a domain name. Some are -- may be entitled to privacy, some may not, depending on how the domain name is used. It's, you know -- we're considering the use of is there a commercial use for a domain name. I think everyone has the right to know who they're doing business with on the Internet, and so it's a natural place to go to -- as one of the checkpoints.

We're also looking at identification of data elements. We've looked at a lot of use cases. Struggled with how data elements currently collected are used and had a very hard discussion of, you know, should all these data elements even be collected? Do we need a registrant admin and technical contact? Some of the -- in a lot of cases those are all duplicate information. We're also looking at data elements not -- not currently displayed. And should this be expanded. I know that's controversial, but we need to look at the whole picture to come to an agreement and a new design for the directory service.

We're also looking -- in looking at those data elements, you know, what should be required, what should be displayed? Those could be two different answers there. So, you know, there's different uses for the info. If it's a technical issue, someone needs to be contacted and it needs to be pretty quick. If it's malware or botnets or consumer protection, free speech, law enforcement, IP, we're considering -- we're trying to consider every element. And every use.

So the question today for you is, should data requirements differ for domain names for commercial versus non-commercial use?

CHRIS DISSPAIN: Thank you, Susan. Elliot, are you standing at the microphone? Unusually?

ELLIOT NOSS: As is Wendy.

CHRIS DISSPAIN: Wendy. So should I have my own personal domain name completely privatized and Facebook obviously would have its domain name without information, let's go to Wendy first.

WENDY SELTZER: Thanks. Wendy Seltzer, non-commercial stakeholder, and I would say that while that may seem intuitively like an appealing distinction, it's not one that ICANN should be making because it's too fuzzy a line to enforce in the collection and provision of public registration information. There are places in law that may impose requirements on commercial sites that can be fulfilled in other ways than through the WHOIS, but to tell individuals if we were to try to make this distinction we would then get into questions of, is the use of ad words on a personal Web site transform it into a commercial site? Does the provision of a link to the site that is selling the book that I wrote transform it into a commercial site? Does the linking to sites that offer affiliate fees for sending you over to make a purchase or a subscription

transform a use into a commercial use? While those are uses in commerce, I think they are also uses that fund a great deal of nonprofit and non-commercial and individual expression and speech. And so trying to draw those distinctions would just either involve us in a morass of finer and finer line drawing and ultimately chill what we should recognize as legitimate free expression without those.

CHRIS DISSPAIN: Thank you, Wendy. Thanks, and congratulations on getting a mention of the book that you wrote in there.

WENDY SELTZER: Hypothetically unfortunately.

CHRIS DISSPAIN: Elliot.

ELLIOT NOSS: Thank you, Chris. Elliot Noss with Tucows. I have now heard what I would describe as a red herring three separate times in the brief moments since we've started which is that consumers -- and this is about consumer protection -- need to know who they're doing business with. So I consider that a red herring in two or three separate ways.

First of all, the place where consumers will find out who they're doing business with will be much more found in the browser bar. If people are transacting online, the site will have an SSL certificate. That SSL certificate will be displayed in every browser bar commonly in use

today. And in fact, recently we have the extended validation SSL certificates which turn the browser bar green. If somebody is unable to parse that information in terms of who they're actually transacting with, I think it's really sophistry or just our imagination that they would then be able to dig a level below that into the WHOIS data to determine who they're doing business with. So we have a huge paradigm already with SSL.

The second thing is we need to importantly recognize the transactional elements online are a tiny percentage of the web. Some well sub 5% of Web sites are transacting online. The vast majority are informational. We have enough problems today with people finding out where their information is coming from. So, you know, you're talking about a couple levels here, the tiny level is transactional, maybe some small layer on top of that, let's call it professionally informational. Anybody in those two layers has a huge competitive incentive to make their information public and accessible. What we're left with is the vast majority of the Internet, which is people connecting with and sharing information with other people. And there the consumer protection or the deep demand -- the deep incentive for us to have access to that information to protect users of the Internet goes down to something approximating zero. So I really think that what we're doing too often here is taking this tiny little slice and expanding it to make the WHOIS into something it's not. Thank you.

CHRIS DISSPAIN: Elliot, I just want to ask you a yes or no answer.

Tucows deal with a lot of cc's. Are there any cc's that you deal with that you know that have differentiation between personal and corporate in their WHOIS?

ELLIOT NOSS: Yes.

CHRIS DISSPAIN: Thank you. Ray.

RAY PLZAK: Just a point of clarification. We're not talking about WHOIS here.

CHRIS DISSPAIN: I apologize, Ray. I was actually talking about WHOIS, existing WHOIS.

RAY PLZAK: Other mentions have been made to WHOIS. We are not talking about WHOIS. I have a problem with this differentiation commercial versus noncommercial. You know, in the end what we're really reflecting here is activity that is the result of a transaction either in the establishment of a top-level domain or reflecting a transaction that is the result of a top-level domain issuing, if you will, or recognizing second level domains, and we're not talking about the registration of Web sites. And so we need to be clear about that. The information is being collected is being collected about transactions. Certainly at some point in time a -- from one perspective, the domain operator, if you will, is going to be reporting the users and it's that point where you're reporting the users

is where you would see a registration that might pertain to a Web site. It might pertain to something else entirely different. So we need to keep ourselves in that transactional thought process. And the question data requirements actually goes back to the first question which is not only what it is you're collecting, what is the requirement to collect but also what are you even required to report. And so that's where you really should make the distinction.

CHRIS DISSPAIN: Thanks, Ray. I'm going to take Don because he hasn't spoken yet. We are running out of time on this session, so Kathy I'll give you a very short time at the end. Don, go ahead.

DON BLUMENTHAL: Appreciate it. Don Blumenthal with public interest registry. I originally was going to raise the point about this economic versus non-economic distinction but I think Wendy covered it as well as anybody could. Interesting idea, not feasible.

I did want to respond to something that Elliot suggested there, though. I used to be in law enforcement and we advised consumers to check WHOIS records. Particularly in the -- and the numbers are growing. You may know generally who you've transacted but an increasing number of Web sites don't have basic things like address or phone numbers or any way to get in touch with them except for e-mail, if that. You know, you've got the -- the dialogue -- (buzzer) -- to submit your information. You don't know where it's going. You may question how useful that information it will be that you get from the domain information. But

the fact is, consumers do use it. They're advised to by law enforcement and from experience I can tell you that they do and check WHOIS records.

CHRIS DISSPAIN: Thank you. Real quick, Kathy.

KATHRYN KLEIMAN: Sure. Kathy Kleiman again. A quick no, no, no, no, this question has always come up across the last ten years and it seems like an easy differentiation, commercial versus non-commercial, but what is non-commercial. Nonprofits collect money, they collect donations. Foundations do, too. By virtue of collecting that money are they suddenly commercial? No. They're still nonprofits. Kathykleiman.com switches between commercial and noncommercial.

CHRIS DISSPAIN: Thank you. Now, Elliot.

ELLIOT NOSS: Very briefly, in response to Don's comment, I think that's exactly right and the WHOIS is a beautiful mechanism. If I'm going to give somebody my money and they don't have information that I want in terms of being able to contact them, I don't give them my money.

CHRIS DISSPAIN: Don't give them the money. Thanks, Elliot. Let's take the next one. Which is privacy requirements, and I'm guessing that may be Stephanie.

STEPHANIE PERRIN: Thanks very much. As our group has been focused on this privacy issue, which I gather has been a key issue for some time, we're mindful that when it comes to data protection requirements, we're operating in a global society, there are differing laws, there are differing jurisdictions, and so the data protection requirements may be slightly different. Nevertheless, they all tend to focus on purpose. So it's important that we understand the purpose for collection, the purpose for use, and the purpose for disclosure. And the impacts that that has on the registration data that we gather.

Now, it is obviously clear that this is interesting and useful data for a number of purposes. The job in most privacy regimes is figuring out which ones are relevant and which ones are appropriate and doing the difficult job of keeping it narrow and restricted to purpose. So understanding what those purposes are is key.

We already have registrar local law exceptions that have been implemented. There is -- we have discussed whether those are working well and how that's impacting the communities. So no doubt we'll be looking at that further. You see that little blue box on the top? The question has arisen and we have started discussions on whether it is time for ICANN to develop a privacy policy and what that would look like, given a global universe of differing laws and jurisdictions where there isn't law.

So I move on to the discussion questions. The first one is whether and how to accommodate Anonymous registrations. If we are moving towards greater accuracy, then privacy by obscurity becomes more difficult. There are technological means of providing Anonymous

registrations, there's also the whole -- the whole question of how we manage the -- the proxy registration services.

And then the second question is, what are the possible safeguards to minimize abuse and protect the privacy of registrants. And abuse, there's various kinds of abuse and we would encourage you in your comments to us to interpret that fairly widely as abuse on all sides.

CHRIS DISSPAIN: Thank you, Stephanie.

Anonymous registrations and protecting privacy, which is kind of presumably protected by an anonymous registration. But, leaving that aside, Bertrand, you're the first to the microphone.

BERTRAND DE LA CHAPELLE: Bertrand De La Chapelle from the board. In the discussions that followed in the past on those issues, I sense that there's this clear distinction between what is, in a certain way, compulsory for legal reasons regarding things that must be protected, particularly for individuals and depending on the different jurisdictions and the second question, which is the optional capacity to shield one's visibility behind the proxy servers. Those are two very different things, I understand. It turns out in places where privacy requirements are particularly strong, i.e, in Europe there's a whole lot of practices among the ccTLDs in the diverse modalities that certainly can build upon. The second thing on this second aspect, the key question is not so much the capacity to have the proxy registration. Because they do exist. The key question is under which conditions they're unlocked and by whom.

CHRIS DISSPAIN: Thank you, Bertrand, Carol has got a remote comment from somewhere in the world. Probably next door in the other room, actually, is usually what happens.

CAROLE CORNELL: Hi. This comment came from Kieren McCarthy, more of a comment or a suggestion than a question.

One of the big problems with domain registrant's information is ensuring its accuracy, especially as there are so many domains out there. It may be worth using the millions of Internet users as a reporting tool providing a simple mechanism in a browser to flag problems. Rubens suggested WHOIS could be displayed in the browser. Elliot identified the different types of Web site owners. It may be possible to do what Nominet in the U.K. does and get people to select whether a site will be used for business or personal. For the business site, you could then display a full registrant's information in the browser. A personal site could have details withdrawn. If the Internet user sees something that doesn't make sense, they could do simple click reporting. Obviously, it's just an idea. But it may be useful to consider if you are completely reviewing how to do this.

CHRIS DISSPAIN: Thanks, Carole. Thank you, Kieren. I know you're not feeling very well right now, so it's good that you're still able to think. Amadeu.

AMADEU ABRIL i ABRIL: Say my name, I appear anonymously. A couple of questions. You said, Stephanie that you're considering the models that are up there. But have you asked for statistics about the request for access or requests for communication with those registrars that have some sort of privacy for individuals, for instance, dot car, dot tell. Or in the ccTLDs the dot FR, dot CA, dot UK in different ways? I think that would be interesting. Because, if we tried to get things in an abstract way and we go from one extreme to the other about freedom of expression or protection of privacy or law enforcement and we don't look at what really happens when you change one of these parameters and what's the real impact of that, I mean, we will miss part of the things. In abstract, everything is difficult. All right? So -- but everything seems simple, but it's difficult. If you see a great example, perhaps we'll learn how to handle that.

Regarding anonymous registrations and all this part, why do we want anonymous registrations? It's not simpler to have real registrations with real data not being displayed publicly and only being disclosed for legitimate purposes instead of having everybody having anonymous and non-accurate data being published? I think that public WHOIS accessible to everybody where everything is entering correct or belongs to a third party that is acting as a proxy, then maybe acting responsibly or not, this is probably is the worst situation we can have. And it's what we're having now.

CHRIS DISSPAIN: Thank you, Amadeu. And, to answer your question, we haven't yet. But we will go and get data from those places that do make the distinction between commercial and non-commercial.

Ray, Wendy, the lady behind Wendy. Hi. That's going to close it, I think. Can I ask you all to keep your comments reasonably brief. Ray?

RAY PLZAK: Yes. The question of privacy really has to do with two things. The storage and the provision has nothing to do with the collection. And so collection is what is needed to put -- to get the registrations done. And the conditions of what is to be reported and how it's to be reported through the provisioning is where you have to apply the privacy and takes care of all your anonymous registrations and so forth. The storage is the -- is protection of all the data.

And so this question really is one that really needs to be taken up inside the areas of both storage and provision. Thanks.

CHRIS DISSPAIN: Thank you, Wendy.

WENDY SELTZER: Thanks. Wendy Seltzer. I really welcome this effort that's taking a broader look at privacy and anonymous speech that have sometimes been deemed out of scope in the old WHOIS discussions.

So, very briefly, anonymous speech in the United States is protected by the First Amendment. The rights of free association are protected under the First Amendment. And domain -- and, as human rights elsewhere in the world, there are similar protections for the right to speak and associate without providing a name. So, as domain names are used as the stable location for --

CHRIS DISSPAIN: But, Wendy, you don't need to have your own domain name in order to protect your right for anonymous speech, do you? There's plenty of opportunities to speak anonymously.

WENDY SELTZER: Yes, you do, in fact. If you want to be able to refer people to the location of your speech without depending on a third party to reveal or not reveal your name and the legal pressures that that third party might be under or the political pressures that that third party might be under, the best way to secure that, when you give somebody a pointer, they will be able to follow it to find your speech is to have registered your own domain name.

There are second best solutions that plenty of people use. But why should we be relegating the speaker to a second best solution when we've got this great technology for speech?

I'm entirely willing to engage in discussions of how we can protect against abuse of the anonymously registered name. As I've discussed in other forums, we could have a rapid takedown procedure. We could have other mechanisms of escrow that would help to ensure that, if these names were misused, they could quickly be deactivated. But I think it's critical to recognize --

>> Wendy, sorry to interrupt your full flow. With respect to your thing about anonymous, are you talking about -- do you want full anonymity or do you want protection of identity?

WENDY SELTZER: I think if a registrar wants to offer --

[buzz]

>> In an ideal world, what would you like?

WENDY SELTZER: Full anonymity.

CHRIS DISSPAIN: We need to move to the last speaker, Wendy. So appreciate it. Thank you.

>> Hi. (Saying name)

I'm actually from a registry of IP address, and we run WHOIS. So just want to share a practice for your reference.

We actually have privacy law in Japan that requires us to protect the privacy information of home users. But we also felt that accuracy of the registrants are very important as well.

So what we did was that we tried to do both. So we require all registrants to register all their information including their postal address, phone numbers, et cetera. But we don't make all the registration data open. So, for the home users, we do not disclose the information. And then, when we receive requests from law enforcement agencies, then, if it's required under the law, then we

disclose this data, if it's necessary to be used for, like, spamming or phishing or those kind of, like, situations. Just for your reference.

CHRIS DISSPAIN: Excellent. Thanks very much. That's incredibly useful.

Next one. Who is in charge of that? Fabricio, off you go.

FABRICIO VAYRA: Thank you. We've been discussing requirements and what requirements there could be for ensuring data accuracy, how those requirements could lead to more reliable data, more quality within data.

And I have to say I'm very happy for Amadeu to have teed this up about three times already in the session, which is that you'll see accuracy is something that is a continuing theme. I'll say something that's thread through the prior comments and topics that you've heard and the ones you'll continue to hear about data accuracy.

To give an example of some of the things we've talked about based on prior comments, just the prior one, accuracy, we've discussed how a mechanism to better protect the privacy of users could increase the reliability and quality of data. So, just to give you guys an idea of some of the things that we're thinking about.

Now, naturally, that topic always turns to also how do you deal with or how do you process people who put in inaccurate data.

So we've had many discussions really linked around what happens today. Should these processes change? Is there room for change? Could the processes be better based on what was intended in today's processes?

So our question today is should the remedies for inaccurate data differ? And the examples we have are between fraud, criminal, and malicious conduct. Not limited to that, we'd love some feedback on if there should be a difference on how you deal with inaccurate data.

CHRIS DISSPAIN: Thanks, Fabricio. This is a no brainer for some CCs. Of course, if you provide inaccurate data, there should be some kind of sanction. And in some CCs -- and the numbers registry, Ray. Thank you. And some CCs will take the name away from you, and others will insist that you correct and so on.

So what do we think? Does no one care about this one? Or is it just so obvious that there should be sanctions that it's just a question of how big the stocks are in the center of the village? Mathieu.

MATHIEU WEILL: Hello, everyone. My name is Mathieu Weill. I'm the CEO of AFNIC, registrar of dot FR. And a number of CC policies have been mentioned. And I think we've been doing a lot in terms of privacy protection and also accuracy for WHOIS in the last few years. Dot CA or dot cat, actually, were inspired by our policies. What we do -- I think the testimony I can give is what do we do when we have inaccurate data in dot FR. It's very simple. It's in French law, so we're bound to do this.

Inaccurate data is a reason for domain name takedown. So we do that on a very regular basis under dot FR. But the law also states very clearly that this takedown cannot happen until the registry has put the registrant in a position to correct the data, whatever the situation -- fraudulent, criminal, malicious conduct. This is not a -- the policy says we don't have to discriminate between those options. And, therefore, we have to give a reasonable amount of time to the registrant to correct the data before we take it down.

CHRIS DISSPAIN: Thank you, Mathieu. We've got -- I'm going to give everyone a minute. So Elliot, one minute. Wendy, actually, now 50 seconds.

WENDY SELTZER: Wendy Seltzer. I think we'll be able to answer this question much better once we have mechanisms for protecting privacy other than the provision of inaccurate data. And so I mostly recommend deferring answering this question.

CHRIS DISSPAIN: Well, hold on. Let's be specific here. Let's assume that you have an option to not display the data. Should you be required to provide accurate data to your registrar? So, assuming you have an option for it not to be displayed, should there be a requirement for accuracy?

WENDY SELTZER: Modulo my earlier comment that you should be able to provide no data because --

CHRIS DISSPAIN: I understand that.

WENDY SELTZER: -- because you should be permitted to have -- I don't -- I think -- I'll say I think it's a better question to answer when we have more information about the privacy options.

CHRIS DISSPAIN: Fair enough. Fine. Elliot.

ELLIOT NOSS: Two quick options. First, it is the case -- we've heard from a couple CCs that the CCs that have more restrictive policies around address and accuracy tend to also do worse, much worse, competitively relative to the gTLDs.

CHRIS DISSPAIN: But if you level the --

ELLIOT NOSS: If you're talking, it's not part of my minute, right?

CHRIS DISSPAIN: That's right. But, if you leveled the playing field so that everybody was roughly on the same level --

ELLIOT NOSS: So you'd like ICANN to -- impose --

CHRIS DISSPAIN: I wouldn't like anything. I'm just asking.

ELLIOT NOSS: -- the WHOIS requirements on dot AU? Did we get you on the record on that?

>> Elliot, with all due respect, I mean, what are the top 5 largest ccTLDs?

ELLIOT NOSS: Don't insult somebody with "all due respect," but yes.

>> What are the top 5 -- Elliot, what are the top five ccTLDs at the moment?

ELLIOT NOSS: I don't think it's a quiz. It's going to be DE, UK.

>> No, but -- okay. So UK has certain differences here. So I'm just wondering what --

ELLIOT NOSS: They have differences, but they don't have nearly the same restrictions around residency. The second point is --

CHRIS DISSPAIN: Yes, Elliot.

ELLIOT NOSS: -- that it's impossible to talk about requirements for accuracy in a vacuum relative to who has access to the data and how they have access. Because I think it's the way that today the WHOIS is abused by some parties who think they should have access that leads to a lot of the anonymity. So I think that those two things in isolation are impossible to answer.

CHRIS DISSPAIN: Okay.

>> And that would be the point of this working group. We're working on it all holistically.

CHRIS DISSPAIN: It's an in principle question anyway. I'm going to need to close the line. Bertrand, you get the last word. But you're going to need to be really quick. Don, go ahead.

DON BLUMENTHAL: Okay. Just focusing on the narrow question of on differential penalties given what the abuse is, I think you get into a definitional quagmire. It's got to be all or nothing. Countries -- laws vary too much. Individual definitions -- what's fraud, what's abuse, what's Internet, law

enforcement, vary too much to start getting into that element, that level of detail.

CHRIS DISSPAIN: Okay. Thanks, Don. Ray.

RAY PLZAK: The choice of the word "remedy" is useful here. There's two things here. Firstly, it's the collection issue. How well does a registry or registrar vet the registrant? How well do they know who they are? What kind of checks do they do? The address registries spend an awful lot of time vetting possible registrants to determine whether or not they're spammers and so forth. So there's a lot of very valid business practices could be done during the collection phase to ensure that.

The second thing that, as human nature happens, people change phone numbers and all kinds of other things. So there has to be a plan to refresh the data, if you will. So a periodic refreshment of the data where a reregistration type activity is the case of that.

If you take the idea of sanctions, I'll leave that up to the lawyers to figure out how big the stocks should be or how high the guillotine should be.

CHRIS DISSPAIN: Thanks, Ray.

Amadeu, one minute.

AMADEU ABRIL i ABRIL: One thing regarding complete anonymity. This could pose serious trouble from the contracting point of view of registries and registrars. They may accept my name is Mickey Mouse. But they cannot sign a contract with somebody saying I don't give you my name. I don't give you my address. I don't give you an e-mail for contact when the name has to be renewed. But that's a side point.

The other question regarding accuracy, please, I trust Michele to have dealt with that. But accuracy and the quality of the data are two things different. I manage the domain names for many of my friends who don't want to know about WHOIS and things like that. Some of that data is not accurate because they have moved physically. It's all -- physical address is still there. But there's still virtual, the e-mail versus the telephone world. So this is what is important. The data is enough to get useful communications, right?

CHRIS DISSPAIN: Which is why we have the word "reliability" up there. Reliable data is, we think, probably more important than accurate data. Steve?

STEVE METALITZ: Steve Metalitz. My answer to this question would be no, if you're talking about the remedies within the registry and registrar world. But, as people have mentioned, national law has an impact here, too. And some countries have greater penalties for committing crimes using -- in which you use false data. Finally, I just mention that data accuracy and quality is also --

(scribes lost audio connection).

CHRIS DISSPAIN: Amadeu, I just realized we lost the scribes. Okay. They're working on it. Cool. Steve.

STEVE METALITZ: Steve Metalitz. If I had a one word answer, I guess it would be no. And probably, basically, for the reasons that Bill Smith said. This really gets back to my initial concern, which was, if there's going to be tiered access, we have to make sure that everybody who may have a legitimate interest in this, every Internet user, is in a tier somewhere. So we don't want to have a solution that works for law enforcement, that works for big trademark owners, that works for others but doesn't really work for the public as a whole.

CHRIS DISSPAIN: I think there's an assumption -- I may be wrong, there's certainly an assumption on my part that the tiered access starts at a level that is open to everybody. What data is contained in that is a different issue. But I understand your point.

STEVE METALITZ: And that no level would be zero. I just find that --

CHRIS DISSPAIN: I understand that.

STEVE METALITZ: Our status quo is we have anonymous access to this information. And I'm sure Wendy would agree with me that there are some very important benefits to that that we want to try to preserve.

CHRIS DISSPAIN: Yeah. Okay. Bertrand.

BERTRAND DE LA CHAPELLE: The term "tiered access" invokes implicitly a hierarchical scale. Like there is a lower level, a middle level, and a higher level and so on. I personally have a preference for the expression I used before, which is "differentiated technical modalities of access," because it allows for something that is not hierarchical but that can be cross cutting, diagonal. Give you an example that can be very interesting academic studies done from the bulk data completely anonymized if this is possibility. I know that there are limits. But, having the bulk for academic study is extremely useful. Having law enforcement access for one layer of information, even an automated capacity to screen, is possible also. And you can imagine systems where the requests are being logged to enable later audits. So thinking about how, not only the requester's purpose, but also the requester's allowance to access the data under certain conditions -- you could have, for instance, law enforcement access free to a certain type of data easily and different depth of access.

But the logging and the capacity to audit is a very important element afterwards because it has sort of a chilling effect on the abuse.

CHRIS DISSPAIN: Thank you. I think we're done on this one. Yes? Anyone just because we've got -- we do have a minute. Does anyone on the panel want to say anything about tiered access? Very quickly. Okay. About -- I just wanted to see if anybody wanted to say anything about tiered access.

MICHELE NEYLON: I'll speak to that very quickly. Something -- what we've been trying to do throughout exercise to date is going back to the very, very basics as in which elements of data are required at a technical level and then moving from there on up. So to, speaking to Steve's point, you know, it's impossible, technically, for a domain name to resolve on the Internet without some data being accessible to the public unless you come up with some new protocols. And I'm sure you can mulletize that. But, you know, on a technical level it's just not going to happen. So you'll always have some type of access.

CHRIS DISSPAIN: Stephanie, you wanted to say something. And we'll finish it there. And Kathy.

STEPHANIE PERRIN: I just wanted to respond on the comments about this more articulated vision. I totally agree. And you certainly don't want to lose research and statistical analysis. And the problem, of course, is that this balance is with the response burden on the community that's providing this. If they have to evaluate each request, that can be burdensome. I mean, there's a reason why things are open now. We have to figure out how

we calibrate this. But I think more complexity is ironically better than less complexity.

CHRIS DISSPAIN: Thank you. We're going to close now with the last two, Bill and then Kathy.

BILL SMITH: Bill Smith, PayPal. In any form of access that requires identification, one of the things that we should be concerned about is not only the privacy of the individuals who are registering domains but the privacy of those who are asking about them. And that is -- that, actually -- [buzz] -- is a more serious concern because of who is maintaining that data in the logs, et cetera. So that's something that the working group, I believe, should consider if you're going to come back and suggest tiered or some other form of access.

CHRIS DISSPAIN: Thanks, Bill. Finally, Kathy, real quick.

KATHRYN KLEIMAN: This is a great conversation. We should have been having it for years. Tiered access and the privacy of those registering domain names and the access to that data and the privacy of those trying to access that data and the privacy of that data. Great discussion. Thank you.

CHRIS DISSPAIN: Okay. I'm going to get the last word on this to Stephanie, and then we're moving on.

STEPHANIE PERRIN: I was pretty brief on the discussion of the potential privacy policy. But everybody should understand that a potential privacy policy looks at all individuals, all data. And there would be different rules for the different areas. So that's a complex beast. It's not just about what goes out on WHOIS.

CHRIS DISSPAIN: Absolutely. Yes, next one. Last one. I think. Yes, sorry, Lanre.

LANRE AJAYI: i think we would like to obtain comment on if it is reasonable to request for costs to access the registry data should we be a mechanism where users will pay some fee to access a certain number of --

CHRIS DISSPAIN: Excellent. I agree we should get some comment on that, but not right now. There's an e-mail address that everyone can send their -- I've no doubt people have comments about that. Absolutely they do.

Storage and performance requirements, which is Faisal, I think. Faisal, over to you.

FAISAL SHAH: This is how of what happens to the data, specifically how the data is stored. We briefly discussed two different models, a distributed model, which currently exists right now, and a second model which is a centralized database which is a central place where all the data would be housed.

There are challenges and advantages to both. With so many additional registries coming on, the question is the distributed model -- a distributed model might be more challenging at that point. But perhaps there may be different flavors of a distributed model.

Regardless of which model is adopted, however, there may be certain metrics which need to be put into place in order to evaluate performance. Perhaps spot checks, periodic audits.

There will also need to be security mechanisms which would be implemented within the system itself. For example, with a centralized database, you can manage access by requiring credential information or you can manage tiered access, but as Rod says, it's differentiated technical modalities. That's how you do it.

We might need to have redundancy by providing for an escrow holder.

But with a centralized database, the question then becomes who will manage this database and what are the ancillary costs attendant to that and are we going to be charging, as somebody just brought up now, to access?

So we haven't really gotten into this topic, and we kind of scratched the surface on it. That's why I think it's so important to get your feedback.

And the question is what are the costs and/or benefits of a distributed versus centralized database.

CHRIS DISSPAIN: Okay.

There must be some registrars in the room apart from Elliot -- no offense, Elliot -- who have an opinion about centralized database.

Possibly some registries, Chuck. Maybe.

I'm going to start with Ray.

RAY PLZAK: So I presume you're talking about this in relation to a single gTLD.

CHRIS DISSPAIN: Yes.

RAY PLZAK: Each one would have either a centralized or a distributed database.

CHRIS DISSPAIN: Well, No. It's possible you could have an overall centralized database for all gTLDs.

RAY PLZAK: So you're talking about every gTLD -- the data collected by every gTLD would be in a master --

CHRIS DISSPAIN: Yeah, there's an organization in Geneva that has the database. All of that stuff.

RAY PLZAK: I would be totally opposed to that model to begin with.

CHRIS DISSPAIN: Okay.

RAY PLZAK: So answering that question as to each gTLD, I would propose you could almost leave it up to the gTLD to decide, but what you need to have are rules and processes that they have to follow in order to do that.

The big thing that has to be done here is process and control audits of the factors that you mentioned there. And that's probably more important than anything else.

So having a policy or sets of rules or guidelines, whatever term you want to use, for every gTLD so they can choose whether they care to do a distributed database or centralized database I think would be a better solution.

CHRIS DISSPAIN: So let's get clear. Let's just get clear for a second. Under the new gTLD contracts, every new gTLD has a thick WHOIS, or whatever we're going to call it, and that means that that is run from one location. Right? Registry.

So we already have that for all the new gTLDs.

So the question -- So it is more about a centralized database across the whole of the space, and whether that is something -- and which you said no to, but --

RAY PLZAK: I say no to 30,000 gTLDs being -- all their data being in one database. That's not scalable. But I do say you should have a choice between whether or not -- each gTLD should have a choice, and you have to provide the rules for it to happen. And the most important thing in that regard is you have to have process control audits.

CHRIS DISSPAIN: Got it. Bertrand.

BERTRAND DE LA CHAPELLE: Bertrand de la Chapelle. I'm not sure it's a completely either/or. The fact is the collection of data is decentralized by nature as Chris Wiki was mentioning so it is a crowd-sourcing system.

The second thing is if there is enough standardization or protocols that are clear, there is the possibility, even if they are maintained separately, to allow people to make the gathering and there may be several actors gathering this type of data for different types of users.

The choice that is being made is whether -- that is apparently presented, is whether there is a single thing that becomes the exclusive

reference point or whether the distributed bases are the reference points and there are different modes of aggregation.

That being said, if you look at the root server model, it is also a single database that is distributed.

So it's not an either/or. It can be a distributed system of access with --

CHRIS DISSPAIN: Yes.

BERTRAND DE LA CHAPELLE: -- single database.

CHRIS DISSPAIN: That's absolutely right. You are correct.

In fact, I think we actually talked about that at some point.

Chuck.

CHUCK GOMES: Thank you, Chris. Chuck Gomes from VeriSign.

First of all, some historical information. The original -- I think it was Network Solution's agreement, it could have been VeriSign, but actually it required us to be prepared to offer both two concepts: centralized WHOIS, which was across TLDs, not just the TLDs we operated, and universal WHOIS, which would have included CCs, and we quickly

discovered CCs might never cooperate on that so we didn't go that route.

I won't repeat what you said, Chris, but I was going to make the same point with regard to the fact that, right now, registries in thick registries, all the data is fed up anyway.

I guess the last thing I would say I would question, and I'd like to talk to Ray further about this, why a centralized solution would not be scalable.

We have a pretty large database for quite a few names coming from hundreds of registrars. So I'm not sure -- And I'm not the technical person that's the right person to answer that, but I think it might be scalable.

CHRIS DISSPAIN: Okay. As you say, you can talk about that off-line.

Rubens.

RUBENS KUHL: Rubens Kuhl.

Continuing on Bertrand's point, it's possible to have distributed database with centralized authentication and logging purpose.

CHRIS DISSPAIN: That's correct, it is.

RUBENS KUHL: So the database could be everywhere but could recognize centralized limited certificates for law enforcement authorities, privacy authorities, and so forth.

CHRIS DISSPAIN: Thank you, and that's an extremely good point. I can't remember who said it earlier on, I think Amadeu said how difficult it was to recognize law enforcement across borders and so forth.

One of the possible advantages of that sort of thing is you only have to go through that once centrally for the law enforcement. Not every individual registrar has to do it.

So thank you.

Steve.

STEVE METALITZ: Steve Metalitz. I think we are in violent agreement this is not an either/or question.

CHRIS DISSPAIN: Absolutely.

STEVE METALITZ: The only point I wanted to add is the WHOIS Review Team, which has not been mentioned very much this morning --

CHRIS DISSPAIN: We've talked them an awful lot amongst ourselves.

STEVE METALITZ: And one of their recommendations was ICANN should establish a centralized portal to all of the registration data for gTLDs. And as I understand it, all those recommendations have been approved by the ICANN Board.

So we are in the process, I guess, of coming somewhere on this spectrum at least as far as a centralized portal is concerned.

CHRIS DISSPAIN: Thank you, Steve.

AMADEU ABRIL i ABRIL: Trying to be very brief. First, no to an uber mega super-duper registry having all the data for everybody and applying the same rules to everything because one of the problems we have here, not the whole problem, but one of the problems we have is for registries and registrars complying to local law.

You have a single rule for everybody with a single, you know, --

CHRIS DISSPAIN: Yeah.

AMADEU ABRIL i ABRIL: -- between Dallas Airport and the Pentagon, somewhere there --

CHRIS DISSPAIN: Got it.

AMADEU ABRIL i ABRIL: -- that would not help.

The other question is yes to what Rubens said and I was just coming here to say. What we need is to centralize the accreditation of the requesters and the orders to the registry that this is really a valid request.

This is also something also we have been discussing with the Anti-Phishing Working Group in a very different context.

CHRIS DISSPAIN: Thanks. Understood.

Sir.

ANDREW SULLIVAN: My name is Andrew Sullivan. I work for Dyn but I don't speak for them.

Two points. First of all, the analogy with the root zone is a little awful because the root zone is tiny and we're talking about all of the registration data here so I think it's a bad idea.

Secondly and more importantly, we already have experience with the idea that you're going to have more than one person have the same data; right? Because we had the so-called thin WHOIS in which we had the registry and the registrars have the data and then we have multiple

registrars who had the data and then we had a problem about communicating that data and shipping it around.

So it seems to me adding yet another layer to the same set of problems is a bad idea. This is fundamentally a distributed system so we should have a distributed database.

CHRIS DISSPAIN: Thank you.

Bertrand is going to have the last word on this.

The next bit is our open session. You can comment on any aspects of this that you want. You can talk about the costs issue that Lanre brought up as to whether it would be possible to charge for this. You can talk about anything to do with next generation registry services that you like. So if you've got other things to say, come to the microphones.

Bertrand.

BERTRAND DE LA CHAPELLE: Yeah, Bertrand De La Chapelle. Just one point. It turns out the kinds of questions we are addressing in the case of WHOIS, particularly regarding law enforcement access to this --

(buzzer) -- is similar to other types of issues that are faced, for instance, in the relationship between law enforcement and large platforms, such as Facebook or others, because they own a lot of data by the activities of their users. And to do a little bit of self-advertisement, the program I run on Internet and jurisdiction at the moment is precisely dealing with

what we call procedural interfaces between the different operators, between the law enforcement, the companies, be DNS operators or ISPs or platforms in the Internet space, but also civil society groups in order to make the triangle a series of interoperability procedures that guarantee due process and streamlining of interactions in an as automated manner as possible with as much checks and balances as possible.

So there are similarities in other regions.

CHRIS DISSPAIN: Thank you, Bertrand.

So the final one is anything else. If we can have the next slide up, please. Okay. They're working on it.

Okay. No one wants to charge about charging for access to this data at all? Everyone is happy with that idea? Good. Tick that one off. Not a problem. We can charge (laughing).

MICHELE NEYLON: Sorry; so we've now solved all of our problems.

CHRIS DISSPAIN: We've now solved all of our problems because we can charge. Exactly.

Next slide --

MICHELE NEYLON: Perfect. Elliot is up at the mic.

CHRIS DISSPAIN: Exactly. Elliot, off you go.

ELLIOT NOSS: Were you just killing dead air there, Michele?

MICHELE NEYLON: Yes.

ELLIOT NOSS: I think that Bertrand -- I wanted to get to this in sort of a closing. I think Bertrand has raised a great point, which is we need to recognize that what we are doing with the WHOIS system is we are public stewards of a resource, which is the DNS. There are numerous private resources, like Facebook, Google, and others, who not only are potentially more appropriate for deep dives on data around people's driver's license for the Internet, which is what a lot of people would like to turn WHOIS into, but also are governed by legal regimes that -- and contractual regimes that make that access, that deeper level of access more appropriate.

We are stewards of a public resource here. This should be the resource where there is the most privacy protection for individuals.

Where people, which is what the Internet is about, where people are able to access and use this resource in a way that allows for the most sharing and the easiest way to get a communication out.

It should not be the lowest common denominator but should be the highest.

And so, you know, I always find it deeply ironic when there are calls, you know, for this resource, being the one that is the tightest regime around privacy and individuals' rights.

CHRIS DISSPAIN: Understood.

Peter, I'm going to go to you. I think that gentleman is just counting the number of people in the room. Going to go to Peter, then Jim, Carol.

PETER DENGATE THRUSH: Peter Dengate Thrush speaking in my personal capacity.

Chris, I wanted to respond in this open session to your throw-away line that it was a license because to me that begs one of the very fundamental questions we should be looking at and I hope that the panel is looking at that because you know in many jurisdictions it is a license, but in many other jurisdictions it isn't. And there are people who think it's actually a fundamental human right, and there are other paradigms and other legal structures that you might use here.

CHRIS DISSPAIN: Yes.

PETER DENGATE THRUSH: For example, gift or trust or responsibility.

For example, most people would think everybody in a cinema had an inalienable right to a really good means of egress if there was a fire

without having to register their name to be able to get out of that cinema. And people in wheelchairs, for example, mobility-challenged people in many countries have a right to access by ramps, et cetera, to and from buildings. You don't have to register the wheelchair to get access to some of these; right?

So I think a very good important --

CHRIS DISSPAIN: Good point.

PETER DENGATE THRUSH: -- discussion is what is the nature of it, what is the legal paradigm. Because if you just start with the presumption that it is a license, then you are imposing, creating a situation where the licensor, potentially in this case ICANN, is going to be able to roll out and dictate conditions all the way down the line and I'm just not sure that's a safe assumption.

So what is the nature of it has to be looked at as well.

CHRIS DISSPAIN: Thanks, Peter.

Jim.

JIM PRENDERGAST: Hi. Jim Prendergast, the Galway Strategy Group. I may be getting ahead. There may be another slide, I'm not sure, but --

CHRIS DISSPAIN: No, There isn't.

JIM PRENDERGAST: The question pertains to timing. I know originally when the work plan said a product would probably be delivered in April or May, but I'm sensing from today's discussion that we're probably a little ways off. Do you have any estimate on when there may be a document and also what will be the internal process you will use to produce that document? Will it be consensus? Will it be dissension? How is that whole process going to work? If you've figured it out yet.

CHRIS DISSPAIN: Jean-Francois, do you want to briefly address that?

JEAN-FRANCOIS BARIL: The timeline is quite difficult to estimate because I think this is a big, big issue that, as you can understand from different and various aspects that the questions were reflecting today. But I believe if we were having the possibility to have a blueprint before Durban, I think it will be a great, great achievement for this team.

CHRIS DISSPAIN: And its consensus, generally speaking, I think.

JEAN-FRANCOIS BARIL: Absolutely.

CHRIS DISSPAIN: So I think what we can say pretty for sure is fewer than ten years, Jim.

Carole.

CAROLE CORNELL: Hi, this is from a remote participant, Joly MacFie. I thought it was a fair point about reliability. That it matters often enough to know that one can reliably contact a registrant as knowing who they are.

CHRIS DISSPAIN: Thank you, Carole.

Steve.

STEVE METALITZ: Steve Metalitz. I just want to dissent from the idea that Elliot proposed about this.

WHOIS, or I should say the gTLD registration data database looked at as a whole is a public resource. And it is a resource that is extremely important to accountability and transparency on the Internet.

ICANN has been the steward of that resource for about the last 15 years. And in my view, ICANN has not done a very good job as that steward. There have been many challenges, but I think the data is less accessible and probably less accurate today than it was then.

So I think what this group is doing, it's extremely important to try to improve the management and the stewardship of that very important public resource.

CHRIS DISSPAIN: Just very -- Who decided it was a public resource? Why?

I mean, if it didn't -- it wasn't here, would we make it one?

STEVE METALITZ: Yes, I think if we didn't have something like this, we would have to invent it because people, Internet users, need to be able to find out who they are dealing with online.

CHRIS DISSPAIN: Okay. I notice Wendy's playing microphone hop, which is fine.

Bertrand, could you let Carole do her remote participant before you? Thank you.

CAROLE CORNELL: Thank you. This one is from Kieren McCarthy.

CHRIS DISSPAIN: Again.

CAROLE CORNELL: Since we are talking about the next generation of services, I think the working group should make sure that you engage the browser companies such as Google, Microsoft, Mozilla, et cetera. They may have some really good ideas.

CHRIS DISSPAIN: Thank you. Indeed.

Bertrand.

BERTRAND DE LA CHAPELLE: Bertrand De La Chapelle.

Actually, I'm not absolutely sure that it is a public resource, but would I qualify it, rather, as a public service.

There is an equivalent of a land record type of function here. The WHOIS, or whatever directory services, is the equivalent of what we call in French the cadastre or land records. And this dovetails with the general description of what the activity and one of the fundamental responsibilities of ICANN. ICANN has a fundamental responsibility in terms of a notary function. The root is a notary function. The supervision of the directory services and establishments of the rule of the land records is a notary function.

So in this respect, it's not the steward of the resource. It is a steward of the process that manages this public service.

The second point is methodological issue. I'm very happy that the Board has taken the decision to launch this exercise and to open up the debate. In terms of procedure, I understand that the role of this working group is basically to frame the issue for further discussion.

Can you explain a little bit the articulation between what you do, where you stop, and the next steps?

CHRIS DISSPAIN: Yes, but not right this second.

In a little while.

Wendy.

WENDY SELTZER: Thanks. Wendy Seltzer.

As we're wrapping things up, I wanted to offer some different visions of what we are doing. And the Internet is a tremendous platform for speech. It is a tremendous platform for communication and connection among people, and we should be very careful that we not set up rules that restrict those communications opportunities.

We have a tendency to think in terms of commerce and mandated contact, but let's also think about free expression and the tremendous opportunities that this brings for contact among people from all different jurisdictions and all different backgrounds. Let's think in terms of those freedoms.

CHRIS DISSPAIN: Thank you, Wendy.

Can I have the last slide up, please.

Bertrand, I'm going to get back to you in a second.

So we have a -- As Jean-Francois said, we have an e-mail address, input-to-ewg@icann.org. That's open for anyone wanting to provide their input, please do so. You can track progress on the Wiki, and as he said, draft blueprint by Durban meeting, which is certainly our goal.

I'm going to hand back to Jean-Francois in a second.

Bertrand, there is a very specific wording about the output of this Experts Working Group going to the GNSO. I don't want to preempt that wording, so when we've got it, I'll give it to you.

I would lick to thank everybody for their participation. Jean-Francois, back to you.

JEAN-FRANCOIS BARIL: Thanks, Chris, for being the very, very good moderator for this session. I think it's not so obvious to assemble all these different thoughts from different angles. But as we said, we came here in a very, very humble way. And I think you responded extremely, extremely well. Probably overpassed our expectation in terms of how many valid input we collected in all the six domains that we were really seeking for your creativity and insight.

So really, really thanking every one of you in the room.

As I said, we'll have this line open in such a way that we will be able to respond. I think Alice is going to put the process in such a way we can be organized to respond so that the journey doesn't finish today. It's just really the kickoff for really inviting the community to help us to shepherd this, I think, fantastic opportunity to make this new generation of gTLD directory services working. And that's people will definitely enjoy this and not complain anymore that ICANN is making things slower and lower level.

So once again, thank you very much for listening to where we are today, but really, really big thank you for you for having so many good insight that we'll take into big consideration.

Thank you.

[Applause]

[End of Session]