ABU DHABI – ICANN GDD: Registry Operator Roundtable
Wednesday, November 1, 2017 – 15:15 to 16:15 GST
ICANN60 | Abu Dhabi, United Arab Emirates

UNKNOWN SPEAKER: This is the ICANN60, ICANN GDD Registry Operator Round Table on the 1st of November, 2017, from 15:15 to 16:15 in Capital Suite 7. [AUDIO BREAK]

DENNIS CHANG: Come on up and join us at the table. [AUDIO BREAK]

Come on up and join us at the table. Here's the seat for you, there you go. [AUDIO BREAK]

This is a one hour session, and we have another session that gets started at 4:00 that some of us have to go to, so I would like to get us started quickly here, if that's okay with everyone.

Let's get started. Thank you for coming. This is the Registry Round Table Session. This is what we affectionately call as the unconference. What that means is that we don't have anything to talk about. There's no agenda. Why are you here? Well, the reason that we are here is so that we can share whatever information we have and we like to have. So the first thing we'll do is go around and introduce yourself very quickly. We're going to start here. Your name, your affiliation and your ICANN age, how long have you been associated with ICANN; can you remember? Go ahead.

MARTIN SUTTON: That's a tricky one. Martin Sutton. I'm from the Brand Registry Group. It must be 10 years now. Thank you.

SUSAN PAYNE: Hi, Susan Payne. I'm from Valideus and I represent the Brand Registry SEA. And about four years.

SOPHIA FENG: I'm Sophia Feng. I'm with ZNS. I've been participating in ICANN since 2012, so five years. I'm in the GNSO Stakeholder Groups.

COLE QUINN: And I'm Cole Quinn. I'm with Microsoft and also the Brand Registry Groups.

DIETMAR LENDEN: Dietmar Lenden, Valideus representing [inaudible], and 14 years.

DIRK KRISCHENOWSKI: Dirk Krischenowski, CEO and founder of dotBerlin and vice-chair of the geographic top-level domain name group. 12 years.

KATRIN OHLMER: Katrin Ohlmer, [inaudible] of DOTZON consultancy for top-level domains. 12 years.

MARK ANDERSON: Mark Anderson, VeriSign. I'm also about 12 years.

AARON HICKMAN: Aaron Hickman, ICANN Org. 4 years.

SHERIE FALCO: Sherie Falco. ICM Registries. 6 years.

KARLA HAKANSSON: Karla Hakansson. ICANN Org. 8 years.

LINETT NARDONE: Linett Nardone. ICANN Org. 4 years.

YUKO GREEN: Yuko Green. ICANN Org. 5 years.

CRAIG SCHWARTZ: Craig Schwartz. Operator of the dotBank and dotInsurance TLDs. 11 years.

MERT SAKA: Mert Saka. ICANN Org. 3 years. And just a reminder. This session I open and is being recorded. We didn't say it, so I should say it.

DENNIS CHANG: Now we know everybody's age.

RUSSELL WEINSTEIN: Russ Weinstein. ICANN Org. 5 years.

VALERIE HENG: Valerie, ICANN org. 3 years.

FRANCISCO ARIAS: Francisco Arias, ICANN Org. I've been around since '97, '98.

DENNIS CHANG: Difficult math.

DAN TRAMPEDACH: Dan Trampedach, Thomsen Trampedach. This is my 10th anniversary this year.

MARTIN KUCHENTHAL: Martin Kuchenthal, LEMARIT, and I think it's 6 years.

MICHAEL FLEMMING: Michael Flemming, GM Reds Consulting, representing Japanese dotBrands. Five years.

YASMIN OMER: Yasmin Omer, Amazon Registry. 7 years.

RAYMOND ZYLSTRA: Raymond Zylstra, Neustar. 9 years.

STEINAR GROTTEROD: Steinar Grøtterød, dotGlobal. Been here since 2000.

DENNIS CHANG: I think you just outnumbered him, right?

UNKNOWN SPEAKER: [Inaudible]. Japan Registry Services. I think 9 years.

UNKNOWN SPEAKER: [inaudible], DB University in Tokyo. I remember I participated in Pre-ICANN meetings, but I hibernated most of the time so maybe three or four years now.

STEPHANE VAN GELDER: Hi, everyone. Stephane Van Gelder, Vice Chair of the Registry Stakeholder Group for Policy and Affiliates representative to that group. 13 years.

JOHN BERARD: John Berard here on behalf of Vox Populi Registry. 14 years.

MAXIM ALZOBA: Maxim Alzoba. dotMoscow. 5 and a half years.

NELI MARCHEVA: Neli Marcheva, [inaudible] Association. About 5 years, or 4.

ZORNITSA MARCHEVA: Hi, everyone. Zornitsa Marcheva, LEMARIT. I think 3 years.

CARRIE: Carrie from ZDNS. 2 years.

MAY KIM: Hi, May Kim. ICANN Org. 1 year.

JENNIFER SCOTT: Jennifer Scott. ICANN Org. 4 years.

ELAINE PRUIS: Hi. I'm Elaine Pruis. I've been attending ICANN Meetings for 14 years.

BEN MCLLWAIN: Ben McIlwain. Google Registry. 3 years.

LILLIAN FOSTERIS: Lillian Fosteris. FairWinds Partners. 5 years.

DAVID MCGILL: David McGill. ICANN Org. A year and a half.

GWEN CARLSON: Hi, everyone, I'm Gwen Carlson. ICANN Org. 4 years.

KIM AUSTIN: Kim Austin. ICANN Org. 9 years.

SEDA AKBULUT: Hi everyone, Seda Akbulut from Global Support for 2 years. ICANN Org.

MICHAELA QUINZY: Michaela Quinzy. ICANN Org. Just under 4 years.

EDUARDO ALVAREZ: Eduardo Alvarez. ICANN Org. 2 and a half years.

UNKNOWN SPEAKER: Hi, [inaudible]. ICANN Org. 4 years.

KRISTA PAPAC: Hi everybody. Krista Papac, ICANN Org. 16 years.

KYLE DUNST: Kyle Dunst. ICANN Org. 4 years.

CHRIS BARE: Chris Bare. ICANN Org. 5 years.

UNKNOWN SPEAKER: [Inaudible] registry.

MICHAEL PLAGE: Michael Plage. Ferris Global. 19 years.

UNKNOWN SPEAKER: Stefan [inaudible], dotSwis. 4 years.

KEVIN KRAIZER: Kevin Kraizer, GoDaddy. About 5 years.

CRYSTAL ONDO: Crystal Ondo, Donuts. 4 years.

RICHARD SCHREIER: Richard Schreier with CIRA. My first ICANN meeting was Luxembourg in July, 2005, so 12 and a half years. Sorry, no. Yeah, that's about right.

DENNIS CHANG: Anyone else? So my name is Dennis Chang. I'm with the ICANN Org and I am 6 years old. So, welcome. And the way the unconference works is this. We're going to ask you now to raise your hand and throw out any topics that you would like to discuss. We've already had, I don’t know, five days here, at least for some of us, and many sessions. I know there are some more to come. But, this is an opportunity where we share information. You can ask the staff questions. You can ask each other questions, and whatever pertinent and important things that you want to talk about.

Now, how many of you have participated in this unconference before? Let me see your hands. Okay, so that's about half of you. So, you know how this works. So, let's start. Who has a topic they'd like to talk about, share, or questions? Go ahead, raise your hand. There, go ahead.

DIETMAR LENDEN: Thanks, Dennis. It's Dietmar Lenden for the record, Naming Services portal. Two pieces, Ts and Cs, and CZDS access fire, the Naming Services portal. And if we have time, GDPL. Did that make sense to everyone?

DENNIS CHANG: Did you get that? Okay. Who else? No other topic? [AUDIO BREAK]

No questions for the staff? You, go ahead.

STEINAR GROTTEROD: I will put the GDPR on the table and not make it just a small portion of the discussion, but hopefully a longer part of the discussion within this table.

DENNIS CHANG: You would like to talk about GDPR but --

STEINAR GROTTEROD: Yes, in a lengthy discussion. Not the last two minutes.

DENNIS CHANG: Oh, you'd like to have a lengthy discussion about the GDPR. Okay. So we have naming services, CZDS, GDPR, what else?

BEN MCLLWAIN: One potential idea -- sorry, were you pointing at -- we can talk about TLD-wide HSTS, which maybe some people here know about but that may also require some explanation.

DENNIS CHANG: Well, we'll find out what it is when we talk about it, so the next thing we're going to do is voting, so it's probably worthwhile actually to find out before we start voting, right? So we're still going to collect topics before we start voting. Okay, final call. Go ahead.

SOPHIA FENG: A topic about DAAR, a domain abused system that ICANN is developing. Maybe we'd like to know more about scope and the timelines and whether it's very important for the registry. Also, there’s some recommendations also brought up by encouraging a registry to use a system to reduce abuse. What kind of mechanisms and policies will help that to achieve the goal that we want to achieve here?

DENNIS CHANG: DAR? DAAR; now it's DAAR. No more? Okay. So let's start voting on these topics. But before we start, TLD-wide HSTS. I think everybody knows what CZDS is, GDPR certainly, and DAAR. Can the gentleman who -- yes, go ahead and tell us what this is.

BEN MCLLWAIN: I'll just take a few seconds to explain, or a few sentences. There's a mechanism called HTTP strict transport security. It's used to ensure that connections to domain names are only secure. So, if you enable HTTPS on your domain name, that's making security optional, but you need the use of HSTS freeloading to enforce that no attacker can degrade security and then allow users to get an unsecure experience.

Recently, it's starting to become a thing that people are using HSTS on the entire top-level domain to secure all domain names. So, that's the topic of conversation.

MAXIM ALZOBA: Maxim Alzoba. Just a small note that HSTS might not go well with GDPR because of super cookies. Thanks.

DENNIS CHANG: Sounds like you want to discuss this.

MAXIM ALZOBA: This protocol contains serious security issues which might cause issues on the GDPR, so I think they either should be discussed together or not at all.

DENNIS CHANG: I see. That's a good suggestion. Maybe we'll discuss it together. Okay. I think we're going to close the topic list for now. So the next thing we're going to do is, with a show of hands, very quickly run down the list and vote on the topics that you would like to discuss here before we run out of time. And you can vote more than once. So, let's start.

Naming services portal, raise your hand. Start counting. Got it?

Okay, next. CZDS. Raise your hand. Okay.

Next. GDPR. I'm almost afraid to say it. There's not that many hands actually. You got it? Yeah?

Next, TLD-wide HSTS. Wow, surprising. I didn't even know what it was until I got here. I'd like to know.

Finally, DAAR. Alrighty. Did we get it? Okay.

So how much time do we have left, Linett? 45 minutes. So, I would say, we may be able to get through all of it, actually. If we combine the GDPR and TLDs at the end, and we'll just talk about that until we run out of time, I think that will work.

So, let's start with DAAR, and I'll hand it over to the person who raised this topic. Who was that? DAAR. You go ahead and introduce the topic and what it is that you'd like to discuss and questions you might have. Now, this question is not just for the staff, but for the registries here. You have peers and colleagues and who is in the business. They're already doing some things. Some of them are experts at this. Go ahead.

SOPHIA FENG: So, the DAAR project was introduced by [inaudible] and also lead by the CTO, David Conrad. We listened to the presentation this week about the reasons and the backgrounds or the state that's connecting to carry on this project. First of all, from our perspective, I think it's very good that ICANN introduced this because I think the TLD registries are facing tremendous issues with all this ranking that's put on by Spamhaus and that definitely affects their performance in the market because also the browser would not list them if they have a lot of DNS Abuse in their domain space.

So, I got some information, but I also have questions with staff with how quickly this program can be rolled out, and what is the expected timeline. On the other hand, I also have a question for the registries whether you think this project is very useful to you or do you have any recommendation for the ICANN staff, for the project leader? And I think the later point is, is there any area that the registry thinks would be worthwhile to discuss in terms of encouraging the registry to do something about the domain abuse. So, I see hands for Maxim.

MAXIM ALZOBA: Maxim Alzoba, dotMoscow. One of the things about DAAR is total lack of communication with the registries and registrars. The other important thing is no, delivering PR speeches is not communication. It's just PR speech one way direction. Despite suggested communications with registry constituencies and registrar constituencies, nothing happened since Madrid. That's the first point.

Second point, we shouldn't mix the definition of abuse and blind trust to third-parties without any kind of proof because the Spamhaus for example is well known for aiding things. We have nothing to do with spam today at that base. They're adding DNS infrastructures there, which is not used to send spam, and DNS infrastructure is something relevant to stability and security. It's not a good idea to help in developing -- we face a situation where these such companies are trying to influence registries without any proof. Basically it's demanding that, “You have to trust us because we are everywhere.”

And I always thought that the community based approach in ICANN is about mutual consultations, sharing of opinions and not a one way top down direction. Until this database contains proofs, registries and registrars cannot use it, and even ICANN Compliance cannot use it because if ICANN Compliance comes to us and says, "Okay, you have pike of 1.5 persons of abuse here," the first thing I ask is, "Please provide me the clause in your contract saying that we have to listen. Please provide us any kind of proof so we can try to investigate it."

For example, Fish tank, they have at least snapshots or screenshots and it can be used, so yes, we say that bad things happened in the past and we have to block it because we can in our anti-abuse policy, but we have inclusion of some URLs in the database without any kind of proof which has nothing to do with our anti-abuse policies because the first thing we ask is properly identify the abuse.

So, I understand that it's a notion to have an understanding of the temperature in the room, but it could lead us into a situation where we spend a lot of funds, ICANN spends a lot of funds, in something which has scientific interest, like, "Wow, how much views do we have?" What can we do with it? And situations where they're too great which is basically useless for registries and registrars and even ICANN Compliance is something we could be at risk in the financial planning section of public comments. Thank you.

DENNIS CHANG: Thank you, Maxim. Anybody else have a comment?

MERT SAKA: Dennis, we have a question online from Jim Prendergast from the Galway Strategy Group. His question is, if all this threat information is already available, what problem is ICANN trying to solve with DAAR?

DENNIS CHANG: Yes, that's what I was going to ask. Anybody from OCTO team? Who was at the DAAR's session? You were?

MERT SAKA: We don't have anyone from the OCTO team. I don't think we can answer the question right now.

MAXIM ALZOBA: To add more, the session of DAAR was made at the same time when registries and registrars met so, basically, they were not able to attend. I hope it was just coincidence.

DENNIS CHANG: I see. So, if there is no one else, from what I understand about the DAAR, it was an effort to collect and consolidate abuse information that's already public and make it convenient for you to use. Now, what I'm hearing is that the communication of that project was uni-directional and you'd like to have a dialog about it, and the DAAR session was that session that was supposed to be used for that, but unfortunately, it was in conflict with your registry session, right? And registrars too, that is unfortunate, so we'll take note of that and make sure that when we do our next session on the DAAR, we'll let you participate. Go ahead, Russ.

RUSSELL WEINSTEIN: Thanks for the questions. I think these are good ones. The one I think we can help you with the most in this session, given the attendees, is the lack of feeling like you had participation and dialog with the team that was helping develop this product. So, I think that's the main takeaway for me, is that we need to do a better job as ICANN of connecting the right stakeholders before implementation of a project like this, and I'm happy to relay that back and create a forum for the team developing the DAAR to interact with you guys, and I think they're looking forward to that too, actually, based on -- I attended bits of that session.

So, I think we can help connect that and create that, and I think we don't have to wait until the next ICANN meeting to do that, maybe we can create some sort of webinar that's more a workshop discussion type format, if that would be agreeable for all of you.

DENNIS CHANG: Any other comments on DAAR? The one question that you asked was, did the other registry find that useful in any way or helpful? Does the other registries have any experience with the DAAR, or are you aware of the DAAR? Used it? Looked at it? No? I guess that sort of goes to prove your point, that it wasn't very well communicated.

So, I think Russ is taking the action to do something about the communications and sharing of the DAAR, so maybe after that we can talk about how useful it is and what we might be able to do to make it more useful for the registries. So if there's no other comments on the DAAR, we're going to move to the next topic, which is Naming Services portal. Who brought this up? Go ahead.

DIETMAR LENDEN: Thanks, Dennis. It's Dietmar for the record. What I was trying to get at there was the terms and conditions part plus the new piece that I found out yesterday or we all found out yesterday about the CZDS potentially being moved from an approval perspective into the Naming Services portal.

So, I'll start on the terms and conditions piece. Have you guys been able to have a chat with the registry individuals within the registry group with regards to the terms and conditions? I think it was yesterday, there was an indication that there would be an attempt to set up a meeting during the course of the next couple of days to have a little bit more of a chat about the redline of the terms and conditions.

And then, just curious how the CZDS access approval piece is actually going to work. Will the existing CZDS portal remain as is for requestors, so the requestors would go to the CZDS portal, and then if we are not in the Naming Services portal at that stage, can we still utilize the old or existing CZDS portal to continue to approve requestors?

And also, I guess following on from that, do we have to use the Naming Services portal to approve requests that are coming through for CZDS? Hopefully, that was all clear.

RUSSELL WEINSTEIN: Thanks for the questions. This is Russ. I think I can answer most of those, but I might need to turn to Mert, who's our CZDS expert for more detail on that, but in terms of Naming Services portal terms of use, we are still attempting to connect with the group. I've got some emails out looking for available time slots with the group, so we're hoping to do that either tonight or tomorrow morning, are some of the time slots, and if anybody else feels like they need to be part of those discussions, please let me know, I don't want to exclude anyone. So, that's where we are there.

I don't think we'll be able to get to zero in terms of gap this week, but I think the more we can narrow this week and then tackle the other items as rapidly as possible, because like we've been saying, I want everyone up and using the Naming Services portal as soon as possible. It will really help accelerate our ability to provide better service to all of you.

DIETMAR LENDEN: Sorry, Russ. I just thought of an extra question to do with the Naming Services portal. Are you able to indicate how many registries have actually signed and joined the Naming Services portal? Because that will be a curious number to hear.

RUSSELL WEINSTEIN: Yeah, I remember seeing some statistics, and I don't have them right at my disposal, and I'm not quite sure if it was -- I'd seen some that about 50% of the accounts had accepted the terms of use and signed in, but I don't know if that was terms of use version 1.0 or 1.1, so I think we're somewhere around 50% ish now.

DIETMAR LENDEN: So I guess then the follow up question to that would be, if during this whole negotiation process you end up with this new set of terms of use, I take it all of those 50% or whatever the number was, would have to reagree to those, so they'd be kicked out and then have to come back in again. Okay.

RUSSELL WEINSTEIN: Yeah, I was nodding my head very vigorously for that one. Just like any kind of software update, like when they update it you have to reaccept, and that will be the philosophy going forward.

After a deep breath, we'll take the CZDS questions now. So I think the first one was about access and just to mention, we did try and get this on your radars earlier in the year. I think we presented at a registry stakeholder call that ran out of time back in September because we did want to start previewing this stuff early so it wasn't a surprise, but the idea there is that the registry access piece where you'll be reviewing and approving CZDS on valid requests will be a screen essentially you can access within the Naming Services portal.

You don't have to be the current Naming Services portal user for your account to have access for that portion. So, if you're the CZDS user today, you'll be given a CZDS credential that gets you into that portion of the Naming Services portal. If you happen to be both, you'll have that single credential where you can toggle between the tabs essentially. So hopefully, that answers one of those questions.

I think the other one was about the community side. So the community side is also getting an upgraded experience, and those two experiences will talk to each other, but it doesn't change what you have to do as a registry user.

DIETMAR LENDEN: Thanks, Russ. I just have a follow up question. Will you make an API available, because we look after a few fair brands and it'll be quite nice if we had the ability to draw the information down in one place, and I or an API, work on the requests and then push back the answers into the system to say yes or no, which you can say no, believe it or not. There are certain rules.

So, have an API process in place because the current CZDS process doesn't -- there is an API in the background and we have offered to help with that, but that API is not functioning. It's not doing anything. So, if we could get an API, I don't know if that's something that's on the roadmap, that would be spectacular. Thank you.

MERT SAKA: Thank you for the future suggestion. We don't have an API for the registries right now, only for the end users for them to download rapidly. But, we're working on an API for end users, yes, but we haven't considered yet about the registry site.

What I can say about the new CZDS for registries, and also the users, is, we're mainly moving it to two different platforms from the existing platform to be able to add these kinds of features. So our intent with the change of platforms is not to add new features but to make it work better for you first off. Then, we'll be able to add new features, just like the one maybe you suggested. So, I'm taking notes. Thank you for your suggestion again.

SOPHIA FENG: Sophia for the record. So, I have questions on the supports on the Naming Services portal. So, a couple of registries that we supported all received emails to access this NSP, but because of the time differences, all of the emails expired, all the links expired. Then they have to require to reset the password and they send the email to Global Support, but without two days there's no response.

So, I'm just wondering, what is the SLA right now for the Global Support email for these kinds of issues and is there any SLA for the moment and what is it, or maybe if it doesn't exist, then we probably need to create some. Thanks.

MERT SAKA: Thank for your question. We actually have Michaela here, director of Global Support in the room and she's going to answer.

MICHAELA QUINZY: Is this microphone on? Okay, great. Michaela Quinzy, ICANN Org. In general, our SLA is 24 hours. As you can imagine, with the roll out of the NSP, we were a little bit overwhelmed in the beginning, but I think we're back to our normal standard of response within 24 hours.

SUSAN PAYNE: Hi, Susan Payne here. This is just a question about the proposal to move the CZDS approval stream into the naming portal. As you know, there's this issue at the moment with the terms and conditions. I know that's being worked on, but I'm being realistic here. Can you give us an assurance that you're not going to turn off the other CZDS access for us, because obviously, responding to CZDS requests for access is a compliance issue for registry operators and if we are unable to access those requests because we're not willing to sign up to your Ts and Cs, then that's an issue for us.

RUSSELL WEINSTEIN: Thanks for flagging that. That's a really good point of continuing that we need to make sure we get you to accept the terms and conditions before the cutover.

SUSAN PAYNE: Absolutely, and you can't do the cutover if we're not willing to accept them, because that's a contract of adhesion and we're not signing up to something we're not willing to sign up to.

RUSSELL WEINSTEIN: Okay. Noted.

CRYSTAL ONDO: Crystal Ondo. For those registries that automatically approve all CZDS requests, can we get a beta test so that we can build out something on our end that will do that for the new portal? Because that's how we're managing now.

DENNIS CHANG: Did you take the request, Mert? Okay, noted. Okay, go head, Maxim.

MAXIM ALZOBA: Maxim Alzoba. Comment about this. Actually, the registry agreement says that we have to use it, but it should be facilitated by the so called CZDS provider. If the provider fails to facilitate it, and since we're not affiliated with ICANN, it's not our fault and thus we don't have to approve any CZDS requests. Thank you.

DENNIS CHANG: Interesting take. Any other comments on CZDS? Okay, one more. Go ahead.

DIETMAR LENDEN: Sorry, I'm going to just jump onto the GDPR piece; I've asked the GDPR to go on the list, but I actually was asking more about the CZDS. Has ICANN thought about that piece? Because obviously, people are coming in there and you're asking them to provide personal informational to you, and then that gets passed on to us, and then we go away and do what we do with that. Just to be clear, I'm in the UK so this will affect us, so I'm just curious as to, is that part of your discussions on GDPR at the moment?

RUSSELL WEINSTEIN: Yeah, from my understanding, we are looking kind of at all the systems that we're taking in data and taking it into account. And just to be clear on the timing of CZDS, this is not something that's coming next week, next month. I think we're looking right now in the second quarter 2018 timeframe. So hopefully, terms of use is long resolved.

DENNIS CHANG: Anything more on CZDS? No? Okay, go ahead.

RUSSELL WEINSTEIN: I just wanted to ask one more question back to the group. I heard Dietmar's request for an API for registry users. It's always good to have one request, but is that a commonly held request? That helps give us some ammunition in terms of development priorities. Maybe a show of hands.

DENNIS CHANG: There's not many hands, so does that mean…?

FRANCISCO ARIAS: This is Francisco Arias from ICANN Org. I was chatting very quickly with Crystal to understand better their needs, and perhaps there is also another need from what I quickly understood from Crystal to have functionality, and I'm not sure if in the version that is currently is being developed, Mert, this is already considered, is to have an option for those registries that approve all the requests to just have something that they will configure. They press a button and everything, all the requests that come are approved. They don't know even need an API if that functionality was available. But like I said, this is a different thing to what Dietmar said about having an API for those that want to review all the requests.

DENNIS CHANG: Any other comments? No? Shall we move on? The next topic is GDPR and I think we can go ahead and talk about the TLD-wide HSTS along with it if you like. I think we have enough time, right? Go ahead. 20 minutes left. So I think that's ample time. Who wants to kick this off? Whose topic was this? Go ahead.

BEN MCLLWAIN: Yes. I guess I'll just briefly expand on this. Maxim is leaving, but yeah. Again, the basic, sort of main point is that a web server that offers the ability to surf content in HTTPS, it’s only optional security, it's not guaranteed security. And even if you have a redirect from the HTTP to the HTTPS, there's various attacks, any kind of network interception like you recently saw, they KRACK Attack against WPA2. If the browser is not acting as the user's agent and enforcing that secure connection and only the use of a secure connection, then you're always going to be vulnerable to some kind of attacker, an active attacker who has network access.

So, that's the basic idea behind HSTS freeloading and it's been the best practice for web security for over two years now. Most of the prominent websites that use it on a daily basis, like almost all of Google services for instance, are already on the HSTS preload list, so that's kind of a done deal. It has support in all major web browsers.

Specifically, the new thing that I'm talking about here at this ICANN meeting is using HSTS for an entire top-level domain. So rather than just enlisting a single, individual domain name one at a time in this list and that list is now going to tens of thousands of entries mind you, you would list an entire TLD at once. That would provide guaranteed security for every single domain name that's under that top level domain. Every user's browser would enforce that. It would only ever use secure connections. It would never make an insecure connection, and in my view I see that as kind of the next level of evolution of security for the web.

There's one major caveat about this that I'm just going to be upfront and honest about. You can't easily apply this to existing open TLDs that already have many websites because there are many websites out there that are not currently served securely and if you put this on that TLD, you will break all of those insecure websites. So, if you're launching new TLDs or if you have a dotBrand TLD and you can control all the sites on that TLD, then you can easily do this, but if you have an existing TLD with many insecure websites, you'll break a lot of them if you do this. So that's the major important caveat. So, it's mostly a looking forward thing for future launches or for existing, closed and dotBrand TLDs. It's a good option.

DENNIS CHANG: Unfortunately, Maxim had to go.

BEN MCLLWAIN: I can answer his question if you'd like. He was concerned about HSTS leaking privacy information, essentially emulating a virtual super cookie. HSTS headers pre-date the HSTS preload list and that is an additional security header that you would put in the response of HTDP saying, "I'm responding securely this time and remember me so that the next time you request me, it'll also be securely."

By running secure and insecure versions of websites and running a lot of them, the published attack use is 24, you can basically do a different pattern for each different user and based on whether or not they access these 24 websites securely or insecurely, you can essentially track each one that's two to 24 different combinations. You could track a lot of people like that.

My answer to that is, that's true, but that's a vulnerability of the HSTS header. The HSTS preload list solves all this information because you don't use the headers to store the individual information per user, it's just those domain names are all on the list period and the user will only ever access all of those domain names securely and you're never leaking any information by attempting to access insecure domain names because you don't.

DIETMAR LENDEN: Hi, it's Dietmar. This is actually a question in my personal capacity as a user of domain names. It has nothing to do with my employer. Just so I understand this, is this going to then force those users, like myself who happens to have a domain name, to actually get a SSL certificate going forward? Because that's obviously a cost incurrence. You can imagine most of the population in the world that has a domain name, individuals aren't going to want to buy an SSL certificate. Unless I'm misunderstanding this thing completely.

BEN MCLLWAIN: So, you're not misunderstanding. That's what I was talking about, how you wouldn't use it on existing TLDs. So your existing domain names would be say if you can choose to continue not serving them securely if you would like, but if you were to register a domain name on a new secure TLD, then yes, you would need an SSL certificate; and the reason that this idea is actually happening now at all is because we're seeing the rise of services like Let's Encrypt that offer easy, free, no hassle SSL certificates.

FRANCISCO ARIAS: This is Francisco Arias from ICANN Org. That's a great point I was going to mention about Let's Encrypt. At least that's an option where there is no cost and you can have that. In regards to the preload option for HTTS, what about the scalability of that? Do you see an issue? In order for that to happen, I would imagine the [inaudible] operators would have to contact each of the browsers to tell them that they want their TLD to be preloaded. How do you envision that to work?

BEN MCLLWAIN: Excellent question. So, preloading entire TLDs actually is a very important way to help solve the scalability problem because the existing way that the preloading works is it's a big patchwork of individual domain names. At Google, we have several hundred different domain names that are all individually on that list already. The list is tens of thousands strong, maybe hundreds of thousands.

Keep in mind, this list is shipped with each install of every major browser, so when you download like say mobile Firefox or something on your phone, part of the data it’s downloading is that list of all those sites that are secure only, and so by storing lots of individual sites in there, it's a lot of information. And the better way to scale that going forward is one entry for every secure TLD rather than one entry for many different websites that are on that TLD. So this is actually helping to address the scalability issue.

DIETMAR LENDEN: Hi. It's Dietmar again. My Valideus hat on now. So, what do you call that free or cheap or whatever it was called SSL service provider?

BEN MCLLWAIN: Yeah, Let's Encrypt.

DIETMAR LENDEN: Okay. So, in the current environment, we, as an organization and as anybody within the industry, you kind of tell everyone, you only go to a website and purchase something if the SSL certificate is valid or if there is an SSL certificate present.

Now, from the sounds of it, we are now going to have to find a different way to educate people about bad actors because if somebody can go to that company, Let's Encrypt, and get a cheapy SSL certificate, and you're forcing everyone to have SSL certificates, there's no way of identifying who a bad actor is anymore because I can imagine getting a free SSL certificate, there's not going to be too much verification done on the individual that's applying for the SSL certificate.

They're going to just go, "My name is Dietmar Lenden," and give my address and pretend to be me, whereas with a normal SSL certificate in the current process, there is some verification that takes place. So, how is that going to work? You may not know the answer to this question. I'm just throwing it out there.

BEN MCLLWAIN: No, I can answer this question. The answer to this is that the existence of an HTTPS connection -- and in order to do that you need an SSL certificate to handle the asymmetric key encryption. That just means that the connection is encrypted. It does not mean that anyone's identity has been verified and indeed you are right. For Let's Encrypt, which offer real certs, mind you. They're not fake certs. They're not just putting warnings on browsers. They're real certificates. Because they're free, they're only doing validation at scales.

So, obviously issuing a free cert, you're not going to have the resources to verify scanned passwords or something. So all they're validating is that the person requesting the certificate actually owns that domain name. So, it's a lower-level of SSL certificate. It's a basic SSL certificate. It;s only good for allowing encryption of the connection, which is still very important mind you, but it's only good for allowing encryption of the connection. It's not an extended level certificate, so it doesn't give you that green padlock and it does not give you that identity verification.

So there's fundamentally two different issues here. There's basic encryption, which is very important for a large variety of reasons, and then above that, there's identity verification that you know who you're actually talking to. For that second level, you're still going to need to pay for an SSL certificate and talk to a trusted CA that will actually do that identity verification.

DIETMAR LENDEN: Sorry, it's Dietmar. So then the implication is that you've got two SSL certificates. Is that correct?

BEN MCLLWAIN: No, if you wanted the green padlock, then you would just use that one.

DIETMAR LENDEN: So, if I'm going to sell something to the public, I'm going to need to have something that the public feels comfortable with. So the public would feel comfortable with dealing with somebody that's got a verified SSL certificate for example. So, in this case then, potentially, I need to have two certificates. If I'm selling a product. Not for me personally as an individual. I'll maybe get one of the cheapy ones. I'll put your name in, thank you.

On a serious note, with regards to the selling side, people have been trained like Pavlov's dog, we've all learned that if you see the green padlock or whatever other thing comes in different browsers, then you assume that that is a valid place to go and buy something. That's not going to appear, so to have that, you then potentially need to have a second SSL certificate.

BEN MCLLWAIN: Sort of. It’s not that you would have two and use simultaneously. It's just the second one would supersede the first one. The Let's Encrypt certs are free, you want a single command line [inaudible] and it downloads and it sells it automatically. So, it's very low overhead to establish. But this is a problem that already exists, I guess it's not anything particular to do with HSTS.

It's just there's been so many threats against insecure connections that having encrypted connections has become of paramount importance and fortunately, people like Let's Encrypt came along and made it easy so that you can just secure everything. As far as user education goes, even an untrusted identity SSL certificate is still encrypted in the connection, so it's a lot better than the previous paradigm where just everything was insecure. You can't say anything about those sites.

DIETMAR LENDEN: I just have to apologize. I just realized in hindsight, my question was actually pretty silly because obviously the verified SSL certificate will supersede and take over the other one. Don't worry about that part.

STEINAR GROTTEROD: I didn't quite understand why this was reflecting the GDPR, but anyway, I hope you're finalized [inaudible] with your discussion. What I want to discuss with the rest of the registrars is, the way I see it with regard to GDPR is that there is very slow progress in the process scene from the way I've seen it from ICANN's side. I'm just wondering what I will do with dotGlobal when it comes to May next year.

The way I see it today is that most likely the best option for me is to remove part of the WHOIS output which is kind of critical. I'm pretty aware of these elements in the GDPR that are not connected to the WHOIS output, but the WHOIS at least is set to something that is publicly available for everyone to see it, and remove that to be displayed, and thereby go directly into compliance with the ICANN Compliance department.

So, the question is, if ICANN doesn't come up with something that I, as a registry operator, can be in compliance with the GDPR and I'm in limbo, what should I do? I hope everybody will have some sort of opinion that is reflecting of this policy because I don't want to be alone in the room when the elephant comes in.

DENNIS CHANG: Anyone have a comment on that?

RUSSEL WEINSTEIN: This is Russ. I'm not a GDPR expert and I think these conversations are happening at the highest levels of our organization, and as you mentioned, they're progressing at a different pace than what the community is looking for in some cases, but I think where we're at is we're really hoping to collaborate together and even if registries and registrars want to collaborate together without ICANN and see some proposals or get to some actual what do you guys think is realistic to comply with GDPR with the minimum impact to WHOIS and then start figuring out what the options are and picking one or picking multiple, I think is where we're at, but I know what that analysis is from the legal side of what it takes to be compliant is still on-going and challenging.

DENNIS CHANG: Don't we have a GDPR session tomorrow? Is it tomorrow?

RUSSELL WEINSTEIN: Tomorrow, one of the big Cross-Community Sessions in the morning is GDPR.

RONALD: This is Ronald [inaudible]. Just a short notice on the RDAP Pilot related to GDPR. This is the very very last step of GDPR. This is the question, am I allowed to display let's say the email address of a private user? The question that GDPR raises much much longer before is, am I allowed as a registry to store that information?

So the RDAP Pilot will tell us how to format the output. Beyond this, I'm very confident that we will get good examples, but GDPR addresses issues far far further on.

STEINAR GROTTEROD: Steinar Grøtterød again. To my knowledge, this autopilot is going to be finalized sometime next year. Even though if you don't consider any policy discussion regarding implementing the RDAP, I know back end providers, ISPs, that will not manage to actually implement that kind of service within May of next year, so then I'm back in the limbo state again even though there might be a technical solution into that.

MERT SAKA: Dennis, just a time check. It's three minutes until the end of the session, for your information.

DENNIS CHANG: Yes. I think we need to start wrapping it up. Does anybody have any final comments on the GDPR? No? Gwen, did you want to make an announcement?

GWEN CARLSON: Yeah, I just wanted to share with everyone that do attend the Cross-Community Session if you can tomorrow on that. We are soliciting input. And then, I also wanted to let you know that from ICANN's perspective, we have a data protection privacy page set up. If you don't have that, I'll quickly put that into the chat room and this will track all of our blogs, legal analysis, and you can get an update on our activities there.

DENNIS CHANG: Thank you, Gwen. So, let's see. If the registries do not have any more questions, let me ask a question to the registries. How many of you are aware of the framework for a registry operator to respond to security threats, that has been published last week? How many are aware? Just one. Two. Three. That is interesting.

Now, how many of you get the mass emails that we put out that went out to announce this? How many of you are on that distribution? The same people. So, it seems like there are a lot of people who are not aware that that's there already that you can leverage. This is an important document that you can all use and it's related to DAAR.

The other thing that I want to let you know is, there is a IGO/INGO policy implementation coming this month, in November probably. Please look out for that, because that is something that registry operators must take action on, is say identify your protection for the IGO/INGO, part of the policy that the board had adapted.

Now, before we conclude, I'd like to give the floor to Russ to close out this session. Go ahead, Russ. You all know Russ is my boss, right? So, be nice.

RUSSELL WEINSTEIN: First, I want to thank Dennis for emceeing the event as he's done many times for us before. It always really fosters communication and participation from all of you and that's the other piece I want to thank. Thank you for coming. Thank you for participating. I learned a lot and took a lot of notes about things like CZDS and how the terms of use and GDPR connect, and a little overwhelming in the moment but we'll figure it out together.

So, I just want to say thank you, and if you have concerns, please don't feel frustrated. Please share them so we can start working through them together because that's what we're here for. We want to support you all in compliance with your contracts and get through some of these tough issues as a team. Thanks, everybody.

DENNIS CHANG: Thank you all.

[END OF TRANSCRIPTION]