ICANN69 | Community Days Sessions – ISPCP Outreach: Impact of COVID-19 on ISPs, DNS, and Connectivity Providers
Thursday, October 15, 2020 – 12:00 to 13:30 CEST

ANDREA BECCALLI: Good morning, everyone. Welcome to the ISPCP outreach session. I'll ask Magali if she can put up the general slides to introduce the session. Thank you. We look forward to a one-hour-and-a-half to go through some of the most interesting topics in what's the COVID crisis brought to the Internet infrastructure, very high-level panelists, speakers that will go through their own experiences from the industry point of view. We'll have a technical run through from ICANN, and we hope that you will find the session engaging and you would join and participate. It's an outreach session, so our goal is to have you ask questions, interrupt when you think you want to know more or make your case, and have you joining this community in ICANN.

I'll let my colleague, Chris Mondini give just a few words of introduction as well, and then we will go into the core of the presentation. Thank you. Chris.

CHRIS MONDINI: Thank you very much, Andrea. My name is Chris Mondini. I'm vice president for stakeholder group engagement at ICANN and the managing director for Europe. So greetings from virtual Hamburg. For

me, it's actual Brussels. But I'm pleased to welcome you at this session and very pleased to welcome the participants.

As I've said in other sessions, ICANN is the organization that coordinates the addressing system's unique identifiers, domain name system that keeps the Internet global and expanding and whole. And we do that through a number of partners, and many of the partners are here today, very important connectivity providers, ISPs, telecommunications companies. They are vital for the functioning of the Internet and the functioning of the DNS.

So I want to thank you for being here and thank them for presenting to us. The title slide is a little bit misleading because we have enough time to cover not just some impacts of COVID but also some emerging technical and technological trends. So please stick around for both halves of the session.

Now, to just give you some logistical information, you may have seen already in the chat the session is recorded, it is archived. We follow the ICANN rules of behavior in the sessions. And most importantly, to ask a question—because the chat can be very active—we ask that the questions or comments submitted be preceded with QUESTION or COMMENT and that lets us know to read them aloud. If they're not bracketed by these QUESTION or COMMENT labels, we'll consider them part of the regular chat. You can also raise your hand to be recognized during the Q&A sessions. So, thanks to all, and back to you to keep us going. Bye.

ANDREA BECCALLI: Thank you, Chris. Okay, so Magali, if we can go quickly to the next slide, we have just a run through of the agenda. You will see it's a quite packed agenda. And it's true, the impact of COVID-19 is not the only subject, the title is a bit misleading. We also must say that these days, there is basically nothing else that escapes from COVID in all aspects of life. So it's difficult to not put it on this topic. But it's true, we'll look into other aspects and see how COVID maybe open up the lead to something [inaudible] happening and not everybody was seeing.

Now I'll pass the baton to Wolf-Ullrich, who is the vice chair of ISPCP. He will give us a short introduction and welcome and present the rest of the session. Thank you. Wolf-Ullrich.

WOLF-ULLRICH KNOBEN: Thanks very much. My name is Wolf-Ullrich Knoben. I'm the actual chair of the ISPCP constituency elected until next year. So, as many of you know, maybe guests do not know, that the ISPCP constituency is part of the GNSO within ICANN and we are representing those who have an interest in telecommunication areas and telecommunication infrastructure and ISP provisional services and activities.

So we had—this is not the first time that we do an outreach event at the occasion of an ICANN meeting. So we did it several times in the past, but it's first time that it's virtual due to the situation we have. And from our past experience we had in several different countries, areas, regions—the last one was in Japan—we had good reactions on

these things. We tried also to cover items particularly of interest for the region where the ICANN meeting was taking place.

In this time, also you will see that we have for the first part with regards to the COVID impact, we have also a presentation related to what is happening in Germany.

So in addition, we have an item to cover with regards to an outlook to the technical future of identifier technologies and what's going to happen there.

I also invite you to use the chat and to use the Q&A possibilities in order to place questions here, and I wish you a good meeting. I hand over in this regard to the first one who is going to give a presentation with regards to impact of COVID 19, which is Lars Steffen. Lars, please introduce yourself.

LARS STEFFEN: Yes. Thank you, Wolf-Ullrich. My name is Lars Steffen, I'm with ECO, association of the Internet industry. I'd like to give an overview of the economic impact of COVID-19 on the Internet industry. So I would proceed now to share my screen with you.

I hope it is visible now for you, first slide. We do every five years a long-term study on the economic outlook of the Internet industry in collaboration with Arthur D. Little, and this is already the fourth edition of this study where I would like to give you some overview of

the highlights based on interviews with C-level staff, primary and secondary sources.

This time, of course, we've been interested in the long- and short-term effects of the COVID-19 crisis because a lot of our members were asking in the beginning of the year what impact does this thing have on our business. And of course, as an association, we've been interested in this question as well. And to be sure, this crisis has already taken longer than originally expected, so it's still quite an interesting insight, what I can show you right now.

So to understand what I will show you in the following slides is that we have a model of the Internet industry that's based on four layers. Those four layers begin with layer one which is basic network and infrastructure like colocation and housing, backbone operation, and also the operation of access networks.

Based on that, we have the level two which includes nearly all as-a-service offerings but also webhosting and domains. On top of that, we have the aggregation and transaction layer which includes B2B and B2C ecommerce and billing and payment, and on top of that, smart industries and paid content that you can consume via the Internet. And the idea is that the higher the layer, the industries rely on the services and applications that are delivered from the layers below.

So, but now we come to the actual effect of COVID-19. So the whole study is having primarily focus on the German market, but experience from our previous studies show that typically, the trends are also

applicable to most European markets, and due to the fact that the Internet industry is highly interconnected, I think the basic trends are also applicable to other regions around the world.

The basic assumption before the COVID-19 situation kicked in was that the Internet industry in Germany would grow from 2019 to 2025 by roughly 9.5% per year. And that was the estimation calculated before COVID-19 was surfacing. And so Arthur D. Little and ECO had to do some adjustments to this prediction.

So what you can see here, that instead of growing by 9.5% from 2019 to 2020, that we see a decline in growth. And when you take a closer look on the right-hand side, you can see that there's a difference in the layers that are affected. So you can see that layers on, two and four are still growing even in times of COVID-19, but that the real slump is indicated on the layer three which is mostly affected by the COVID-19 situation.

So this includes payments, transactions, advertisements, but also travel and transportation bookings which are taken into consideration why this part of the Internet industry would suffer most.

This next slide shows you a little bit more in detail on the left-hand side the development on the time level. As you can see, the whole industry will see a decline in 2020. That will also have an effect on 2021 and into 2022. But on the long term, we expect that this will catch up and will lead into a little bit higher growth of the whole Internet industry than was predicted before due to the fact that we see a higher

demand of basic infrastructure due to home office and homeschooling which has an impact on layer one. So there is just a very small decline in 2021 but then growing steadily due to the higher demand in the future.

On layer two, you can see there is already growing strong during the crisis and remaining on a higher level of growth. For the level three, you can see that it's having the strongest impact of the crisis and pulling down the overall curve, and level four, you can see the same negative impact but that will be compensated in the next one or two years with a smaller growth as well.

What is maybe still interesting is to have a more detailed look which subparts of the Internet industry will be affected, just on a temporary scope and also on a sustained growth. As I already indicated, there are parts of the industry that will only have a short-term impact by COVID-19, and some of them will have a longer impact by COVID-19.

And as you can see with the red dots, the basic infrastructure on layer one is affected at least from all sectors of the industry, and those who are affected the most are the layers three and four which are actually based on transaction on the B2B level but which also rely on bookings in the travel and transportation industry.

But for the rest, as you can see, there is a growing demand, for example, for entertainment services which are on the top right corner of this graph, and also when you take a look at services that provide

online education and also medical and healthcare services, they are growing strong already in the COVID-19 situation.

So this is just a basic overview of the study and what we have found out in surveys, studies and interviews on the impact of COVID-19 on the Internet industry. If you're interested in a more comprehensive overview, I can put the link to the full study in the chat of the session. and I hope that you find these insights useful. I'm looking forward to questions, feedback and discussion. Thank you very much.

WOLF-ULLRICH KNOBEN: Thank you, Lars, very much for that which gave us a brief outline of what's happened and is going to happen here in Europe based on certain assumptions, I understand, and [we all do] understand these assumptions maybe will have some questions later on with regards to that. But before we come to a question, to your part, I would suggest that Esteban from Argentina is going to give his presentation right now, and after that, we could then summarize and go to the questions. Esteban, please go ahead and introduce yourself.

ESTEBAN LESCANO: Hi Wolf-Ullrich. Thank you very much. It’s a pleasure to be at this outreach session. My name is Esteban Lescano. I work for CABASE which is an Internet association in Argentina. I am the head of the commission of legal and public policy issues.

Let me share with you a presentation. I want to talk about policy and regulatory impact of COVID-19 on ISPs. And as I'm from Argentina, I will show the situation in this country.

To begin, let me take a glance to Argentine ISP figures. Argentina is a country with a population of 44 million people. We have more than 1200 [fix] ISPs, mainly SMEs and cooperatives. CABASE runs an Internet exchange point network with 31 points all around the country. The Internet penetration for fix access is 62.8. We have only 12% of fiber optic in houses, but this level is increasing year to year. The average speed is 37.5 megabits at the country level. During the COVID-19, the traffic increased 35%.

But one characteristic of Internet access in Argentina is the unequal distribution between main cities and province towns and rural areas. This situation combined with the crisis of COVID-19 increased the demand for regulations in my country. Beginning with the government who with this pandemic begin to think about price regulation, also in prohibition of suspension in case of nonpayment or late payments.

On the other side, also the public opinion willing to talk about Internet as essential service due to the lockdown and the necessity of home office and home schooling. Also, a push for improving quality and bandwidth, and also requesting an affordable price.

And one important thing that public opinion begin to ask for a legal declaration of Internet as a human right. In my country, it began a

discussion about if Internet is a human right, then it has to be free because human rights are free and for everyone.

Also, ISPs request new claims from users in case of technology updates and also more bandwidth, and also to pay less due to the economic crisis generated by COVID-19.

From the workers and labor union side, well, the workers ask ISPs to keep safe at home, request special [kits] of protection, and also request to establish rotating shift and small worker teams.

All that situation push the ISPs to adapt and to solve all these problems with the aim of continuing with the services to increase the quality, to give the service that users, governments, public opinions claim, and was not easy.

But the result of all these forces pushing on ISPs was that the government passed a new regulation that declares Internet access a public utility via presidential decree, and also, these new regulations establish that ISP prices for every service, not only for final users, will be defined by federal government, by regulators.

Also, this presidential decree establish that government will define a minimum mandatory service for ISPs in order to cover a minimum service for all the people all around the country. Also, the government approved regulation with the prohibition of service suspension in case of nonpayment for vulnerable users.

As a conclusion of this new regulation, we have now in Argentina more governmental intervention in ISPs' activity. It is still an open market, but under the rules of public utility service like gas or electricity or water.

Let me say that, however, with a positive and optimistic view, we think that—well, all crisis bears opportunity, and then government has to write and approve secondary regulation for ISPs and other ICT services. ISPs trade association, CABASE, have filed into the government regulatory proposals that reduce public utilities' impact while ensuring continuity of service to users because we understand that a full scheme of public utility for Internet access will be very negative.

Then we are requesting an asymmetric regulation to preserve and boost SMEs and ISPs and cooperatives to set up new conditions for investment and provision of connectivity services in the country. Currently, we are waiting for the regulator answer.

As a conclusion of all this very quick review of the regulatory situation, in my country, we can say that the COVID-19 brings new rules for ISPs and we must adapt to them. Those rules are not much positive, but we are confident that government will reduce its negative impact via secondary regulation and these secondary rules may create new opportunities for ISPs in Argentina. Thank you very much. I am here to answer questions or to begin to chat about this specific issue. Thank you.

WOLF-ULLRICH KNOBEN: Thanks very much, Esteban. That is really an interesting aspect, regulatory aspect that at the time being, we don't have to take great care here in Europe about, and Germany, not in this respect. So we will have this in the discussion afterwards as well.

The last presentation is done by Adiel from ICANN. Adiel, please go ahead and introduce yourself.

ADIEL AKPLOGAN: Thank you very much, Wolf-Ullrich. I will quickly take you through the impacts of COVID overall on the infrastructure and give a brief overview of what ICANN did, particularly in terms of measuring some aspects that are relevant to us. I'll try to share my screen now.

WOLF-ULLRICH KNOBEN: In the meantime, I have to look at the time. I'm sorry to have to say that, but we have to take care about consuming time. You have several things to cover. Thank you.

ADIEL AKPLOGAN: Okay. I'll be quick. Okay. So for the sake of time, I'm going to quickly present what I will talk about. So from the ISP infrastructure point of view, you know the COVID has been a very unique situation where we had a global situation where everybody was locked down and the demand for online activity has grown significantly. And that has been

also measured by many ISP who have noticed increase in the traffic that they're handling from 20 to 30%, in some area, even 60%.

One interesting thing that was noticed as well is the change of traffic pattern. Downtowns in country has seen decrease in the traffic while suburb areas, residential area has seen an increase. And also, the peak time for most of the ISPs have also changed. Usually, it is from 5:00 PM to 11:00 PM when people come from office. Now it is really from 8:00 AM in the morning to 11:00 PM because people work from home and then when they finish, they use the Internet for other stuff like watching a movie and so on.

So those impacts have been visible, but overall, most of the infrastructure in the ISP have hold its [inaudible]. They have been able to provide the infrastructure and the bandwidth to allow the Internet to continue to serve. We haven't see any major collapse of the Internet in general. Even though the speed has been impacted here and there, most of the ISP infrastructure has been able to cope with this.

Another aspect important to notice which has been measured and reported by some ISPs and vendors is the increase of the denial of service attacks. Because people see a lot of traffic, people see opportunity as well from connectivity from home permanently from what exists before. So that has increased.

But all of that has not shown any disruption at all on the infrastructure globally, and that is a good thing from our perspective because it

shows that the resiliency that has been built into the Internet has been very effective.

From ICANN perspective, we have looked at two specific aspects. Very early of the lockdown, we have done a study which we published the result in OCTO document 08 to look at the impacts of the lockdown on traffic to the root server. We studied specifically the root server host in Paris because at the time, the lockdown in France has been very abrupt so the events were very quick. So we can clearly see the difference between the before and after lockdown.

Overall, that study has shown that the traffic at the root server has increased, and following the pattern that I mentioned before, around 30%. What is also interesting to see, which confirms what many people have observed as well at the root level, is that the proportion of negative answer from the root server and actually existing domain has not changed. The proportion remains the same. If you look at the graph that is there, the orange represents nonexistent results from the root server which constitue the majority of the traffic, which we call kind of noise at the root server level.

The proportion of that against actually positive response has not changed either. So both of them has increased of about 28%. So that actually was reassuring for us, to see that there is an increase but that increase has not had any significant impact on the operation of the root server that ICANN manage, which is IMRS in general. You can read the full report online on the ICANN website.

Another thing that we study during that period is to kind of assess if the COVID situation has had an impact on abusive domain name registration, and there again, our research team has looked at domain names that were registered during that period, look at those who may have any link with COVID using name and comparing. And from that list, look at those who have some kind of abusive report from different reporting and abuse database feeds and see if there is any negative reports.

Roughly from about 121,000 domain names registered during the period of May to August, 8000 had some reports that indicate that there may be something happening, and from that, only 1700 actually warranted a second look. What that means is that there is not only one report but more than one, so there is actually something happening.

So it pushed the team to look a little bit even closer to what is happening and see if it is actually report or if it is just because the name may be a non-English-language name and it's not something that is [inaudible] or the registration pattern is not good.

And after looking deeply at that, only 126 actually was reporting. All of this to say that although the situation has triggered a lot of legislation around the COVID situation—the next slide will show exactly what was measured—not very much actually has an abusive behavior.

And why we did this is not to actually take any action or police this thing, but only to see if there is an impact on the registration, and also

provide some additional support to the registry and registrar so that if there is action that needs to be taken, they can do that.

This initiative actually has evolved into a more permanent initiative where the research team will constantly look at the registration trends and try to analyze what we see there.

So, what are the names that were analyzed? From everything that was collected, we can see that domain name registration with keyword like mask, COVID, and corona were about 73% of all those kind of "abusive" domain name that were analyzed.

What is interesting as well from the findings is that there is a significant number that matched non-English terms which again shows that with the COVID situation, with the lockdown, all IDN-related registration has also raised during that period of time.

So those are the two aspects on the infrastructure that ICANN specifically studied. Both of them have shown that the impact of the COVID overall is not as negative as we have imagined, even though the situation was new and has changed a lot of our old behavior, individually and from corporate perspective.

Thank you. That's all I will say. Happy to further discuss this.

WOLF-ULLRICH KNOBEN: Thank you very much, Adiel. Thanks for this comprehensive and short enough presentation. That sets the scene here for question and answers. I would like to encourage also participants from other

regions like if they are available from Asia and Africa for example, well, to share experiences or views form their side, what is happening in these regions. So it's open. Andrea, would you like to guide us for the Q&A, please?

ANDREA BECCALLI: Thank you, Wolf-Ullrich. Yes, we have now some time, seven minutes, more or less, to go through some questions and answers. There have been some very interesting presentations and points to reflect.

I've seen some questions on the chart, so I can read them. This one is for Esteban, from [Shinya Masaki,] "As far as I remember, you mentioned ISPs requesting asymmetrical regulation. Is that for a few dominant ISPs?"

ESTEBAN LESCANO: Thank you, Andrea. I was asking him saying that the idea of asymmetrical regulation in this context is to consider the special situation of ISPs which are SMEs and cooperatives in issues like scheme of cost, also in geographical location inside our country, and also, the technology used, because it's not the same. If you're a wireless ISP, fixed ISP or a satellite ISP, that is why we are asking to the regulator to consider all these differences at the time of passing the secondary regulation that is needed in order to complete this public utility declaration for ISPs and all ICT services in Argentina.

ANDREA BECCALLI: Okay. Thank you. Indeed, what you just presented from Argentina, from European perspective, is actually very interesting because there has been similar discussion in different countries in Europe, but none of them have been able to go that far in putting regulation at that level. And I wonder what will that—and how that will be dealt by the industry here.

Okay, so we have another question from Paulos Nyirenda to Lars on the chat. "With regards to mobile versus fixed Internet access, last slide or figure eight in you report, the situation in my region, in Africa is the reverse. Temporary decline has been observed in fixed while mobile saw more sustained growth. Seeing fixed served institutions which were forced to lock down while mobile faced less lockdown effects. So, what is the reason for this in Germany?"

LARS STEFFEN: Thank you very much for this question. First of all, the data that I showed on the slides has been produced in the first half of the year, in the beginning of the COVID-19 situation, so most of the data has been trying to predict how this situation will develop.

But coming back to the question, which is quite interesting, so what I can say is in terms of fixed Internet access, that this also affects the current situation homework and home schooling, which is primarily based on landline connections, at least in Europe, and that also when it comes to home office or virtual office environments, that people are

using IP phone lines for communication and less mobile communication.

So this pattern of behavior may explain that we have strong growth of fixed Internet access networks and maybe show a little decline and also a temporary decline in mobile access networks which has been predicted in the beginning of the year.

But I have to admit it will be very interesting to have another round of surveys and interviews to see how the actual development has been throughout the last weeks and months to double check if this prediction has been conducted in the beginning of the year reflects the reality. Thank you very much.

ANDREA BECCALLI: Thank you, Lars. I don't see any other question. Is there any question that any of the participants—you also can raise your hands and intervene. If not, I do have one for Lars. Please, Wolf-Ullrich.

WOLF-ULLRICH KNOBEN: Yeah, it's just myself. One question to Esteban, because that situation seems to be very strange, I would say, so what you presented is that it's the ISPs and the providers, [inaudible] providers, network providers are under high pressure right now to cover the requirements coming from the government and from others. And I wonder how that could happen. So, in Europe for example, the European community, you have big financial programs and supporting programs for all the

economy. Is that going on in South America and in Argentina as well, that there is some light at the end of the tunnel?

ESTEBAN LESCANO: Thank you, Wolf-Ullrich. Yes, there are many programs of economic support, but there is a very curious thing that those programs are not for ISPs because as Internet is considered an essential service, that is continue at full velocity during the COVID crisis, the ISPs are not eligible for this kind of economic support. That is why we are very worried about these new rules, about declaring Internet access as a utility service, because we have all the obligations and less or just a few rights connected with this declaration. That is why we are also waiting for the secondary regulation that we need, that we understand is necessary to correct and adapt, and in some way, make less hard this public utility declaration.

ANDREA BECCALLI: Very interesting, Esteban. Do you see similar initiatives being implemented in other countries in Latin America, or is this something that only Argentina has been ...?

ESTEBAN LESCANO: No, I think that in Argentina, it was a very big debate about this issue, but I'm seeing other countries, for example, in Chile there is now a discussion at the congress level about if telecommunication services have to be a public utility or not, but in that case, it's just, we can say,

the title of the service, not the full obligation and the price restriction as in the case of Argentina.

But not in other countries, not in Uruguay, not Brazil, not Colombia. I think this is a very focused situation in Argentina when the governments understand that as traffic is growing and business is going well, then they have to pass a deeper and stronger regulation about ISPs and their services.

ANDREA BECCALLI: Very interesting to learn. Okay, I see two questions getting in. We are actually just at the end of the question time, but we're going to just take a couple more and then keep them for the rest. From Banface Witaba, "What has been ICANN's response to this impact? Is ICANN providing relief to registrar [inaudible] fees? Also, any plans to set up a special fund to support ICANN-recognized registrars?" Adiel, do you have more information on that? We did some really ... But I'm not confident on all the details.

ADIEL AKPLOGAN: Hello Andrea. Yes, I think there's been some relief for those registry and registrar who requested it, but overall, there hasn't been much impact, so I don't think there are many of them who requested that relief. But the detail, that is more from the finance department than [I or you.]

ANDREA BECCALLI: Thank you. Bonface, we can get you more details about that. At the same time, your question made me think about—I think it was Lars when he presented the sustained or temporary impact of COVID, and at one point, I remember that webhosting of domains did have a growth.

And that's something that definitely is shared in Europe among the ccTLDs. Some of them saw double-digit growth that they'd never seen before. The question is also for how long that will go, and if it's temporary or if it's going to stay. But we can give you more details about that.

Okay, I see that Esteban responded to the other question from [inaudible]. So we can now go to the second panel which will basically help us to look forward on the horizon. We now have a clear idea what's going on or what happened in this last month, but that's not all. Actually, there is more to come, and quite interesting development. And for this panel, Christian Dawson will take you through four presentations and very interesting topics. It will be technical but we'll make sure that it's not too technical. We want you to have a good understanding of what's going on in the technical landscape. Thank you, Chris. Over to you.

CHRIS DAWSON: Thank you, Andrea. I appreciate it. Thank you for your time today. I'm very pleased to be able to walk us through emerging issues in Internet infrastructure. This event is designed to showcase not just the issues

that are happening on networks around the world, but hopefully, we're going to close by talking about the role of the ISPCP within ICANN representing the views and interests on topics related to emerging technologies, the domain name system and the related impacts on ISPs and connectivity providers.

We have four experts here that are going to walk you through some of the emerging technologies that are out there right now. I think that it is appropriate, after we talk about the effects of COVID, to talk about the effects of changes to networks, because when you're talking about what's going on right now, COVID's not the only thing that's affecting the networks that we as ISPs are managing and maintaining throughout the world.

Obviously, technology is moving forward and we've got to keep abreast of changes to those technologies and be involved in the important conversations around how those are able to change.

One of the ways in which we can be involved in that is to get people from technical communities and ISPs to join the conversations that are happening at the ISPCP.

A really quick background, my name is Christian Dawson, I'm executive director of a trade association called the I2Coalition, but I'm also on the executive committee of the ISPCP. This is designed as an outreach campaign in part to [grab] ISPs who are not part of the ISPCP and introduce them to the idea of getting involved in our community.

So hopefully, you're enticed by some of the things you hear to go ahead and reach out to us and get involved. We're going to start by introducing our four panelists real quickly and then we'll jump into short presentations and statements from each panelist who will talk about the things that they're involved in from their perspectives on emerging issues.

And the first one that we're going to introduce is somebody that you have already seen today, Adiel Akplogan, vice president for technical engagement at ICANN who's already talked to us about what they've seen at ICANN from a perspective of COVID response. But Adiel, you've done a really interesting report on issues surrounding emerging technologies in the DNS, and we would love to see what you have for us today.

ADIEL AKPLOGAN: Thank you, Christian. Well, for this panel specifically, our input is going to revolve mostly on what we see on the encrypted DNS front. I have one slide. I don't know if it's worth showing it.

In short, what I will say is that on the front of encrypted DNS, we know that DoH and DoT has been standardized a few years ago. That is done. They are technologies that are being in use now.

DoT is getting implemented [widely,] people are using it. There is not much questioning and [inaudible] around DoT. DoH, however, continues to raise some question, but I must say that sine the early days, implementation, things have significantly evolved since then.

More and more people are implementing the protocol, more and more, they're learning and trying to address some of the concerns raised originally which are mainly from ISP perspective the risk of user evading some local and internal policy related to how the DNS is used and concentrating DNS traffic to remote DoH server.

This s been tackled from different manner. Even the IETF point of view, there are discussions on the way right now to ensure that DoH service is discoverable and provided by ISP, they can push their own DoH server discoverability to their customers so that it's set up for the customers and not used DoH server that they have no control of.

From our perspective at ICANN, our position has not evolved that much on this area. We continue to keep a kind of independence when it comes to technology standard, because if the technology is [inaudible] it will be picked by vendors, ISPs and so on an deployed, what we pay more attention to is the impacts of the implementation of those technologies on the security and stability of the DNS.

Early in the adoption of DoH, sometime last year, we have done a study and published a document, OCTO 003, that actually lay out some of the question we have, some of the potential implementation impacts of DoH, DNS encryption in general on the infrastructure. Most of the findings there have been taken on by the IETF as well and a lot of work is being done to try to address them, particularly those related to change in the DNS behavior generally.

Although from that study, one concern that was raised as well is the centralization of the resolver in general. That means with DoH for instance, we will see more and more traffic being redirected to very few resolvers which will kind of disrupt the resolver landscape globally because you can now [inaudible] add the resolver in application, in browsers, so you will completely bypass proximity resolver.

So what was done was to add in the ITHI initiative that you may know about, which is an initiative run by ICANN research team, to measure over a certain period of time some metrics that allow to see if [they are] involved in positive or negative ways.

So after the discussion about DoH, a new metric was added to ITHI which is metric 5.6, which studies the concentration of resolver if we can see any pattern in that.

Over the past 12 months, though, what was noticed is that it takes around 200 resolvers to see 50% of all Internet traffic, and it took about 2000 to reach 90% of all the traffic. And that has not significantly changed over the past 12 months.

So it's an indication that at least for now—and the very early level of DoH or encryption implementation—we are not yet seeing any significant impacts on the resolver concentration globally. This metric is going to continue to be monitored over the coming month and year to see if we can identify any pattern.

So globally, that's what we can say on DoH. Of course, from the IT perspective, the work on discoverable DoH implementation is key

because that is what will allow ISP to continue to have a kind of "control" in how DNS resolution happens within their network, avoiding or solving the concern that was raised very early whereby the DNS traffic will evade completely the ISP, and they would be facing some kind of regulatory or even security threat problems because they won't see the traffic anymore, the traffic would be going somewhere else that they have no control over.

That's it. I think we will hear more from some ISP on what exactly they're saying within their network on ...

CHRIS DAWSON: Absolutely. We'll move right on to that. Thank you, Adiel, for that ground setting for our discussion on encrypted DNS moving forward. I'll note that the paper that you were describing, a link to that has been put into the chat for those of you who are interested in digging in.

For now, I'd like to start that conversation we were talking about by turning to Philippe Fouquet. Philippe is a senior technical expert at Orange, and he also serves on the GNSO council on behalf of the ISPCP. I'd like your reflections on that, and also to learn a little bit more about incentives for ISPs to deploy DoH.

PHILIPPE FOUQUART: Thank you, Christian. Hopefully, what I'm going to be saying will follow on nicely from what Adiel just said. And indeed, I just wanted to

touch upon one particular aspect that is hardly ever mentioned, and for ISPs, it's generally the elephant in the room. And that is money, essentially.

Just a few elements of background. As Adiel mentioned, there's been a lot of papers on this, mostly policy-oriented on the potential impact of the deployment of DoH, or rather, the impact of certain models of deployment, i.e. the association of DoH with public resolvers. I think that was pretty much the issue.

And on this, industry associations and groups like us, like the ISPCP, have produced papers, highlighting the issues, some of which are technical, such as the resolver selection that I'm sure Chris will address in a moment. And also, policy issues, things that relate to obligations of the ISPs nationally, and things that we actually do through our DNS servers. Sometimes people call them cache servers, resolvers.

So various papers have been published. I'm sure we can share that. I see that Lars shared the ECO paper. I'm sure Chantelle could do the same for the ISPCP's paper. There's one in the making at GSMA, I understand.

And all of them are pretty much in agreement in terms of recognizing that encryption is good. DNS being one of the last protocols "in clear" on the RP stack, and that there would be some benefit for ISPs and operators in general to support—or migrate for that matter—to encrypted DNS, Support meaning supporting DoH interface on the

current cache servers or—sorry, migrate would mean that, or support meaning you deploy an HTTP server where you have the DNS interface.

And I think there's wide recognition that this would be useful. But the sort of recurring question that we tend to get when you turn to business units and operational teams is, how much is that going to cost us.

I have a well-functioning cache server. It fits the bill. It does what we intend them to do, converting names into something, that something being, in general, IP addresses. Why would you like to make it more verbose through encryption, potentially providing a leverage for DDoS attacks? Why would you do that? And in essence, what is that problem that DoH would [intend to solve]?

We understand that it addresses a particular problem in the grand thing of Internet architecture, but from the ISP's perspective, what does it solve? And the argument that all these operational teams put forward is that, well, it's well and good that DNS is in clear text or unencrypted on the IP stack, but as far as we are concerned, people say, look, this is not in clear. When you have a mobile device speaking to, say, a BTS or something, it's not in clear. It's encrypted. The DNS requests are sent over an encrypted channel, and the security people that would analyze it would say, look, if I'm clever enough to have an IMSI-catcher or something to hack the mobile interface or to forge the interface to a set top box, for instance, then there are so many bad

things you can do when you can do that, is that reading the DNS requests is no big deal in that grand landscape.

So really, the one and only argument I'd like to put forward—and would welcome discussion on this—is because I think moving forward, it will be a recurring question.

I understand that there's a lot of policymakers who would love the ISPs to keep the DNS anchor point, if you'd like, to make sure that [locked] lists are enforced, that national regulation be enforced to the ISPs, and only to the ISPs because they're domestic players, and it's so much convenient for policymakers to have them in front of them rather than reaching out to all the top players, etc.

But in essence, the rationale, the incentive for deploying that may be questionable. I guess that's what I'm saying. And whether now or in the future, I'm sure the ISPCP would have that discussion. But it is something that, to some extent, is a stumbling block to deploying DOH and encrypted DNS in general in ISPs' network.

So I'll finish on this and turn to you, Christian. Happy to take questions if there are any. Thank you.

CHRIS DAWSON: We definitely are going to jump to questions after our presentations. For now, I think I'm going to move us along to Chris. That was very interesting perspective. And the kinds of conversations that the ISPs are ripe to have at the ISPCP. Chris actually comes from BT but has a

background working with IETF. Chris Box is a senior manager of BT. Chris works in mobile network design in the UK for EE and BT. He also led on DNS standards work for BT since DoH became a potential issue. Chris, could you talk to us about what's going on with encrypted DNS, including DoH and the conversations that are happening in the IETF around it?

CHRIS BOX: Sure. Hello everyone. Hopefully, you can see on screen. I've put some information to share with you about how these developments have occurred. And so in terms of this timeline here, as previous speakers have said, we had DNS over TLS four years ago. That was seen as not good enough because it's too easy to block. It runs on port 853.

So DNS over HTTPS was invented here, and then all these kinds consequences that people are talking about became apparent. So there has been many different steps going on in the IETF to try and resolve this. And the core question is, how do you select the appropriate resolver for your DNS? Because when we're talking about an encrypted channel, that becomes very important because if you're talking to a resolver who is far out on the Internet, then nobody in-between will obviously be able to understand or see or influence any of that.

So there's been a number of birds of feathers meetings talking about exactly how should this be set up. And then there was agreement that we could have a working group. This is called the ADD working group,

adaptive DNS discovery, and it's looking at defining protocols, essential, that allow a client to discover which encrypted resolvers are out there, and what they do, and hopefully shed some light on this problem of which resolvers should be used, because down here in the picture, you've got a typical home network environment. There are a number of devices. There's a home router. That home router has been there a number of years, it's quite low powered and doesn't support encryption, and it's hard to upgrade, which is very common.

You've got an ISP network, and you've got the rest of the Internet. So the problem we had originally was that when DNS over HTTPS was deployed, the easiest way to use it is for a client such as a web browser to say, "Okay, we'll set up a partnership with this one company out on the Internet and we'll send all the requests out to them. So we've got DoH, it works, it's encrypted, but you get all the problems that are created and flow from that.

So this is hoping to build what should be a better soliton. So this, at least for ISPs, means we can preserve a lot of the functionality that our customers are expecting. So in this model, we've got clients that can talk just using normal unencrypted DNS to the home router, but by some mechanism, we hope that they can learn about this thing over here which is an encrypted resolver that the ISP has built.

Now, Philippe's just said that that requires money to build, and yes, it does. But the IETF is assuming that's not a problem, ISPs will be able to build these things. If they build them, how do we get clients to use

them? So this is the issue that's being worked on, just to give you a sense of what's likely to happen over the next year.

So there is a meeting in November—well, one meeting with two actual session, which will be discussing topics about the requirements. And then I'm hoping sort of the middle of next year, we should have a first discovery protocol which can potentially make use of this.

So that's the general overview, but obviously, people might have questions, so I'll be happy to hear those.

CHRIS DAWSON: No, that overview is fantastic. It's very helpful and I appreciate it greatly. Let's really quickly move on. We'll hold for questions in just a moment. Certainly feel free to write them in the chat and we'll get to them as soon as we finished our short presentation from our fourth and final expert [inaudible.] John Woodworth is senior lead architect at Lumen Technologies, which is formerly Centurylink. John, you also have some words to share with us about DNS security and DoH.

JOHN WOODWORTH: Good morning, good afternoon, good evening. I'd lie to thank all of today's organizers and participants and say it is a pleasure to be here. As you mentioned, I work at Lumen. A lot of you may still know us as Centurylink. As a technology company, we deliver adaptive networking, edge computing, adaptive security, collaboration services

with over 450,000 global fiber route miles to customers in more than 60 countries.

I'd like to also echo a lot of what Chris mentioned. There are a lot of complications, I guess, around the encryption of DNS. We offer a robust international DNS presence and content delivery network and believe that having a secure DNS infrastructure is vital to providing a safe, secure environment to our customers and our network.

We are also dedicated to the security of our customers and Internet community. To this end, we are continuously innovating and evaluating new technology and using technology such as request policy zones and DNSSEC and evaluating encrypted DNS, specifically—well, DoT, DoH.

We are also engaged in the adaptive DNS discovery working group that Chris is on. He is a lot more vocal at the moment. And we acknowledge the benefits of encrypted DNS and see it as part of our commitment to security and our comprehensive inventory of security products and services.

So DNS, for a lot of people, is the Internet. It kind of represents how fast the Internet is to most people. If something takes longer to resolve, it takes longer to load, "My Internet is slow," so forth. So we're definitely concerned with the impact, that performance and stability impact that moving potentially some of this traffic off network, it would impact some security features such as threat intelligence.

I know a lot of this is being discussed within the IETF and other communities, but it definitely is a concern. There is, as previously mentioned, a price associated with implementing the new service, there's a new network overhead, new devices have to be deployed.

As a provider, local gateways offer a lot of—like a DNS proxy feature. There's a lot of complications involved in trying to implement DoH/DoT on that because of certificates. And with the ability to kind of get a legitimate certificate now with some of the CAs that are available out there, that's another concern, is like, who is seeing this traffic? Because without that discovery protocol and a mechanism to kind of hand off that control, it may be invisible but it's not necessarily the right person you're talking to. So that's another concern of ours.

Another thing that I'd like to mention is I guess the consistency within the operating system, because today, what we have is, minus of course the implementations that are out there for DoH/DoT, the operating system kind of controls the consistency for looking up names and other DNS-specific queries. And for troubleshooting, that's going to potentially cause some issues where a customer for example would call in and say, "I'm getting this page," and then we have them do a ping or a traceroute or some other troubleshooting mechanism and we're getting a completely different answer.

So for that consistency, we would like to see that, ideally, I guess, at an OS level just for maintaining that consistency across all the applications on a device.

CHRIS DAWSON: So, John, thank you very much. That is a very good overview. What I'd like to do is quickly, as we've reached the end of our panel time, I wanted to note that over the course of this panel, we've learned from our experts, we've gotten a good deal of background information on DoH [and emerging] technologies surrounding particularly encrypted DNS.

I wanted to point out that we've also heard about concerns and things we still need to work through in this technology. So before we move forward, I wanted to hit my colleague, Philippe, with one question. And I actually want to answer the question first and then I'll go ahead and see if you have anything to add, Philippe.

We are faced with technologies changing over time and we as ISPs need to be responsible about engaging in those conversations and having a part in making sure that technology moves forward in a way that resolves issues, that resolves questions or concerns, that things march forward in a way that is basically not going to screw up our networks and make things as smooth as possible for our users.

I'm interested in how that happens at the ISPCP level at ICANN. And one thing that I wanted to note is that one of the things that I like about the ICANN is that when I go there, I meet folks that are technical, I meet folks that are in the Internet governance space, and that are engaged in the ITU or the IETF or the IGF and are parts of conversations that are elsewhere within the I-Stars community, and

they bring all sorts of different aspects of what's going on in those communities back here so that we can have a conversation among colleagues about what's happening from a technical standpoint, from a policy standpoint and procedure standpoint, and we can have conversations that are productive and move the ball forward.

I'm interested in hearing from you, Philippe, why Orange commits its time and resources to being involved in the ISPCP. And maybe if you have suggestions on how people can get involved in the ISPCP.

PHILIPPE FOUQUART: Thank you. Your question, Christian, is not as simple as it seems, because it's always a challenge these days to make sure that in such a complex environment as ICANN can be, the issues that are debated here are well understood internally within our organizations.

I think one of the reasons why we committed to working within ICANN was a recognition that because of its [own] organization, if you look at how the GNSO is organized—and obviously, for the reason that all stakeholders have their say in the way gTLD policies are defined, that was the purpose of the organization. But the result of that goes beyond this, is that the origins of these people within the Business Constituency, within the IPC, etc., is such that, as you said, you can sort of meet all the relevant and the people that count within these companies. You can hear about all the arguments—and I haven't mentioned the ACs, but certainly, people within SSAC are much more proficient in security than any one of us can be.

So you have the whole range of business, to IP, to technical people that you can meet and make sure you can integrate that, and come with your own requirements, of your companies' requirements, making sure they're digested, because you've spent some time here, and you can get nurtured with all these different channels, if you like. And I think that is, in essence, on an almost purely human basis, if you see what I mean, why we get involved, even beyond the fact that ICANN matters and the fact that without IP addresses and without domain names, there would be no Internet, without root servers, there would be no Internet at all.

But I accept the argument that it is not sufficient for an ISP to get involved. This is probably not the reason why we do. But the reason why we do is because of this, because of the variety of different people involved and the fact that we can get nurtured by their expertise and feed it back into our own organizations.

CHRIS DAWSON: Thank you so much, Philippe. And we are well past time. Andrea, thank you for your patience. I really thank our panelists for educating us today. All of you, Adiel, Chris, John, Philippe, thank you for your time, and I turn it back over to you, Andrea.

ANDREA BECCALLI: Thank you, Chris. Indeed, it was a very interesting second panel. Congratulations to all of you. Lots of things to learn. Yes, we have a few minutes left for this session, and there had been some discussion

happening in chat. Let's do like that. We will have just Adiel now coming with a short presentation on how to get engaged or contribute, and then I would pass it to you, Wolf-Ullrich, to do the conclusion and see if we have any time left to take some question. Otherwise, we'll try to address those in the chat. Adiel, please.

ADIEL AKPLOGAN: Thank you, Andrea. I will not use the slide anymore because we have a very limited time that's remaining, but it's a very good follow-up from what Philippe just mentioned. It's not always easy to get the attention and the incentive for ISP to participate into ICANN forum in general and the ISPCP in particular. And what we're trying to do from inside and with the ISPCP leadership and everyone is to bring more of technical issue, more of program that can incentivize people to actually join. Of course, keeping the ISPCP within the context of the GNSO, but also expanding its outreach to some of the work that we are doing.

And as you know, the office of the CTO within ICANN is doing a lot of different things and initiatives to actually support the security and the stability of the DNS and we know that the ISPs have an important role in there. From that perspective and engagement perspective, we also think that the ISPCP can be a good vehicle through which we can work and collaborate to bring those work, to bring those analyses, those research globally and work in different region with different ISP who have different reality as well in order to have a holistic view of what's happening and also inject more best practices and so on.

As you know, the new strategic plan from ICANN focuses a lot on best practices and securing the DNS, and for that, for instance, we have been working over the past few months in revisiting the way we engage with the technical community, basically network operators, DNS operators on security matters.

We have come up with almost 14 different courses around the DNS, the security, universal acceptance and so on that we are seeing that is now original, is ready to take up with the ISPCP or the ISP originally to deliver. So to raise the awareness on some of those issues, but also on the issues that we talk about today, DoH and so on, hyperlocal implementation, for instance, which are new things that ISPs have to catch up with and that can have a technical impact on overall security of the DNS.

We have initiatives like ITHI—I mentioned that in my presentation—which help us also measure and monitor some of the key elements that allow us to say, well, the overall ecosystem is secure and stable, and there are metrics where we need input and data from the ISP. And the ISPCP could be a good vehicle as well to get in touch with ISP who are willing to contribute data, to contribute expertise into these measurements of these research projects that OCTO is leading.

And ITHI is a [inaudible] where the participation is open, the different level of participation, and one area where we are connecting and trying to understand [a lot is the recursive] area and for that, we need information and data from ISP.

So if you are interested to engage and to work with us in those areas, feel free to reach out to us, OCTO@icann.org if you want to join either the ITHI initiative and contribute data or other initiatives like DAAR or interested in what we're doing to promote or raise knowledge around technology like hyperlocal and so on, contact us. Our team, as I mentioned, that is regional now, would be more than happy to work with any of you to engage the community more widely. Thank you, Andrea.

ANDREA BECCALLI: Thank you, Adiel. Wolf-Ullrich, now you do have an elevator pitch for ISPCP. The hour and a half flew by very fast, which is a very good sign. Thank you all for that. Wolf-Ullrich.

WOLF-ULLRICH KNOBEN: Thanks very much, Andrea. Just being brief in that, as ISPCP chair, I am interested, not just to increase the number of members of this group but to increase the number of active members. and that is a major challenge. I understand that from when I first joined ICANN more than ten years ago.

So when my company was sending me there and they decided—I was with a big German telecom company at that time—and then decided at the end not to stay with ICANN, rather than to participate indirectly through an association like ECO for example. So this could be another platform for those who are interested and who do not have the money

or won't invest the money to send people directly to participate in those meetings. So that's also an alternative to indirectly participate.

From all this, we will have gain support also in what we are doing, and [I rely] a lot of that, what you're saying, Adiel and Philippe as well, that we have to focus also more in the future on technical things. On the other hand, we are [beholden] to work on policy matters which is a lot of work with regards to processes, which is not everybody's really first choice to work on who is coming from a technical area.

But nevertheless, this all makes a good mix within our constituency to work on, and I really would like and offer you all to join the ISPCP. The address is being delivered also in this presentation at the end where you can get in contact. And that's it.

So with this, I would like to thank you and thank especially ICANN and the team of Chris Mondini and Andrea in helping us, supporting us and organizing this session. Looking forward to seeing you once around. Thank you.

ANDREA BECCALLI: Thank you, Wolf-Ullrich. Thank you, everyone. It's been a pleasure for us. Thank also to our colleagues, technical team, that let us use five minutes more. It's been a pleasure. Looking forward to seeing you in the rest of the ICANN week. We will share all the presentations that will be on the ISPCP website, and we actually achieved doing this session without waking up Esteban's seven children, which I think is an achievement in itself. Thank you so much.

[END OF TRANSCRIPTION]