GISELLA GRUBER: Good morning, good afternoon, and good evening. Welcome to the fifth webinar from the At-Large Capacity-Building Program, 2020, on the topic of "DoH/DoT: Benefits, Drawbacks, and Way Forward," on Monday the 7th of September at 21:00 UTC.

This webinar is scheduled for 60 minutes. Holly Raiche is our presenter and Joanna Kulesza will provide a brief introduction shortly after my introduction. We will not be doing a rollcall, as this is a webinar, but attendance will be updated on the agenda Wiki page.

We have French and Spanish interpretation on our call today, so a kind reminder to please state your name every time you speak to allow for interpreters to identify you on the other language channels, as well as for transcription purposes.

We also have real-time transcription. The link is on the Wiki agenda page, and I'll also display this now in the Zoom chat. It's also very important to speak at a reasonable speed, and clearly, to allow for accurate interpretation. All lines will be muted during the presentation and open to questions and answers at the end of the presentation.

If you are in the Zoom room, please raise your hand and the moderator will make note of the speaking queue. Or if you do type your question in the chat, we have the format of how to ask a question, and this, again, I have just posted in the Zoom chat.

We will keep track of all the questions, and these will be addressed during eh Q&A session, or please do raise your hand to ask them over audio

channel. It's always more interactive. If you are only on the phone bridge, please speak up, and you will be added to the speaking queue. With no further ado, I will hand the floor over to our moderator, Joanna Kulesza, co-chair of the At-Large Capacity Building Working Group. Thank you all for your attention, and over to you, Joanna.

JOANNA KULESZA: Thank you very much, Gisella. Welcome to yet another webinar on one of the technical aspects of DNS and Internet governance in the broader sense. We are looking at a lovely acronym that has gathered quite some interest from the At-Large community and beyond: DoH/DoT.

We have a most appropriate speaker for that topic, who is Holly Raiche. For those of you who might be new to the At-Large, Holly has an extensive experience when it comes to the DNS to Internet governance, as she has been elector with the law faculty and the department of media and communications, and has extensively taught in Australia and beyond.

You can see our agenda in the link that Gisella shared. The outline for this meeting is quite predictable. I will try to be as brief as I can, going under the five minutes that have been appointed to me, leaving 30 minutes for Holly, for a presentation and a pop quiz. We would like to hear back from you how effective this meeting is in terms of introducing the DoH/DoT protocol and everything that it holds.

We've also accommodated 20 minutes for the Q&A session, as Gisella indicated. We welcome interactivity. If you have the possibility to speak up, please feel free to raise your hand and you will be offered the mic to ask your questions.

We would like to collect the questions for after the presentation. If any thoughts come into your mind and you would like to share them instantly, do feel free to use the chat, indicating that you have a question, as Gisella shared, in the box that you can see on the right of your screen.

We will also ask you to provide a brief feedback. This is one in a series of webinars. We're trying to best meet the needs of the ICANN community, so we will ask for your thoughts about the specific events, whether it has met your needs, whether you have any suggestions for us on how best to improve.

And with that, I am more than thrilled to hand the floor over to Holly—thank you for accepting our invitation—to speak on a somewhat ambiguous acronym, even to this community who loves acronyms, which is DoH/DoT.

Here, you can see on the screen a brief bio for our speaker today. Please, Holly, tell us what this acronym holds, whether it's a good thing, whether it's a threat to end-users, and is there any policy behind it that we should or could get involved in? Thank you again for joining us, Holly. The floor is yours.

HOLLY RAICHE: Thank you very much, Joanna. I have to say, there is lots to be said both for and against, and one of the … I did not do a pop-up question because it doesn't lend itself very well to pop-up questions, but it's one of those subjects which starts off as being very technical, with—let's put it this way—a lot of geeks very aware of it.

I, personally, do not have the technical knowledge. So, if I've got any questions, one of the people listening to this is Geoff Huston, who has got a blog called "Potaroo." He's got a very excellent column, very obviously technically far above what I know.

So, if I've got any questions, I've got to ask Geoff. He is also a member of the board of Internet Australia. I am looking at this from a purely non-technical point of view, and it's one of those issues where the technology itself raises some questions for … Well, end-users, but for governments and for how we understand that the Internet is run.

We're starting off with just a simple … This is what I'm going to talk about. Hopefully, I'm not going to take longer than half an hour. I don't think I will. But first of all, what is the terminology? How do these two technologies work? What are the pluses for introducing this technology, and what are the minuses? What are the disadvantages? What is the way forward, or is there?

Now, for those of you who have attending ICANN meetings, you will recognize that we've actually had two sessions on this topic. The first was more of a technical session, and it was really the last face-to-face ICANN meeting we had.

The second session was one I ran, and that was in March, one of the virtual meetings. So, this should be familiar to many of you, but I don't expect it'll be familiar to all of you. And in the end, probably, I'm going to be asking Geoff some questions, as well. So, let's start with the first slide. Thank you. The second slide. Okay.

There is basic terminology. I am assuming that most of you understand the way, classically, the Internet works, just in case. We all know—or we should know—what a DNS message is, or at least the way it's being used in this context. And I'm going to have a little diagram to show exactly the process I'm talking about, because that's critical to understanding what the issue is.

Essentially, it's a query-response protocol. The purpose of it is to change what you type into a browser, the h.raiche [inaudible] .net, or h.raiche@sydney.edu.au, into a bunch of numbers, an IP address, and it's the IP address that will get from your computer, or your phone, or whatever, to my computer, or phone, or whatever.

DoT, which is one of the terms that we're talking about, is really domain names over the transport layer security—TLS. TLS being secure, this is the protocol, the "TLS protocol." The purpose of it is to provide privacy and data integrity. The TLS layer will be what the IP address, the little packets, travel on when they're going from my computer, or my laptop, or my mobile, or whatever, to where they want to go.

The DoH. I'm sure all of you know that, you look at a domain name, you're looking at HTTPS. The S stands for "security." So, it's the transfer protocol, secure. It's the secure version, the primary protocol, to send data between a web browser and a website.

If you'll notice, both of these terms are about privacy, about security—security in the sense of the security of the data that is moving from one place to another. The middlebox is a term that's used, actually, in Paul

Hoffman's presentation. It's kind of a generic term. It's something between the client and server that looks at, and perhaps modifies.

The transit might be a firewall or it might be how you introduce filtering. It might be something that actually looks at the content. But it's something between when your packets first ask, "Where do I go?" and when the packets actually head on their journey. I hope that makes sense. It will in a minute. May I have the next slide, please?

I hope you can see the diagram on the left. This explains what we're talking about. If you look at the diagram, start from the upper left. I type in an address. I type in atlargeicann.org/alac. That goes to a resolver, and the resolver goes, "Well, I have to find the numbers that will send these packets on their way to this address."

So, the packets start from the resolver. They head up here, which is the root server that used to be called IANA—now, it's called PTI—and say, "Where do I go? What beginning IP address is going to send me in the right direction?" IANA or PTI is going to say, "Well, actually, you need to go to the [GNS Inter-Org]." That would be PIR, and we all know about PIR—Public Interest Registry.

Oh, okay. Now that I've got that information, I know I can go to ICANN. Then I know, when I come back on this trip, is At-Large. So, you've had a send-and-response to get, instead of numbers, the IP address that goes back to me and says, "Okay. Now, we've got the roadmap as to where we're going. Let's go."

Why did I spend that much time? To make a point that these trips are in red to say they are unencrypted. This is where the issues lays, and it was

this area that is unencrypted that began to be of concern. So, while this journey, once you send your packets on the way, can be encrypted, but classic DNS lookup isn't, and that opens all sorts of things. It opens the possibility for filtering, for child protection, for DNS abuse; for a lot of things. Next slide, please. Nic, could I have the next slide, please?

Okay. Recently, there have been far more awareness that the classical lookup leaves this bit of the lookup process as unencrypted. So, even if you've put in place things like DNSSEC, TLS, over security measures, there is still this red bit that's unencrypted, and therefore leaves open the kinds of DNS abuse that has become of growing concern: man-in-the-middle, tax spoofing, etc.—certainly privacy.

And after Edward Snowden, everybody has become aware of how much material—unencrypted—is looked at, is used, is abused, and without the consent, if you look at, when the consent is asked, whether that consent is freely given or not, or even knowing it.

This is where all of that data is being collected. The other issue is that, in that red space, that's where controls and filtering happen. So, we suffer from DNS abuse/loss of privacy; we gain, or not, from controls and filtering. Next slide, please.

To make the point more clear, the only change that either of these makes is to add some kind of encryption or security in that lookup process. Neither change the queries and responses, and any change beyond encrypted transport or result of implemented … They are not DNS … Sorry. DoT or DoH protocols themselves. So, we're simply looking at

encrypting in some way what has been unencrypted up until now. Next slide, please.

Okay. Back in 2016, there began to be an awareness of both the good and the bad stuff that happens because of the unencrypted nature of the DNS lookup process. What happens with DoT—putting this in, hopefully, my language, probably not Geoff's language—adds encryption with a TLS. Thus, you get Domain Names System over TLS. It's just between the end-user's computer and the recursive resolver. That's the first hop in my diagram, not later.

So, in Paul's words, this is designed primarily as a more private transport for DNS messages. Could I have the next slide, please? This is the illustration for what it would look like in the DNS lookup process for a whole network. That's not encrypted in the browser to the computer. That's encrypted. This is the whole recursive resolver process, which I've pointed to, and that's not encrypted. What that does is it breaks connection between who you are and where you're going. Next slide, please.

Okay. For an enterprise network—we're still on DoT—this is where the encryption is put in. Again, that's not encrypted, and this is not encrypted. But again, the connection between who you are and where you're going is broken here in the red arrow. Okay. Next slide, please.

DoH is a bit more sophisticated. It is a layer version of, how do you protect, or how do you add privacy, to the actual lookup process? And again, this is from Paul's presentation. The message is wrapped in HTTP messages and transported over the TLS. So, you can see there is more

protection or encryption. It allows servers to push DNS responses before being requested, and it's primarily designed to encrypt—this is what we're worried about—DNS traffic for applications.

And there is another party in the ICANN world that came up with their own SSAC paper. It's available on their website. SSAC109 was released about the time of the March meeting, when the second of the DoH/DoT sessions was held: high DNS transactions. So, as the TLS was carrying the packets because the actual DNS transaction was hidden in the HTTPS, it simply passes through.

There has been a lot of interest in both DoH and DoT, as you can imagine, even up to the government level. The U.S. Congressional Research has issued a paper just to explain in words of one syllable. And interestingly, they don't talk about DoT. They only talk about DoH. In their words, the content of a DNS query is visible only to the user's browsers in the DNS, not to third parties. This is the critical bit. This is the one where you get both a lack of privacy, the gathering of data, and possibly—well, assuredly—security breaches. Next slide, please.

Okay. We'll see the arrow is a lot bigger in this diagram. This is taking the DNS over the transport layer, all the way here. There can be no … Well, there can't be attacks in the middle, so it provides more security in terms of … And, in fact, can pass by your normal process on the way to the resolver of the choice of your browser. Next slide, please. Okay.

DoT can be identified and blocked by intermediaries, not DoH, because DoH, if you remember, passes through. DoH is designed to be indistinguishable from the normal HTTPS traffic. So, it's harder to block

and it's harder to know this is what's happening from your ISP view. It cannot be blocked without potentially blocking other traffic. So in fact, in one way, it's more secure, but that raises some other issues, as well. Next slide, please.

Now, governments are finally beginning to be interested, and I love this particular quote from Baroness Thornton, when there was a discussion in the UK Parliament, House of Lords, on what is this thing. The baroness is worried about the geeky question that was all about DoH: what concerns and is finally concerning governments?

"There is a fundamental and very concerning lack of accountability when obscure technical groups"—she's talking about the IETF, here—"are employees from big Internet companies." Well, maybe, or maybe not. "They have taken decisions that have major policy implications," and in that case, she is absolutely right. "Enormous consequences for us all."

And she asks, "What engagement have the British Government had with IETF?" and she probably doesn't understand that they have, probably, a long-standing engagement by many UK engineers. She just hasn't been told. But it highlights the fact that governments are finally beginning to ask, what's going on?

Thus, you have the House of Lords debates, you have the U.S. Congressional Report. You have a lot of discussion about the implications of both of the technologies. Next slide, please. For both of them—and we're talking about the pluses, here—why would you do this?

It's privacy. Where you, as an individual, are going is encrypted for both of them. The connection doesn't ... Will make sure you don't … There is

no connection between you and the recursive resolver. For longer, for the whole trip over HTTPS, DoH protects. So, in fact, where all that data is collected that we worry about, with both technologies, the connection between you and that data is broken. Next slide, please.

The pluses. If you've got the classical lookup, DNS queries can be intercepted. Legitimate traffic is manipulated. As a result, aside from the security issues about that, services can be unavailable or delayed. All of that information about you and where you're going is harvested. Other malicious activities, the DNS abuse categories, because we're now on DoH, those things are prevented, certainly from a security point of view. Man-in-the-middle attacks, DNS abuse, spoofing, and so forth, is prevented. Those are the pluses. Next slide, please.

And, the reason I don't have a quiz, there isn't an easy answer as to which is better. There are good and bad sides. So, what is prevented in that service providers can have firewalls, you can prevent website … What happened? No, no. There. You can prevent e-mail that typically sends malware. The ISPs can prevent communicating with malware servers after being infected.

Another critical thing—and this is what really grabbed the attention of the UK government—parental controls are available for parents to stop their kids being able to see stuff. If you're blocking the traffic or hiding the traffic, you can't do that anymore.

Filtering. A lot of governments actually—including the Australian government—have a filtering regime. That can be bypassed. Another thing that happens: many companies, particularly ones dealing with

sensitive information, will watch the traffic that comes into and out of their system, and they will see what material is going out, by whom. A good security measure for them.

However, it can be used to prevent communication by dissident groups. It can access information, it can provide all of that information on where you're going, and that's what happens. That's all the personal information that we want to actually prevent from falling into people's hands for privacy reasons. So, on balance, you can say there are pluses and minuses to filtering, either one of them. Next slide, please.

Okay. Benefits. There is a single set of DS policies to understand. There can be larger caches, leading to faster responses. This is one of the things that both Paul and the SSAC pointed out. That is, if you have traffic being sent to just the chosen resolvers of the IPS, you are actually now in the place where packets can go, and possibly creating a target for bad actors, if you will, for denial-of-service attacks, and so forth—malicious actions.

And because there are fewer places for the packets to go, there is the possibility of slowing web traffic down. Again, what you see is there are some pluses here, and there are some minuses. Next slide, please.

Okay. Where are we up to? If you use Firefox, they have what's called a "trusted recursive resolver program." They have only got two resolvers: Cloudflare and NextDNS. So, the packets are going to one of two places. They are bypassing the normal process, the classical DNS lookup process, and they're going to their own trusted resolvers.

[inaudible] testing. I'm not sure how far that has gone. Google has automatic encryption. Microsoft is starting to look. So, this is not a

theoretical problem anymore. This is here, it's now. And in fact, I'm sitting on my computer, which uses Firefox and Mozilla, so that's what's happening to me. Next slide, please.

From Paul's paper, unless the middlebox and the associated computers are configured in such a way as to provide the middlebox, which suggests there may be a way to preserve some of the anonymity but allows some of the middlebox controls. Certainly, I think that's being looked at, because that's where some of your protections lie. That's where some of the parental controls lie. That's where some of the filtering happens. We may be able to actually move away from the classical DNS, but we may be in a way to preserve some of the pluses.

The middlebox still knows endpoint as a traffic. It's got one IP address. It can assume the encrypted traffic and can enforce local policy. So, there are some possibilities that, even if you have DoH or DoT, you may be able to preserve some of the positives, the privacy, the filtering, and so forth. I'm not a technologist, and I would hope that [Jack] would talk both possibilities. Next slide, and I think that's it. Thank you. Yeah. Okay.

Useful links. If you go to ICANN's website, you will find that the two meetings where this was fully discussed by Paul Hoffman and others, the 12th of March in 2019 and a year later … This was last March and this was the first of the online meetings.

Those two things and the slides are available. Paul's paper is available. He's with OCTO. The SSAC paper is available from the ICANN website. The Council of European National Top-Level Registries has done an issues

paper. It's only over DNS or, it's only DoH. It's not DoT. U.S. Congressional Service. There is UK parliamentary debate.

So, there are lots of papers. I think the best thing to do is start, though, with the ICANN website, with Paul's paper, and with the SSAC paper. I think that's the last slide. Thank you. Okay. We've got 20 minutes for any questions. My first question is, what did I leave out? Okay. Could we go back to where I can see the chat? Okay. Geoff.

GEOFF HUSTON: Thanks, Holly. That was a very clear explanation. Perhaps I could just give you a bit more detail? And just for the record—

HOLLY RAICHE: Yes, please.

GEOFF HUSTON: I'm with APNIC. There is a critical difference between DoH and DoT, and it's actually all about the locus of control. The DNS used to be provisioned by your internet service provider, and it was something your operating system library did. No matter what application you were running, all the queries got funneled down the protocol stack, came out through the operating system, got sent to the Internet service provider, got resolved.

Now, DoT, DNS over TLS, doesn't change that picture. DoT is typically implemented as an operating system transport protocol, and the whole idea that applications don't worry about the DNS is left alone.

So, in some ways, DoT is infrastructure as we knew it. Why DoH excites so much reaction is that DoH is typically implemented on an application basis. So, I might run both Mozilla and Firefox. I might run an electronic mail service. I might run any kind of application. And that application may choose to query the DNS using its own preferred resolvers, without reference to any other application on your device.

So now, your queries are going everywhere or anywhere. The solution proposed by Paul Hoffman to give middleboxes entree into the security domain between you and where you want to go does seem almost antithetical to good security practice. Middleboxes should never share secret keys with the destinations or you. You shouldn't trust them.

So, that kind of solution framework you're proposing, Holly, or Paul was, actually isn't a very effective one. But as I said, the real issue that is going on here, and why it's such a difficult problem, is that, now, the DNS is not corralled into channels that are well understood.

Each application has the ability to fuddle its DNS queries anywhere and everywhere it so chooses, without referencing the end-user, without referencing national policies, or anything else. And that really is why DoH is at the heart of these conversations, whereas DoT is safely corralled to one side. Thank you.

HOLLY RAICHE: Thanks, Geoff. Much clearer, and why, in fact, probably, it was DoH that was the subject of some of the discussion for the congressional report, and probably some of what may have been behind the Baroness Thornton. I like Olivier's comment: "It's called chaos."

Maybe, Geoff, you can answer the question for me. There was some discussion about—and it has happened in the SSAC paper, it has happened in Paul's paper—the centralization that possibly happens with, particularly, DoH, and whether that's a good or a bad thing, whether that may delay messages getting through or whether it may, if you will, present itself as a honeypot.

GEOFF HUSTON: Okay. I'll very quickly answer that. It is common knowledge that the Chrome browser has about almost 80% of the Internet's entire eyeball population. So, in the browser world, the Internet is highly centralized.

Now, a lot of folk do use Google's public DNS service. Around one-quarter of users send their DNS queries via Google's public DNS. That's a lot. But the scenario is, what is the application Chrome decided, by default, without reference to anyone, sending all of its queries via HTTPS, otherwise unblockable, to a recursive resolver of its choice. All of a sudden, all the DNS goes to one service point.

And the chilling thought is that, if that service point didn't answer geoffsfavoritedomain.com anymore then, almost irrespective of the root, irrespective of the DNS, irrespective of anything else, geoffsfavoritedomain.com is now dead. And this centralization actually places the locus for control with the dominant application, with the dominant application vendor.

And that centralization creates a chilling alternate control mechanism that is well-distanced from the current delegated DNS structure, and I think that's at the heart of the centralization concerns: one vendor, one

operator, one provider has almost a stranglehold over the entire name infrastructure of the Internet if that were to come about.

Now, I stress Chrome hasn't gone that way. Chrome is still looking at mechanisms that provide some degree of either choice or use existing DNS infrastructure. So, this is largely a hypothetical concern at this point in time. But would you notice it if they did it? Would you be aware if that was the new default operation? Well, of course not. None of us are. So, in some ways, it could slide in without anyone even noticing. Thanks.

HOLLY RAICHE: Thanks, Geoff. I have got a couple of comments. First, to note, Olivier, one, one, one, a single point of failure—I think you answered that. And from Cheryl, indeed, that's hypothetical. One question, and this is … Let me find it. Okay. From Pablo Rodriguez, ccNSO Council, "It seems that DoH and/or DoT complements DNSSEC. How can one use it independently from DNSSEC?" My answer would be, it is independent of DNSSEC. But Geoff, correct me if I'm wrong. Thank you. This is just [inaudible].

GEOFF HUSTON: No, they are entirely independent.

HOLLY RAICHE: That's [what I said].

GEOFF HUSTON: DoH and DoT are transport. They stop people looking at your packets. DNSSEC is all about believing what you hear. You, yourself, the end-user, can you trust the answer that you got? That's a DNSSEC-related question. Thanks.

HOLLY RAICHE: Yep. If you go back to my first and second slides, Pablo, what you'll see is that DNSSEC is basically what happens apart from the lookup process that's there, and it's … Okay. Next slide. Oh, I think it's the next slide, where it's … It doesn't matter. DNSSEC is about making sure that where you think you're going is where you're going, but it doesn't actually deal with the process before that, which is to find out where you're going in the first place.

So, I hope that actually answers the question. Gopal, you had a question as well. We're not hearing you. Thank you. I'm not hearing … You had your hand up, Gopal, so I'm just wondering if you'd still like to ask a question? Well, are there any other questions? As you can see, this doesn't actually lend itself to a quiz. So, people are going to get a ten-minute early [ride] if there are no further questions.

JOANNA KULESZA: Hi, Holly. If you look at the chat, we have a comment from Bruce you might want to look into, and we also have a question from Vrikson.

HOLLY RAICHE: Okay.

JOANNA KULESZA: And I'm also curious if Pablo had anything more than just a question that he wanted to share, since he also had his hand up.

HOLLY RAICHE: Sure.

JOANNA KULESZA: So, these might be helpful.

HOLLY RAICHE: Gopal, would you like to ask myself or Geoff a question? Are you muted? Joanna, I can't …

JOANNA KULESZA: No, I can't, either. We can see you, Gopal, but we can't hear you. if you could type your question into the chat, that might be helpful, and we might want to pick up the question from Vrikson.

HOLLY RAICHE: Yes, please.

JOANNA KULESZA: Let's make sure if … So, Vrikson just posted the question in the chat: "What is it that Geoff said that Chrome does not have, or is dealing with, if I heard right?" So, if you could go back to that explanation, Geoff, and

kindly provide it in a bit more detail, that might be helpful. And we also have a comment from Bruce. Holly, I don't know if you can see the chat or if you would rather I—

HOLLY RAICHE: Yes, I'm reading it.

JOANNA KULESZA: That would be perfect. So, if Geoff was kind enough to give us more detail on that difference between the browsers or the applications, that might be useful to respond to Vrikson's question. And I see Olivier's hand is up, as well. So, if Geoff has an answer, that might work, and then I would be happy to give the floor to Olivier and Pablo. I see his hand is up again.

GEOFF HUSTON: Right. Let me very quickly answer the difference between Chrome and Firefox right now. In the United States, and only in the United States, we believe, releases of Firefox from October 2019, by default, and with no change in the configuration on the part of the user, pushed DNS queries over HTTPS to one of its trusted recursive resolvers, which, at the time, I believe, was Cloudflare's 1.1.1.1.

Users had their DNS moved elsewhere, away from the ISP, away from the platform, by default. Chrome certainly looked at this but decided not to do a default change, per se. the behavior that Chrome is contemplating is to look at the resolvers that are currently configured in the operating system provisioned by the ISP and probe those resolvers to see if they can support DNS over HTTPS, and if so, they will use it.

So, Chrome's behavior is not to change who resolves your DNS names. Its change is, if supported, it will use those same resolvers but in an encrypted channel. Firefox, as I said, in the U.S. only, and not elsewhere, has put in a default behavior to literally shift the DNS away to a resolver of their choice. That's the critical distinction that I was referring to. Thank you.

HOLLY RAICHE: Thank you very much. Sorry, Holly.

HOLLY RAICHE: Yeah. I was just going to say thank you to Bruce. Hi, Bruce. Let me read the comment out for people who aren't reading the chat. "Given some governments are increasingly seeking to direct ISPs in their country to filter and block via DNS access," as is happening in Australia, as well, "will this inevitably drive users to be more comfortable with a DoH solution, where they feel they have more user control? I can imagine, for example, that people might use different browsers for different purposes; for example, one browser for work, one browser for accessing things like movies, or TVs, or shows that may not be available in a particular country."

In fact, that is exactly what was talked about in some of Paul's later OCTO paper. I think that may be part of SSAC, but I don't know. Geoff, was that part of SSAC, the possibility that you may use different browsers for different purposes?

GEOFF HUSTON: Not different browsers, but if you broaden your mind a little bit, different applications go in different ways. This, of course, is a nightmare. We're used to seeing the DNS as the same everywhere. You ask a domain name a question, I ask a question; it's the same answer.

But when I use application A, browser or not, and then try and check it using some other application and get a different answer, we all get terminally confused. This is, I suppose, an argument that supports the larger thesis that the DNS is fragmenting badly, and it's all blowing up out of control: chaos, as Olivier referred to earlier, staring us in the face. Thank you.

HOLLY RAICHE: Thank you, Geoff. Olivier, would you like to make a further comment?

OLIVIER CRÉPIN-LEBLOND: Yeah. Thanks, Holly. I'll actually defer to Pablo because I think he has been waiting for quite some time, and then I'll ask a question after him, if that's okay.

HOLLY RAICHE: That's fine. Pablo?

PABLO RODRIGUEZ: Thank you so much, Olivier, and thank you so much, Holly and Geoff, for the excellent answers. Quick questions regarding the implementation of both of these protocols. It seems that, based on the different setups that

you may have, it will be more or less difficult to implement. Is that the case? And also, would one be more secure if it were to implement both DNSSEC, DoT, and DoH? Thank you very much.

HOLLY RAICHE: Thank you. Geoff, I'm not sure, but would you think about implementing both? I can't imagine you'd be thinking of implementing both DoH and DoT. Sorry.

GEOFF HUSTON: A very quick answer: don't forget, in some ways, there are different places. DoH is typically something that's bundled into your application. You wouldn't separately build it or separately add it. Now, I know Cloudflare released a DoH package that you can run on your mobile or your laptop, but that is really rare. So, DoH is not something that, as a user, you would install and configure. The application that you just downloaded and are running may have it there or it may not, but that's really the application's responsibility.

DoT is something that you would normally install as a driver. It certainly requires hands-on. It requires twiddling with the knobs. It is very rare. They are both implemented exactly the same way. They use the transport layer security platform, typically, these days, using OpenSSH and that library, or they may use GnuTLS, or one of the others. But these are just straight-up library calls.

The encapsulation above TLS, whether it's HTTPS or raw DNS, makes almost no difference. So, as a coder, the amount of work is actually the

same for both. As a coder, it looks much the same. Library calls to TLS, and then a certain layer of encapsulation.

So, the implementer would find either of those easy. DNSSEC is completely different. It is part of the resolution code in your DNS library. It is not part of the same technique. It may also use OpenSSH to do the cryptography but, again, that's just a common cryptographic library at this point.

So, DNSSEC is different from DoT and DoH, and DoT and DoH both use a common TLS substrate to give them security. What differs is the wrapping, but the real difference, as I pointed out earlier, is the locus of control. DoT is part of an operating system, as we normally see it. DoH is packaged inside applications, and therein lies the issue. Thank you.

HOLLY RAICHE: Thank you, Geoff. Joanna, do we have any more questions? We're probably two minutes off the hour.

JOANNA KULESZA: Thank you, Holly. We have a comment from Olivier that's pending. I also see a question from Gopal in the chat, and we will be requesting our participants to take the survey. So, I would suggest we might want to take the comment from Olivier, since he already had the floor.

I would encourage all other questions to be posted to us, to the mailing list of the Capacity Building Working Group. We have consent from the interpreters to extend the meeting by five minutes and, if that's okay with

the participants, we encourage you to stick around just for a very brief wrap-up.

So, that would be my suggestion. I would suggest we hear from Olivier. There is a hand from Pablo. [If it's a two-thinger], then you're more than welcome to take the floor, Pablo, as well. I would encourage all questions to be shared via the mailing list. That would be my suggestion as the moderator, Holly, but you have the final [inaudible].

HOLLY RAICHE: No, I think that's right. I think that, any further questions, we would be happy to take them on the mailing list. Actually, Joanna, could you type into the chat where they might address questions?

JOANNA KULESZA: I will do that. I will share the capacity-building dashboard with all of the information. thank you, Holly.

HOLLY RAICHE: Thank you. I think a last word to Olivier?

OLIVIER CRÉPIN-LEBLOND: Thank you very much. Yeah. Thanks very much, Holly. Actually, it was a question. We've heard of the thing which is of real concern, this whole concentration of control, concentration of power, potentially. To me, that translates into less resilience and, of course, less resilience translates

to being things like blackouts, networks just turning themselves off for some time.

And as we know, some of these service providers/Cloud providers that shall remain nameless are good at sometimes coming offline for unexplained reasons, which we find out later was caused by some error of some sort on a Saturday night.

Is there any way to counter this by multiplication of providers, DoH providers, or something? I mean, have we found something to counter this loss of resilience?

HOLLY RAICHE: Geoff?

GEOFF HUSTON: I'm sorry, quickly, no. Sorry. No, we haven't found anything.

HOLLY RAICHE: Thank you, Geoff. Thank you as my partner in presentation. And Joanna, I think, over to you for a wrap-up and a quiz. First of all, thanking everybody for attending, particularly thanking Geoff Huston, APNIC. Back to you, Joanna.

JOANNA KULESZA: Thank you very much, Holly. That was an impressive presentation. Thank you, Geoff, for chipping in. That was most appreciated. Thank you, everyone, for taking the time to join us. I particularly appreciate the

somewhat governmental side and security side of this discussion. Let me emphasize and thank the GAC members that I can see on the participants list. I welcome the opportunity to work together with the GAC with regard to capacity-building.

Before we wrap up, can I give you more details about how to get involved with the webinars to suggest topics? I would like to ask Gisella to provide us with the brief survey we do after, or at the end of, every webinar, just for us to get a feedback from you what you liked and what you thought could have been improved for further, future webinars that we will be setting up. Gisella, is it possible to have the survey now?

GISELLA GRUBER: Thank you, Joanna. Can you see the poll on your screens? Just double-checking.

HOLLY RAICHE: No.

JOANNA KULESZA: No.

GISELLA GRUBER: Just bear with me. Do you see it now?

JOANNA KULESZA: Still nothing on my screen, I'm afraid, Gisella. Now it's up. Thank you. Seems to be working.

GISELLA GRUBER: Wonderful. I will briefly run through the questions. So, question number one: how did you learn about this webinar? The options are Twitter, Facebook, At-Large mailing list, At-Large calendar, Skype, colleague, or other. I will give a few more seconds. Hopefully, many will be participating. As Joanna said—

JUDITH HELLERSTEIN: Can we use more than one answer?

GISELLA GRUBER: Have you tried using more than one answer?

JUDITH HELLERSTEIN: No.

GISELLA GRUBER: Judith, have you tried?

JUDITH HELLERSTEIN: No.

GISELLA GRUBER: I'm not 100% on whether you can.

JOANNA KULESZA: Judith, I'm going to try and pick this up. I'm not sure that the survey allows for that at this point, but we will note that this would be a welcome change. I understand. So, you might get that information from two different sources. At this point, please indicate the one that got to you sooner. So, choose the one that reached you first. But that is duly noted. Thank you for the question, Judith.

GISELLA GRUBER: Thank you very much for that. Just bear with me for a second while we get to question number two. Apologies. There seems to be a slight technical issue with the poll.

JOANNA KULESZA: Gisella, in the meantime, let me invite our participants to yet another webinar coming up in two weeks, since this will be the time leading up to the next ICANN meeting. Oh, I can see the question popped up. This seems to be question number one, Gisella. I'm wondering if we could move to number two?

GISELLA GRUBER: Yes. Correct, Joanna. This is question number one, and question number two does not seem to want to appear. So again, apologies for this technical issue.

JOANNA KULESZA: Okay. So, I think what we might want to do is we might want to try and wrap it up, and we will work on the survey, making sure it is available next time during the next webinar, that I just only starting advertising. Would this work? Would this be okay?

HOLLY RAICHE: Yes, that's fine, Joanna. Go ahead.

JOANNA KULESZA: I think that's how we should proceed.

HOLLY RAICHE: Yes.

JOANNA KULESZA: So please, let me just wrap up, Gisella, and we will try to get your feedback through other channels. So, the next webinar will be presented by Jonathan Zuck. We are leading into ICANN69, and we would like to invite you to talk to us about your experience with remote meetings and how to do them well, how to do them better.

So, the next webinar—the title, I'm also inserting into the chat—will focus on giving better presentations, being a capacity-building opportunity leading up to ICANN69. You are all invited and more than welcome to join us on September 21st, this time at probably a little less an Australia-friendly time, which will be 13:00 UTC.

I have inserted the link to the capacity-building dashboard. You can see all the details there of the planned and upcoming meetings. You're more than welcome to join the group to try and make these meetings as useful and as smooth as possible.

I will wrap up, thanking our guest speakers today. Holly, thank you so much. Thank you, Geoff, for jumping in with all of those very practical and very useful comments and observations. Thank you, everyone, for taking the time to join us, as already said. I welcome this as a cross-community exercise.

Thank you to Alfredo, my co-chair of the Capacity Building Working Group. Thank you to our wonderful, supportive staff. We could never do this without you. And thank you to all the interpreters making this a truly cross-cultural and cross-lingual exercise. Thank you, everyone. Have a good day, good evening, or good afternoon. Until the next webinar.

GISELLA GRUBER: Thank you very much to everyone. The webinar has now been adjourned. Wishing you a good evening, or good afternoon, or good morning, wherever you may be. Thank you very much. Bye-bye.

[END OF TRANSCRIPTION]