BRENDA BREWER: Good morning, good afternoon, good evening, this is Brenda speaking. Welcome to the Not-For-Profit Operational Concerns Webinar number six, on the 7th of April 2021, at 14:00 UTC. Today's webinar is recorded. Kindly have your phones and microphones on mute until questions are taken and I will turn the webinar over to Ioana Stupariu.

IOANA STUPARIU: Hi, Brenda. Hi, everyone. Thank you for the introduction for organizing this call once again. My name is Ioana Stupariu. I'm vice-chair of NPOC and I'm happy to welcome you here today. Glad to see so many of you returning, and I'm sure that many others will join in the minutes to come, as usual. Today, as you know, we have our sixth webinar in the series of NPOC webinars, prepared by our colleagues; Adam Peake, Patrick Jones, and their team.

Thank you once again for being present here and for all your effort. And today, you're going to a special guest speaker: Mr [Brian Huberman], who is going to speak more about the DNS security issues. But before we go into introducing him, I just want to go over the agenda for today. The one that you've received in your calendar invites.

Basically, today we are going to speak about domain name security management, HTTPS, a bit of an introduction to DNSSEC, what it protects against and how, a bit of DNSSEC implementation, and many other technical and security stuff. I for one, as a lawyer, am very curious to hear the content, because I'm not very familiar with this. So I also encourage you to ask questions, to prepare comments, if you have case studies or if

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

you have examples from your own work, feel free to raise those matters, because as you know, we try to make these sessions as interactive as possible, and as useful for you as possible.

So this being said, I wish you a great session. I hope that you will not be afraid to ask questions on the chat or during the Q&A part of the webinar, and if everything is set, Adam, back to you. Thank you very much and enjoy.

ADAM PEAKE: Thank you very much, Ioana. So, we're actually going to begin today with Patrick Jones—and Patrick, we know has spoken before—and then move on to David Huberman from the office of the CTO's office, OCTO Team.

Just a reminder, these sessions are recorded and you'll find the archive of the previous five webinars, and we'll put the link up in a moment. And also, a reminder for the course, there are two ICANN Learn courses that are very relevant to this. There's the one on registrant basics—an introduction to registrant issues, many of which we've already covered in the previous webinars—and also the introduction to the DNS. You will also find courses on DNSSEC and other security-related issues.

We'll take a look at those and probably send links to those around to the NPOC mailing list. So thank you very much and with that, over to Patrick, and thanks, Patrick.

PATRICK JONES: Well thank you, Adam, and thank you, everyone. Greetings, I'm Patrick jones from the Global Stakeholder Engagement team, and I'm happy to be speaking with you once again. I'm going to set the stage for David's talk on encrypted DNS by giving some background on how we got to where we are today with DNS privacy.

Brenda, if you're controlling the slides, can I have you move to the next one? One more. Great. So if you look back, almost eight years ago to June 2013, when the Snowden revelations first became public. It brought to light the massive surveillance on citizens, world leaders, and many people not just in the United States, but around the world.

Snowden exposed National Security Agency signals intelligence-gathering programs and this exposure of that activity is what indirectly led to the responses by governments such as the European Union's General Data Protection Regulation, financial penalties on platform providers such as Google and Facebook, but also against corporations, including British Airways and many others for data-breach violations. If you go to the next slide.

And quite a lot has been written just on the past few years, looking back at the impact of those revelations. And so I'm going to use that as the starting point to set the stage for responses by different actors in the DNS ecosystem that David will cover when he's talking about encrypted DNS. And if you go to the next slide.

The first such response was from … That I'm going to talk about, is the response of the Internet technical community. This image shows a document from the Internet Engineering Task Force that called this type of pervasive monitoring as an attack on the Internet and Internet users. If you go to the next slide, please. So this was first discussed at the IETF technical plenary in 2013 and it led to the publication of the "Pervasive Monitoring is an Attack" document in May of 2014. Within the IETF, there is a working group that is currently called DPRIVE and that's the working group that's responsible for the creation of these new encrypted DNS protocols that David will spend more time talking about.

Some of the work that has been done by the DPRIVE working group at the IETF has been developing requirements for adding confidentiality to DNS exchanges between resolvers and authoritative servers. They've also investigated potential solutions for adding confidentiality to the DNS. Defining and publishing performance data for measuring the effectiveness of these technologies against pervasive monitoring, and documenting best current practices for operating DNS privacy services. If you go to the next slide, please.

Another example of the Internet technical community's response is in this document. It's the Montevideo Statement from October of 2013. And this statement was developed following a meeting of what we call the ISTAR organizations, the Internet technical operators that collectively work together to ensure the coordination of the Internet's technical infrastructure. And in this document, they expressed strong concern over the undermining of trust and confidence in Internet users globally, due to the revelations of pervasive monitoring and surveillance.

This statement called for the acceleration of the globalization of ICANN and the IANA functions. So it set the stage for the work that led to the creation of the Empowered Community, and the changes to our by-laws, and really deepening the responsibility of different Internet actors in the work that we do within ICANN. Go to the next slide, please.

Now there have also been government responses to these revelations coming forward. Within Europe, data protection is a fundamental right and the European Union adopted the General Data Protection Regulation in 2016, it was implemented in 2018. I won't spend much time on this, because there have been many other webinars over the past few years, within ICANN, that have drilled down into this in [quite] detail. But take note, that there have been other jurisdictions that have developed their own privacy legislation.

Some of these different laws are based very much on the GDPR, but they all differ in many ways and we're seeing this in Brazil, China, Japan, Singapore, and other locations. If you go to the next slide, please. Now, from a business and consumer perspective, in 2008, Apple Computer incorporated encryption into its iOS platform.

There has been a wider use of secure messaging applications, adding encryption into platforms such as WhatsApp, use of similar platforms for communications platforms such as Signal, or Wire, and also wider adoption of virtual private networks for accessing DNS. If you go to the next slide, please.

I want to talk a little bit about public DNS services. This is a famous image from 2014, where Turkish protesters were protesting the government of Turkey's blocking of Twitter and they had spray-painted "8.8.8.8", which is the IP address for Google Public DNS. Google's public DNS service was launched in 2010, but it really took off around this time of 2012 to 2014.

And in a traditional DNS resolution model, users would take the DNS service that was provided to them by their ISP or the company network where they operate, perhaps the university where they access the Internet, and they take that as it is. But users can choose to configure their own DNS service and they can do this using a service similar to Google Public DNS.

There are others out there; Quad9, Cloudflare has 1.1.1.1, and there are other public DNS services. But in a sense, the operators of these types of services claim that they provide efficiency and speed benefits to the users, but also privacy improvements. If you go to the next slide, please. So what are some motivations, depending on the type of user that you are?

If you're an end-user, you might primarily concerned with having secure web-browsing and accessing the information that you might be looking up on your phone, or your tablet, or laptop. If you're an Internet service provider, an interest that you have is in observing and managing the DNS resolution for your customers.

You may be obligated by local laws to perform certain types of monitoring or management of content, depending on the jurisdiction. If you're an enterprise, whether that be a corporate network operator, a university, or an employer network, you're concerned about the data within your network, and also about what type of risks there may be to your employees, your staff, and the devices that are in your corporate, university, or employer network, and you want to prevent that information from leaking out to others.

If you're a browser operator, you're probably concerned about the application that acts on behalf of the user and providing the interface to connect what the user may be looking up to the DNS, so that they can retrieve that information. Go to the next slide, please.

So I’m going to give an example. This was some research that was shared at the ICANN DNS Symposium in 2019, by our friends at APNIC, and these researchers presented an example of how Google public DNS queries were being intercepted and redirected in China. If you go to the next slide.

This shows an example of a user who may have been looking up YouTube, within China, trying to access the information via Google Public DNS and their queries were being re-routed to a different name server. And again, this shows both the use of these public DNS tools and some of the issues that users face when they’re trying to access something within the DNS.

Now, I’m going to pause here, and I believe, set this up to turn over to my colleague, David. Hopefully, David is here and ready to take over. Maybe, perhaps first, I will hand it back to Adam and we’ll take any questions as we go along. But this is an overview of DNS privacy in general. So thanks very much.

ADAM PEAKE: Thanks, Patrick. If there are any questions—and I don’t see any at the moment in the chat, but if you have any questions then now would be a great time to raise your hand, but we will always keep time at the end of the sessions for any questions. But I’m not seeing anything, so I think we can probably go over to Brenda … Sorry, over to David. So David, apologies for that. If you’re ready, then over to you, and thanks.

DAVID HUBERMAN: Ah. Thank you Adam, thank you Patrick. Hello everybody, I'm David Huberman. I work in ICANN's office of the CTO. Patrick has set the table very nicely, describing why DNS privacy is good, why it's important, why it's relevant.

So, I want to show you a little bit about the fundamentals of DNS privacy, some of the technologies that are relevant today to policymaking and the considerations of DNS privacy, and goals that we may have as societies, as communities, as stakeholders, as governments. So let's talk about … Next slide, please.

We're going to talk about three different technologies. Something called QNAME Minimization, which refers to queries—the queries that we make. What is the IP address for www.example.com? That's a query in the DNS. So, how do we minimize the query for the purposes of privacy? And we're going to talk about the ones you've heard about, DoT and DoH, DNS over TLS, and DNS over HTTPS. Next slide, please.

So what you need to know is that in regular DNS, which is by far the most used protocol today, DNS send data in clear text, and what that means is your device is connected to a router, connected to an ISP, some sort of organization network that provides you access, and then that data is sent over another wire to a different server, and a different server, and a different server, and then eventually, your query, "How do I get www.example.com, what's its IP address?" a response is returned and it's got an IP address and that tells your device where to go.

All of that data is transmitted over wires. Physical lines. Are you using a wireless ISP? Are you on a cellphone and using 3G, or 4G, or 5G? Okay, it's not a physical pipe, but it is a pipe. It's a data pipe. Then eventually it hooks into physical pipes, and those physical pipes can be surveilled. They can be listened to. Governments, attackers, terrorists, hackers, all sorts of interested parties want to tap into a physical line, capture the data that goes across it, and use that data to do something.

When DNS data is traditionally sent, it's sent in clear text. It's ascii. It sends David's computer at this IP address, my computer, asked on this time and date for the IP address of www.example.com. They can see what I'm doing because it's sent in ascii, unencrypted. Next slide, please.

Importantly, there are three types of DNS resolvers. There's your device that has what's call a stub resolver where your device has a thing in its operating system that will ask the question that you need—"what is the IP address of www.example.com?"—and they will ask it of a recursive resolver that you've configured.

Your operating system's configured it automatically based on the ISP you're connected to, or in your office that your company's network has told it to, if you're at the university, that university's network has told it to be used. And sometimes governments require ISPs or require DNS operators to set recursive resolvers for the users to a government-approved recursive resolver.

But, either way, something has said, and it's done so purposefully, the answers to the questions we need for DNS so we can get to websites are on very aptly named authoritative name servers, and each DNS question is broken up into constituent parts. www.example.com is a part. Example.com is a part. Com is a part. And actually hidden to us, is there's actually a dot on the end of every domain name. You don't have to type it. The computers know that it exists, and handle it whether you type it or not. And the dot is also a constituent part. It refers to the root—the root for the DNS. Next slide, please.

This is just a simple visualization of what we talked about. On the left we have an iPhone and on its operating system is a stub resolver. And here, we're using Apple Safari as a web browser. And when you type www.example.com into Safari, it does and API call to the stub resolver, which then sends the query to the recursive resolver to be resolved—to find the answer. And it does so iteratively, to a bunch of different name servers. Next slide, please. So QNAME Minimization—we set all that up so we can talk about QNAME Minimization. It takes the message and it breaks it into constituent parts, and it only asks each authoritative named server about the specific part the authoritative named server's going to know about.

So I told you about that dot at the end of all our domain names—the hidden dot—that's for the root. So [it] first starts with the root, and it asks the root about the next part, "com". Because that's the only thing the root knows about. In traditional DNS, the resolver asks the root, "Hi, can you please tell me the answer to the question, 'what is the IP address of www.example.com?'" It gives all that information to the root server. And that's your data. You have asked about this specific website, www.example.com. But the root server doesn't know the answer to your question, it only knows the information for a top-level domain—here, .com.

So what QNAME Minimization does, is it doesn't provide all that other data. It doesn't give them your IP address. It doesn't give them the time and date of your query. What it asks is, "Just give me the answer for .com, because I know you know that." So it gets that answer and then it goes to the .com authoritative server, and it doesn't ask about www.example.com, it only asks about example.com, because that's what the .com server [has].

Finally it gets to the authoritative server for example.com and it asks the entire query, because that's the only place you can get the answer. And the whole point of this is that servers upstream of the destination don't get to know what you're really querying for. It affords you more privacy. Why should a root server operator know exactly what question you asked, when it can't answer it? It can only answer for the top-level domain.

Similarly, the .com server only knows about example.com. It doesn't need to know what specific device at example .com. mail.example.com, www.example.com, fileserver.example.com. it doesn't need to know about that query. It only is supposed to tell you where example.com is. So QNAME Minimization gives you more privacy. Next slide, please.

Real quickly, this is just a visualization of this. There are steps on here. It just shows that the root server only gets the .com, or in this case the .TLD and that the TLD server only gets the next level—example.TLD. And then, when you get to the authoritative server for example.com, it gets the www. Next slide, please.

QNAME Minimization is not a controversial technique. It's very simple and straightforward technique that nobody has argued, yet, that is in any way bad. In fact, it's widely believed it's doing a pretty okay job. It's doing a pretty good job of increasing query privacy for end-users.

Hi, Judith. Yes, the public DNS resolvers like Google's 8.8.8.8, like Cloudflare's 1.1.1.1, that Patrick talked about, are recursive resolvers. That's exactly what they are. There are resolvers set up by organizations so that anybody in the world can use them if it's to their benefit. So QNAME Minimization does and okay job of increasing query privacy, but it doesn't encrypt text. Just like regular DNS, it sends the data in clear text.

So it's not a good way to increase privacy, it's an okay way of increasing privacy. QNAME Minimization is starting become widely deployed. At least, we at ICANN suspect that is the case. So we are measuring. ICANN runs an initiative called the Identifier Technology Health Indicators Project, ITHI. It's a public website, just Google ICANN ITHI. It has all sorts of interesting measurements about the DNS, and one of those measurements is how well deployed QNAME Minimization technology is.

And in March of 2021, we found that basically a third, 34% of all queries that reach root servers were only getting the .com part, the .TLD part, which means that they were being asked queries by a recursive resolver, using QNAME Minimization.

Now, QNAME Minimization is pretty new. It's only a couple of years old. And it takes time for new technologies to get deployed. So we're at a third, roughly, by our measurements, and we think that's pretty great.

It’s a good thing. Woops how am I going … Oh, you control the slides. Brenda, next slide, please.

Okay, let’s talk about DoT, DNS Over TLS. DoT is a DNS technology that is only configured in an operating system, and it’s very widely implemented today in Android, no less. Google has turned it on by default for the newer and more modern Android operating systems in its phones and devices.

Now what happens, is when an application like a web browser requests a DNS look-up, the operating system takes that information and it encrypts it. It hashes it into gobbledygook, and when it’s sent over the wire, you don’t know what that gobbledygook means unless you have the decryption key, which only the server that’s receiving it is supposed to have. It only works between the operating system, the device and the recursive resolver.

But that’s where somebody would be sitting if they were monitoring you. That’s where someone would be sitting if they were monitoring your company, or your country, or whatever. The physical line, the cables between your device and your recursive resolver are the ones they do listen to. And so, by encrypting the DNS traffic in that pipe, so that it can only be decrypted at either end, anyone passively or actively listening on the line, cannot see, they can’t see it, they can’t make any sense of it. And in that way, their users, us, we’re assured of confidentiality because of the encryption.

So it’s a good thing, it’s a good way of increasing the privacy of our DNS queries, so that unauthorized third parties or third parties we don’t want listening to what questions we're asking, can't see those questions. Okay, next slide, please.

The big one we talk about is DoH. DoH. DNS over HTTPS. Now what is HTTPS? It's secure HTTP. It means it's encrypted. When I go to my bank, I do my banking online, I do it through my web browser, or I do it through an application my bank has, I use an iPhone, [the app,] and if I do it online, I type the address as https:// my bank's domain name, because if I only do it over HTTP, it's sent over clear text, it's not encrypted. So anyone who's able to look at port 80 traffic can see that information.

So any time you're thinking about securing a website that people access, make sure that you are doing so over HTTPS, you're accessing it via HTTPS, and if you're running it, you support HTTPS queries. Because that's better for everyone and that's a basic, fundamental web technology. For DoH, when we're talking about DoH in the real world, what we're talking about is web browsers. We're talking about Firefox, Chrome, Safari, but what we're really talking about is Firefox.

Firefox is the big browser right now that people install and DoH is turned on by default. And what DoH does is it completely circumvents the resolution process we've described. It doesn't ask the [device's] operating system to do the resolution. Instead, the web browser takes your DNS query and does the resolution itself. It packages your DNS query with all of the other HTTPS traffic that is transmitting, encrypts it on port 80 and sends it out. And it sends it out to a specific DoH server that you may or may not have configured and you may or may not know about. It gets the answer back and it displays your website, just like you asked. It takes milliseconds so you don't see it happen, you don't know it's happened, it happens behind the scenes, but it completely circumvented your operating system and it's not going out … It's going out of the pipe that's leaving your computer, but it's doing it as part of the regular web traffic that's in HTTPS. It's not distinct and it's not distinguishable from other web traffic.

And that's very different from how DNS has ever worked in the 38 years in DNS. So in green I've got … This is a good thing—nobody listening to your DNS traffic on the wire can see, they can visualize, they can identify and recognize the DoH traffic. And so our queries as users are assured of confidentiality, by way of the queries being inside of HTTPS packets that are inter-mingled.

They're part of regular web traffic. This is very good for privacy. But I've put some red text of possible badness. It's because it relies on pre-configures DoH resolvers that are run by third parties that you may not know about. What country is that third-party resolver? What legal jurisdiction is it subject to?

The resolver has the data and it has it unencrypted at the end. It absolutely depends on what country, because the resolver might be in America and maybe you don't want the United States legal framework governing your DNS data that the resolver stores. Maybe you would prefer it to be in Switzerland. Maybe you would prefer it to be in your local country. And the problem, or the challenge that browser manufactures have, is how to handle that. Because the truth is not many people, not many ends users, know what the DNS is, and those that know what the DNS is are less likely to know what DoH is.

So there are some challenges around that and we're going to talk a little bit more about that in some upcoming slides. Right, next slide, please, Brenda. So I want to talk about a couple of general concerns about the concept of encrypted DNS. Now, QNAME Minimization is not encrypted, it's just a privacy technology.

But as I've said there are no policy concerns, yet, about QNAME Minimization. But DoH and DoT and other similar technologies, they're all brand new, they're raising eyebrows. They're three years old. They've been raising eyebrows since the day they came out. They raise eyebrows in the technical community and they raise eyebrows in governments. So let's talk about two of those. Next slide, please.

The first concern, generalized concern, is the circumvention of DNS filtering for security. I'm coming to you, today, from a device that's inside of ICANN's network and the wonderful women and men who run our network have a lot of filters in place, meant to protect me and meant to protect the network from badness.

Some examples of that badness are the website that I could go to that's known to install malware. So our network team make sure we block that website. They don't let us go there because it's known to be a site you shouldn't be at. Maybe it's an e-mail server that's spewing malware. Well, the network will block that e-mail server from sending us queries, and we can do so via the DNS very easily, to make sure we can't resolve that e-mail server name, and that protects our e-mail from getting bad stuff that has malware. Maybe our machine's infected already, and when machines are infected, they're taking data that the person who controls the badness wants, and it can communicate with our machines, and our machines are communicating with our servers and we can block that very easily in the DNS. And that's this fourth bullet point as well, exfiltrating data that someone who's compromised on our machine—sending that data to them, if we know who they are, we can block them.

These are all very important filters and they're fundamental to how you build security into a network. They're very widely used. But DoH and DoT circumvent these filters, because the traffic is encrypted. It's gobbledygook. It has been encrypted by an encryption key, and the only way gobbledygook becomes useful is if you decrypt it with a decryption key. And our network operators don't have that decryption key, and so they can't see, they can't visualize, and they can't process the rules … The filtering rules—they can't process the data.

So the DNS data is not available to the filtering software and these filters break. That's not a good thing. This is fundamentally not a good thing, because in the name of privacy, which is a good and virtuous idea, we're taking away some of the protections that protect our networks from breaking down, from infecting us and making our computers useless. Or from stealing our data if we are compromised.

So that's one of the things that the technical community has been working on to try and fix. Next slide, please. There's also this idea that encrypted DNS circumvents filtering [through] local policy. Well, what is local policy? Local policy is developed at a local level at ICANN Org. It's at a local level, it's at our ISP. It's at a local level, it's our government, in the U.S. a city, or a state, or a federal government, they have a policy.

Maybe that policy is preventing users from seeing particular content. There are some countries around the world that legally forbid the access of certain URLs because of its material, or sometimes the words. Sometimes specific sites, the local governments do not want users accessing. And the best way to do this is filtering it in the DNS, it's the easy way to do it.

Maybe there's a local policy that reduces the chance of unauthorized websites from tracking users. And sometimes, in some countries, we enforce limits on the use of sites to particular hours.

All of these types of filters are very easy to implement in the DNS. It's great place to do it, because it's easy, it's very simple, it's very … Elegant's probably the right word, because it's not complicated, it's the opposite of complicated. DoH and DoT, once again, they circumvent these filters because the traffic is encrypted.

And the local policy and the filtering software can't visualize it, can't see it, it can't process it. Right, next slide, please. If you take anything away from this talk, it's that, please understand that ICANN stresses to you that increased DNS privacy is good. Technologies like DoH and DoT and QNAME Minimization and others that we continue to work on—the increased DNS privacy is good. They work towards a goal that benefits our world. So, governments that want to increase privacy for end-users could do so by asking DNS operators to implement things like DoH, or QNAME Minimization and similar technologies.

They can ask DNS operators to put on QNAME Minimization, they can ask ISPs to do it, and they can ask browser vendors to, "please turn on DoH," that can benefit the privacy of their citizens. Governments who want to increase privacy for end users could also do so by asking the operating system vendors, “could you please implement DoT at the operating system?” that would help increase the privacy for their end-users and do so in a fairly simple way.

And you know, if they did that, that’d have a really interesting side-effect. We’ve talked a bit about public DNS. People often use public DNS to get around things that they don’t like, and a lot of that is privacy. They don’t want … Hi, I’m David Huberman, I set my devices … My personal devices to [use a] recursive resolver that I trust. It’s in a different country than I live in and my ISP doesn’t get my data, because my ISP happens to take my data and monetize it, and I don’t want them doing it. So I set it to public DNS.

If governments were to promote things like these technologies, maybe end-users would be better incentivized that their services wouldn’t have to go outside that country. It’s an interesting side-benefit. Something to think about. Next slide, please.

I think we’re at the end. Good. We have one quick event announcement and then we’ll go into a little Q&A. Next slide, please. We have the ICANN DNS Symposium coming up. It’s coming up next month. The 25th through the 27th of May. It has been scheduled for the Central European time zone, which is +2 UTC, because it was supposed to be hosted in Europe. But everyone in Europe and Africa who is in +2 UTC, it’s in your time zone, for everyone else, just adjust. We’re going to do it virtually one more time.

And the theme is DNS ecosystem security. We're all in this together, because we very much are. You'll see presentations that talk about measurements, and mitigations, and progress on a lot of what we've just talked about, and a lot of what we've talked about throughout this webinar series. DNSSEC, DNS privacy, encrypted DNS, and a lot of others. We're going to talk a lot about this [in May]. It's completely free. It's happening over a few hours a day for a couple of days. The agenda will be [posted] ahead of time, so you can show up just for the things you're really interested in. Its free and open now if you just search for the ICANN DNS Symposium, you'll get to the registration form.

Okay, so we've reached the end of our presentation, and now we'll open up the floor to any question you have. I do see one in the chat from Olévié. "Is it possible to enforce software editors to implement Dot and DoH in their products?" So "possible" is a legal question, and that depends on what country you live in. And that depends on the country where the software's being made and how the laws work. So what we do at ICANN is, we generally encourage by going through the Internet Governance framework, by going through outreach and engagement efforts that Patrick, and Adam, and Brian, and many others at ICANN do, is we work with everyone, including software vendors, so that they understand the benefits and the virtue of incorporating better technologies for the purposes of privacy, if it works for their product.

That's really the best way, Olévié, to get to software vendors, is to make them understand why it's good, and why it might be a selling point—a virtuous selling point, that they can use to help sell their product.

And with your follow up, "What can NPOC members do in such a situation?" Well, that's a great question. The most important thing is awareness. The most important thing is working with your constituents in the non-profit world to, as we said last week, incorporate good cyber-security practices to protect domain names, to protect domain name registrations, to protect websites.

And on DNS privacy is to think about what kind of privacy do they want for their users, and how do we get that? We get that by checking to see if our ISPs, if our access providers support DoH and DoT, are using DoH and DoT, if it's better for us to use web browsers which have DoH on by default, if it's better for us to incorporate operating systems in our devices that have DoT on them—it's by asking questions. It's by asking questions of our vendors, of the software that we use, of the operating system that we use, and fitting it into the framework that's good for us as a non-profit organization—of what meets out privacy goals, what meets our security goals.

And as NPOC members, you want to socialize this. You want to synthesize this material that we've been sharing with you and talking with you about, and synthesize it into learning opportunities for your constituents. And again, ICANN can help you with that. Where you're able to put together more formal events with groups of constituents in your ecosystems, while you're non-profits, if you're able to put them together into an event, you could work with your local Global Stakeholder Engagement Manager, and we can help you train, socialize, and learn all of this information. We are happy to help you any time. All right, we have a hand raised. We have a hand raised from Judith.

JUDITH HELLERSTEIN: Yes, Hi. So, my question is, when you talked about Firefox and others, do they … I have two questions, one: do they only turn on for people in different countries? So, oftentimes, sometimes, you have websites that were available to you when you were in a different location, but are no longer available to you in that location, even though it's the same website.

DAVID HUBERMAN: So um, very good question, thank you, Judith. When a website is not available to you in one country, when you're in another country, can be one of two things. It can be filtering in your country. A very good example that's very public and I hope is in no way insensitive is in Turkey. For many, many years, Turkey forbade anyone in the country from seeing Wikipedia. They have now changed that policy, now if you're in Turkey you can go to Wikipedia.

I use that example because I hope it's not insensitive, but also because it happened at the DNS level. All the ISPs, all the DNS servers didn't allow … They just blocked it right there. So that's an example where that [will] happen at the country level.

JUDITH HELLERSTEIN: Yeah but I—

DAVID HUBERMAN: Hang on. Just needed to cough. It can also happen at the site level. Pretend Wikipedia wants to give a different answer for different countries. They can set up their website so that it detects what country you're in, based on your IP address, and gives you a different answer for the different country. In that scenario, which is very common, the DNS isn't implicated. It's geolocation of IP addresses, which is not a DNS [inaudible].

JUDITH HELLERSTEIN: All right, but then they put up these false things that they say, "Oh, it's a security issue," or something when it's not. And sometimes going to another browser helps and sometimes it doesn't.

DAVID HUBERMAN: Right, but that's not a DNS thing. That's a [crosstalk]—

JUDITH HELLERSTEIN: So that's not a DNS issue, oh, so using a public DNS won't help you in those situations, because there's a geolocation. [inaudible]—

DAVID HUBERMAN: Unless the public DNS is the geolocation … Matches up with what you want. Maybe you want to be in the U.S. so you use 8.8.8.8 and you get the response that U.S. people get, and maybe that's what you want, so you should use 8.8.8.8 for that. But, generally, what you're talking about is a local policy decision that is not related to the DNS.

JUDITH HELLERSTEIN: Oh, okay yeah. I was just wondering whether it was that, or whether Firefox overrides your public DNS thing because it does it by browser.

DAVID HUBERMAN: Right. Not a DNS.

JUDITH HELLERSTEIN: Okay.

DAVID HUBERMAN: Adam.

ADAM PEAKE: Ah yes, thank you. And I was thinking about the question that Judith also asked in the chat which I think you addressed in the slides, David, which was talking about filtering. And one of the issues that we hear quite often come up about DoH and DoT, is the filtering … Parental control filtering where Internet service providers must, in many cases, be mandated by a government to implement some kind of parental control so that the parent can decide what kind of access their children will, or will not be able to have.

And these can be affected by both these implementations, or certainly the DoH implementation, I think—and the people working around that. I was also thinking Olévié in the chat mentions about, how can we encourage people to sign up for DNS and then DNSSEC in their networks?

And I was remembering a buying guide. A guide you produced, David, for governments I think, and how they can address a lot of these issues in their procurement. And I think that includes encouraging governments to when tendering for networks … Provision of networks for their own government services, that they require DNSSEC as something that would be implemented. And we've also seen that with IPv6, for example.

So we'll share that document with … Ah, there you are, you shared it. And I was going to say we'll send it around or put it in the chat. Thanks very much for that. Now, I also have a question and I can see that Caleb does, as well. But I'll be a bit selfish and ask my question, which is about QNAME Minimization. So I was wondering, is QNAME Minimization something an organization needs to implement? How does deployment happen?

So, what I'm really wondering is how NPOC member would find out if, for example, [unsure] if their Internet service provider has deployed it, or if it's something that their organization should deploy or … How would you go about making QNAME Minimization happen, and is it a good thing, I suppose? Thank you.

DAVID HUBERMAN: Yeah, that's a great question, Adam, thank you very much. The DoT and DoH happen at application levels, QNAME Minimization does not. QNAME Minimization is outside of our direct control. I guess my camera has stopped working, sorry.

QNAME Minimization only happens on recursive resolver, so if we're interested in ensuring that our queries are minimized by the recursive resolver, we have to ask. We have to … NPOC members have to ask their upstream ISP, or specifically configure recursive resolvers in their networks for their users, that they know, by asking, have turned on QNAME Minimization. It's not something that we can detect. It's not something that we can go test for. It's something we actually have to ask.

Where DoH and DoT, we have much better control because we can see, we can purposely configure it, and we can see it. So good question. It's only the recursive resolver operators.

ADAM PEAKE: Okay, so yeah. Essentially then, if it's a larger NGO that's providing its own DNS then it's something that could be provided and asked to be switched on, and if not, it's probably just whoever you get your DNS servers from, I would guess from your answer.

DAVID HUBERMAN: Yeah.

ADAM PEAKE: If that's not correct let's … If I've just muddied things up—if not, Caleb, over to you please, thank you. Thanks, David.

CALEB OGUNDELE: Okay I actually didn't know my hand to be still up, but then I actually wanted to add to the contributions earlier on, based on the question that Judith asked about website issues. So I wanted to mention that one: one of the things that could happen also, is, specifically to a website, is that one: if a specific website, let's say NPOC.Org is getting some form of cyber-attack, and then I have to filter and get some IP addresses where those attacks are coming from, and I decide to filter out a block of IP address, right? The IP address which I've actually filtered could be one of the addresses that Judith is trying to access the website from, and unfortunately, she might just be unlucky to be on one of those IP address ranges, and then she won't be able to access the website.

Perhaps if [you try] the [inaudible] VPN, that could also help her in such kind of situation. So it's just adding to what has been said earlier on likely or possible issues that could posit that you can not be able to access certain websites from certain countries. And that's it. Thank you.

ADAM PEAKE: Thanks, Caleb. David, I don't know if there's any reaction to that. Ah, I see Joan with her hand up, so let's jump over to Joan with questions because we're going to run out of time in a moment. So, Hi Joan. Always good to see you.

JOAN KERR: Hi, how are you? Hi everyone. So I keep putting my hand up and down because if it's addressed then I put my hand down. So David, one of the things I always think of is, how does a not-for-profit do all of these things that everyone says for them to do? So, for example, having … I mean, I agree with everything you are saying, and I think that no-for-profits are not aware of the risk that they're at in order to mitigate some of these security issues and address privacy issues, and things like that. And I know that you answered some of the questions that NPOC members need to do this, but is there … Larger organizations can pay someone to do this. How does a small organization take steps to implement some of these privacy issues?

DAVID HUBERMAN: Thank you, Joan. It's a very good question. It can be a very challenging question, as you know. It becomes a question of resources. When we have to measure—as a non-profit, we have to measure how important certain aspect of our security and privacy are with how those synthesize with our mission, and the information we are trying to convey, and the way in which we engage with our constituents as a non-profit—the way we engage with them.

Are we engaging them through technical means, through forums, through Zooms, through whatever technology we're accessing, and how secure is that and what are the costs involved if insecurity causes problems? And when we do that type of analysis, that illuminates the kind of resourcing we need to put behind it. Now, finding that resourcing is a challenge, I understand. But when we find those resources, it's then a question of education.

Yeah, you can contract it out, but if you contract it out, you better be careful. It's about training a staff member. It's about training a set of staff members, doing this analysis and then implementing the results of this analysis. In our last webinar, we talked a lot about DNSSEC, we talked a lot about various security paradigms, and talked about important it is that everybody do these things to protect their sites and to protect their technologies. And one of the things that we stressed during our last webinar is that ICANN is here to help.

So where organizations do analysis, or do some thought and decide they want to be more secure, and they want to promote privacy, we can put together events. We can work with NPOC members and put together events where we can train, hands-on training, on how this technology works, how this technology … How you implement it from the ground-up—how you maintain it.

And some of the processes you need to follow so that it's not lost when you leave the company, when your team leaves the company so that it's all written down so that the non-profit could continue to do this with new staff in the future. These are outreach efforts that ICANN is making and offering to NPOC members, to create events and to create training and outreach opportunities. We will team with you on that. And we think that's the best, most effective way of getting some of this out there and helping individual non-profits overcome some of these very challenging hurdles.

JOAN KERR: Yeah, I think that would be a really good way because, like I said, a lot of smaller organizations don't have that capacity and so it's not that don't think that they should address it, it's just that the mission and the services are what they focus on with limited budgets. Well, thank you for answering because it's a cost that I was looking at, for people to pay someone to do it, or have a staff person do it. But it would be really good to have a follow-up seminar, just on that. So, thank you.

DAVID HUBERMAN: Right. These webinars … This webinar series that we've been together on for many weeks now, we've given a lot of information to you, and when you look through the transcripts and when you look through the presentation materials, there's a lot that you can incorporate all on your own to help with your constituents. And again, we're always available to help to work with you and team with you on that.

ADAM PEAKE: And next week we've now, thanks to David and Patrick today, we've now completed the agenda of topics that we have for this series, so next week is for review. So I think, Raoul, Caleb, it will be great if you could start a discussion on the NPOC list about topics you would like to review and we will think from our side. Brian, Patrick, David, and I will think from our side. And we'll … Also, we've spoken about what we might want to do in the future.

We've just had one example here of another webinar that would be useful. And there are other topics as well. So it would be great if you could, from the NPOC leadership side, think about how you want to have a discussion next week—what you'd like to hear a little bit more about to review if there was something that was unclear. And then what do we want to do in the future, because as David's just said, we are here to help. That's what we want to do with this series.

And of course, we're also thinking about the future activity of how do we work with you to create some presentations and materials that you can use in your own outreach and engagement work, so what we've done here can be done as a sort of ongoing basis, run by NPOC. So great to hear for next week. And we're reaching the top of the hour. I don't know, Raoul or Caleb, if you'd … I see that Ioana's had to leave the meeting—I don't know if you want to say anything before we close, but if not we'll take it to e-mail and see what we can do for next week. So, over to you [crosstalk] –

[RAOUL PLOMMER:] Yeah, okay.

CALEB OGUNDELE: Thank you so much Adam, and I would like to thank David Huberman, Patrick Jones, and Brian, as well as all ICANN staff that have made the webinar possible today. We sincerely appreciate everything you've done. And our special thanks also to Brenda who has also supported this webinar and has given us a very good platform to work with. And thanks to everyone for also attending. We do hope that we will continue the engagement on the mailing list and see you next week. Thank you.

ADAM PEAKE: Thank you. Thank you and goodbye. Thanks, Brenda. Cheers.

[JOAN KERR:] Bye.

[BRIAN GUTTERMAN:] Thank you very much. Good day everyone.

[PONCELET ILELEJI:] Thanks all, bye.

[END OF TRANSCRIPT]