YESIM NAZLAR: Good morning, good afternoon, and good evening to everyone. Welcome to the first webinar of the five mandatory ATLAS III webinars, taking place on Wednesday, the 24th of April, 2019 at 1200 UTC. On our call today are Alan Greenberg and Olivier Crepin-Leblond. We will not be doing a roll call for this webinar, however, we are taking attendance for the first 10 minutes on this call. After that you participation will not be valid entry for the required attendance metrics. If you are only on the phone bridge, please join the Adobe Connect room as soon as possible, as this is an attendance requirement.

We have French and Spanish interpretation for this webinar, so a kind reminder to people state your name when speaking to allow for the interpreters to identify you on the other language channels, as well as for transcription purposes. Please also speak at a reasonable speed to allow for interpretation. Phone lines will be muted during the presentation and hold for questions and answers at the end of the presentation. I will now hand the floor over to Joanna Kulesza, Co-Chair of the Atlas III Capacity Subgroup. Over to you, Joann. Thank you very much.

JOANNA KULESZA: Thank you very much, Yesim. Welcome to everyone participating in this second rendition of our first webinar. Welcome, we are glad you're here, we're looking forward to your questions. Feel free to put them into the window as our presenters progress. As Yesim noted, your participation in the first 10 minutes of this webinar and throughout the presentation today will be viewed as having met the mandatory

condition of participating in the ATLAS III application process. Over to you Alan and Olivier. Please demystify domain names for us.

ALAN GREENBERG: And Olivier will be starting.

OLIVIER CREPIN-LEBLOND: Thank you very much, Joanna, thank you very much, Alan. Olivier Crepin-Leblond speaking. Can you hear me correctly? That's the first question I'm going to ask today.

JOANNA KULESZA: Yes, we do, Olivier.

OLIVIER CREPIN-LEBLOND: Fantastic. Okay, welcome everyone, I'm really excited to be able to present this webinar with my colleague Alan Greenberg. I have to thank Alan for putting together the majority of the slide deck. We had a really cool session yesterday going through it. I see some people are actually so excited, they're on this call, as well, so that's really good. Just one thing, for those people that are just following us at the moment on the phone, the reason why we need you to be also on the Adobe Connect is that it's going to be very difficult for you to understand anything if you don't actually have the slides in front of you.

That's the main reason, really, because at the end of the day, you're here to learn So, yeah, if you're just on the phone at the moment

please, you've got another six minutes, I think, to be able to get online so this gets counted towards your participation. Anyway, let's get going and let's turn now to the next slide, please.

So, today's agenda is going to be looking first at the terminology related to domain names; dot com, dot net, dot org, all of these, there's a whole terminology, a whole vocabulary that goes along with it, so we'll start with that. Then, we will be looking at how the DNS works, the Domain Name System, this whole tree, the technicality of it and so on.

So, how that works, how the resolvers work, and all this. After that we'll be looking at the root zone, the most important of the whole internet, the center point, the place where you have all of the top level domains. So, we're going to find out more about the root zone. We'll look at the types top level domain, I just mentioned those, there are many types.

And then we'll look maybe at some of the technicalities related to this, including DNSSEC, all of that will be explained today, and after that we'll have a good rundown on how you can register a domain name and also what rights and obligations there are for domain name registrants. That should take us about an hour, maybe a little more than an hour, and we'll be swapping between my colleague Alan and I to be able to look at the different sections. So, I've rambled enough, let's go over to the next slide, and over the Alan Greenberg. Alan, you have the floor.

ALAN GREENBERG: Thank you very much, Olivier. We'll start with some simple things, hopefully none of this, the first slide, is a surprise to you, but maybe as

we go forward you will learn about. What is a domain name? Well, a domain name is something like ICANN.ORG. There are something over 200 million domain names registered on the internet, so it's a fair number of them. They are the prime way that a human being can access things on the internet.

Now, the internet itself doesn't use domain names. The internet itself physically uses Internet Protocol addresses, IP addresses, you'll see on the slide two examples, one is an IPv4, the type of address that's been used for most of the history of the internet, and it's made up of four sections, connected by dots.

More recently, we have IPv6 addresses, they are much larger and there are many more of them available, and they're made up of sections connected by colons. Both of those, it is conceivable you could remember them, but they're not particularly easy for most humans to remember...

YESIM NAZLAR: Alan, I'm so sorry for interrupting, this is Yesim speaking. We have an issue with the Adobe Connect audio, it's currently no audio, just please bear with me for a second, I'm going to try to disconnect and reconnect. Thank you.

ALAN GREENBERG: Fine. For those who can hear and were not on the phone yesterday, we had about six of these during yesterday's call. I'd like to think this will be only one today, but I suspect not.

YESIM NAZLAR: Testing the audio. Test. It seems that we still don't have the audio in the AC room.

OLIVIER CREPIN-LEBLOND: I wonder if someone can be heard now.

ALAN GREENBERG: Only on the phone.

YESIM NAZLAR: Okay, can we try once again? Yes, audio back.

ALAN GREENBERG: We can, I hope someone is keeping track of how long between each interruption. Where were we? Okay, we were talking about internet protocol numbers, the addresses that are used to direct traffic on the internet itself. But humans don't particularly remember long strings of numbers well and the Domain Name System is the way that we get around this. The Domain Name System maps or connects individual names such as ICANN.org with a particular address. Next slide please.

So, here's another one. This is learn.icann.org, this is the system you would be taking courses on if you weren't on this webinar. Org is the right most part, it is a top level domain. It identifies the registry, and we'll talk about that term in a little bit, that manages these names. ICANN.org, the next part -- can someone please mute whoever is

talking? Thank you. ICANN.org is the domain name and other parts to the left of the second identifier, and in almost all cases it's the second identifier, is up to the domain name owner to set up. Next slide, please.

So here in colors, we have org, the top level domain name, the second level is ICANN, and third level in this case is 'learn'; 'www' in this particular example would be the fourth level identifier and this overall address, by the way, doesn't exist, it's a nice visual example, but it doesn't exist as such. Next slide, please.

Visually, the domain name system is often structured like a tree. It's an inverted tree, with the root at the top instead of the root at the bottom, and what we have here is the root, and we'll be talking a fair amount about what the root means a little bit later in the presentation. Then we have four examples of top level domains; .org is one of them, it is a top level domain that traditionally is used for nonprofits, although there is no actual restriction on it; .ca is another example, that's a Canadian country code domain; .berlin is one new TLDs that was instituted by ICANN over the last number of years, it happens to be a city TLD, and the last one is the Chinese IDN, Internationalized Domain Name, a top level domain that happens to mean 'restaurant.' Underneath those you have the domains that individual registrants may register. ICANN is an example, and ICANN itself may have several sub-domains within it, in this case we're showing www and learn. Next slide.

So, that's the same slide, but it now shows who manages it. So, the root, again, we'll be talking a lot about the root, is the main point that you start off trying to look for things, that's managed by IANA the Internet Assigned Names Authority, which is essentially a part of ICANN

and managing IANA is one of the prime responsibilities of ICANN; .org, one of the top level domains, happens to be managed by the Public Interest Registry (PIR) which is part of the Internet Society, and ICANN obviously is managed by ICANN. Next slide.

So, how do we figure out where something is? Well, within your computer is something called a Resolver. It may be a Real Resolver, it may be a Stub Resolver, but it's a Resolver. Its job is to be given a domain name address such is www.icann.org, and figure out where it is. And what it does is it talks to perhaps other Resolvers, there may be a Resolver within your wireless modem, there may be a Resolver within your ISP, almost certainly there is, and there are other Resolvers around the internet. So it essentially says, where is this, and gets answers back, and those answers help it find the real place. And we'll now talk about the specific example of how it works. Next slide, please.

Alright, so we want to find out where let's say learn.icann.org is. So, the Resolver either asks other Resolvers or directly asks the root servers, and Olivier will be talking a lot more about the root servers, where is learn.icann.org? And the root server comes back and says, I don't know, but I know where .org is, and it gives the IP address where you can find out more about .org. The Resolver now asks the .org server, where is learn.icann.org? And it responds, you'll probably see the pattern here, I don't know, but I know where icann.org is. So each of the levels in the tree is responsible for knowing where the things under it are, but doesn't go much farther down than one layer.

It then asks ICANN, where is learn.icann.org? And ICANN says, I know where it is, and points to it, and it's done. The next slide is another

example, a very similar one. And in this case we're looking for www.iana.org, which is the organization that manages the root zone. But from the point of view of a Resolver, it's just an address, and again, the Resolver asks, where is www.iana.org? the root server says, I don't know, but I know where .org is, and it repeats that whole scenario with .org, .org comes back and says I don't know, but I know where .iana is, and it goes down and asks .iana.org servers where is www.iana.org, and it comes back with an address. And then that address can be used to reach the actual place that you're trying to get to. And now, I'll turn it over to Olivier.

OLIVIER CREPIN-LEBLOND: Thank you very much, Alan, Olivier Crepin-Leblond speaking. You've heard Alan speak about the root, the root, the root, all the time talking about the root. So, let's talk about the root. Let's go to the next slide, please.

And so the root is actually a database. It's a database that identifies what Top Level Domains actually exist. So, any top level domain like the ones that Alan has spoken to you about, like .ca, or .org, or .restaurant in the Chinese character script, all of these have to be in the Root Zone and this Root Zone is maintained by IANA, they manage it, that's one of the primary responsibilities. It accepts changes to the list of top level domains, so when there are new top level domains, it issues the request for adding them, or it processes the request for adding them, and who manages each one of them, where to find its directory and all sorts of other information, including DNSSEC information, DNSSEC is like

security extensions to the DNS, and in fact we'll be speaking about DNSSEC in a moment, after we've spoken about the root.

So, that's what IANA does. It distributes the new version of the Root for distribution to all of the Root Server Operators around the world, it does that very regularly and in fact, if you look at the next slide, please, you will find the 13 Root Server Operators distributed around the world and the reason why they are as they are now is actually quite historical. The Primary Root is what is called the A Root. You will find it at the bottom left of the screen, there you go, over here, and it's run by a company called VeriSign Naming and Directory Services.

So, IANA is the organization that is the wholly owned subsidiary of ICANN. It runs the updates on the Root, and then it tells this contractor to add or delete or make amendments to the database in the Root. And then VeriSign then has that file, which is then copied to all of the other root server operators around the world, some of which are located in the US, some of which are located elsewhere.

Historically, there were 13 of them, but of course the internet has grown so much now, that if you go to the next slide, you'll then find out that in total there are something like 980 instances of the Root Zone distributed among the different operators. So they're all copies of that root, they are local to many of those countries around the world, as you can see.

There is a concentration of them in Europe because of course every country in Europe has at least one, or two, or three copies of that in different parts of the country, but you can see that there's not a single

continent on the map here that doesn't have, well, perhaps Greenland doesn't have a local root, but others have a local root. Antarctica doesn't because it's further south, so I know that there is no actual root zone there.

But this is of course in order for the internet to be very stable and the advantages of having a local root zone, is as I mentioned, one, stability, two, the fast response rate, less international traffic when your computer comes on the net and makes a request, so there is less international traffic to try and get these root zones. It's great to have a local root zone.

Plus, if your country gets disconnected from the internet for any reason, having a local root zone, a copy of the local root, is likely to actually make it more stable, make you network more stable. So, that's why there are so many of them around the world. Now, let's have a look at the next slide, which will now show us an example of a Root Zone Entry, the type of information that you have in the Root Zone.

And here we have the entry for .hamburg, .hamburg is a generic top level domain that is used for the city of Hamburg in Germany. And you can see that the entry itself in the database has the details of the operator, including its address. It's also got contact details of a primary and a secondary contact. Often one person is administrative, the other person is more technical in nature. And then it's got all the technical configuration that actually goes in the DNS Resolver, in the system that runs the internet. You've got NS Records, which are Name Server Records, and that provides the details of the name server for .hamburg.

As Alan said, the overall root doesn't know anything below .hamburg, but it knows where to point people to for .hamburg, and so here you've got first the name, and then you've got the IP address in IPv4, so Internet Protocol address in IPv4, and then Internet Protocol address in IPv6, the more extended IP addressing. And you can see there is a primary server for .hamburg and there is another one, and there is a third one just in case one of them or two of them break down. Okay. And then there is also -- and I just had a whistle, I hope that people can hear me...

YESIM NAZLAR: Olivier? Yes, correct, we can hear you, but we have an echo, let's try to locate the echo.

OLIVIER CREPIN-LEBLOND: If it doesn't bother people too much, I can continue speaking, even though there is an echo. If we can look at the echo. Let me just continue on this. So, you've got the NS Records which are at Name Server Records, and you've got the DS Records which are at DNSSEC Records, the Domain Name Security Records, and you can see the set of undecipherable data there, which are alphanumeric in scope, and these are, of course, the DNS keys, they're electronic keys that will be used to secure the domain. And then you've got some metadata that's included, including maybe the website of .hamburg, and also the address of the whois system for .hamburg. And in fact, whois is the system that is used to see all of the details.

So, let's go to the next slide, please. And I note we can't find out where that echo is at the moment. So, I spoke about DNSSEC, and DNSSEC is a thing called Domain Name System Security Extensions, and that's used to protect the Root Zone and to protect many top level domains. Not all top level domains are signed with a DNSSEC key, so unfortunately not everything is secured, but it may be used to protect domain names, it could be used to protect a whole zone, a domain name, indeed, anything that goes from the top level domain all the way down to the second level, the third level, et cetera. "Protect" means that someone who takes the trouble to check DNSSEC, of course, will detect if the entry has been tampered with, or not. Unfortunately, the current status is that because the internet is really on a best effort basis, not all operators use DNSSEC, not all domain names are assigned by DNSSEC, and not all operators check for DNSSEC records. So, we're in a bit of a problem with regards to that. Have we found out where the, no? It's still there, okay.

So, then you may be thinking, well, okay, so does DNSSEC work? And the next slide is going to take us through an example.

So, let me pick my little green arrow, I hope you can all see it. Let's say we want to go to www.majorbank.se. As Alan told you earlier, you've got your local DNS resolver which is usually located either in your own router or it's located in your internet service provider, so you type in www.majorbank.se, the DNS resolver locally says okay, let me forward this over to the top level domain server for .se, and it goes over to the top level domain server for .se, and it does the whole thing, as Alan showed your earlier...

ALAN GREENBERG: Olivier, we're out of sound again.

OLIVIER CREPIN-LEBLOND: Oh dear, okay. We're out of sound and in the meantime we still have an echo, I'm not sure where that comes from.

YESIM NAZLAR: Olivier, this is Yesim, I'm sorry, we're still trying to locate where the echo is coming from. Meanwhile, I will again try to disconnect RBO and reconnect back on Adobe Connect.

OLIVIER CREPIN-LEBLOND: Thank you, Yesim. In the meantime this little break is allowing me to read the comments that are being made at the moment.

YESIM NAZLAR: Olivier, I think your echo is gone.

OLIVIER CREPIN-LEBLOND: The echo seems to be gone, yes.

YESIM NAZLAR: And I'm still working for the Adobe Connect, apologies for the delay. Okay, it's back now, thank you.

OLIVIER CREPIN-LEBLOND: Thank you, Yesim. Let's welcome everyone back, sorry about this. Let's start again, because I'm not quite sure where I lost you. So, I want to go to www.majorbank.se. My local DNS resolver, usually that's based at my internet service provider, is going to forward this request to the top level domain server for .se. Either that, or it will basically interrogate the root and the root will say right, the top level domain server for .se is this server, it will go over to the .se server, the.se server will point to the .majorbank server, and ultimately we will be receiving an answer back from the system which will tell us www.majorbank.se has got the IP address 1.2.3.4.

And therefore my computer will then get the page from a web server at 1.2.3.4, and in response I will be receiving the web page from this web server, which will be the sone for my majorbank, I'll log into it, I'll use my username and password, get the account data, et cetera. So all of that is all fine and great, when it all works well. Now if we go the next slide, please.

What basically happened is that there actually are not just one customer for majorbank.se in my ISP, but there are many, many of them, and so for some domain, there are several hundreds, if not thousands of queries about the same domain, and that, of course, creates a lot of international traffic, and as a result, the important thing is that I need to, well, the local server, the DNS resolver is able to cache the information, rather than having to ask the overall DNS server which might be some distance, in order to answer faster, it caches those

results and maintains a local copy temporarily, and it responds right away. It says, oh, I know what majorbank.se is, it's 1.2.3.4.

And again, we're able to go over to the web server and everything works well. But of course, this was then. One thing that one can find is, well, there's a way to try and hack the system, and the way that hackers have found over the years is to actually say well, what if we attack this DNS resolver, this local DNS resolver, and we poison it with the wrong information, then we can direct the traffic to our own website, rather than directing it to the major bank website. Let's go to the next slide, please.

So, that's exactly what this attack is, the DNS Cache Poisoning Attack. In this system where the attacker monitors the traffic on the internet and it monitors the request for www.majorbank.se. Once it finds that from the DNS resolver, the local DNS resolver that we have here, it poisons that. It basically answers faster than the internation normal DNS server answers, and it say, wait, wait, you need to go to 5.6.7.8. And so the local DNS resolver returns to your client, to yourself, returns the IP address 5.6.7.8. It does that very fast.

And so, because this whole thing is again on a sort of first come first serve basis, your system says, okay, let’s go to 5.6.7.8 and you end up connecting to a webserver that looks exactly like your major bank, it's got a log in page, that's got the username and password request, and so on, and you end up typing your username and you type your password, and the website returns and says oh, sorry, there's an error, try again.

Well, try again, because now it doesn't care, it's got your username, it's got your password. And the hackers keep that in the password database and use it in order to be able to take all the money and do all the things that they want to do inside your account in your major bank. That is something that has happened not just once or twice, but thousands of times, and therefore something needed to be done very fast to counter this kind of attack, a real major, major attack. So, let's go to the next page, please.

In order to do that, what happened is that the system called DNS Security Extensions was added, so that every query from a DNS server would include also the use of a private key and a public key infrastructure. So the overall root, so for .se, would be signed by the private key and the public key, and then the .majorbank domain would also be signed using DNSSEC. And that actually, if the response is given with this system, it actually guarantees that the response comes from an authoritative server and not from an attacker.

So, your local DNS resolver that runs DNSSEC, that checks DNSSEC would effectively ask for www.majorbank.se and if an attacker responds very fast and says, oh, it's 5.6.7.8, it would not actually have the private key of the private/public key system, and so your DNS resolver, when it checks the response with, sorry, that is a fake response, that's not correct and it doesn't validate, I'll drop it. And therefore that gives the chance for the real DNS server with DNSSEC response, and provide you with the real details, thus receiving the answer 1.2.3.4, and 5.6.7.8 being dropped out. And that was the way to basically get rid of this type of a hack.

As a result, you get connected to your own bank and you don't have an overall attack on your service. That's one of the things that is needed, but as I mentioned earlier, if your DNS resolver does not check for DNSSEC, then it's not going to be finding out the difference between a fake response and a real response. Let's go to the next slide, please.

So, as we said earlier, there are three main types of Top Level Domains, each one is managed by a registry. There are Country Code Top Level Domains (ccTLDs), they are managed on behalf of countries and territories around the world. They are very different from the next type, which is the Generic Top Level Domains (gTLDs), because the gTLDs have a contract with ICANN. The Generic Top Level Domains are like .com, .net, .org, and so on.

And then you have the Legacy TLDs, .edu, .int, .gov, .mil, .arpa, that are not actually run by ICANN. As such, they don't have a contract with ICANN, and Alan, I think might be able to give you a little bit history on this. But the three different types are there. The important thing is that the Country Code Top Level Domains don't actually legally have a contract with ICANN as such, so each one of them has got its own rules.

The Generic Top Level Domains have their rules set by the Generic Name Supporting Organization in ICANN; in a future webinar we'll be telling you all about the Generic Name Supporting Organization. But the Country Code ones are completely independent and the only thing that they are subjected to is to have rules and technical qualities that do not actually break the internet, as such. Let me hand the floor over to Alan, because he can take you through this and through the next few slides. Alan Greenberg.

ALAN GREENBERG: Thank you very much. Next slide, please. Alright, so we just talked about Registries, the organizations that oversee and manage each top level domain. The next term that we often hear about in ICANN is Registrar. Now historically, if you go far enough back, the only domains that were available were .com, .net, and .org., and you went to the same organization that ran them was also the place you went to, to obtain your own.

With the formation of ICANN, it was felt it was very important to split the function over two different organizations. So we have Registries, and now there are a lot more of them than there were before, and we have Registrars. Registrars are the type of organization you go to, to obtain a Second Level domain, a regular domain within .org, .com, or any of the new ones. Registrars are accredited by ICANN, so you can't just decide you want to be a registrar, you have to get approval from ICANN. You have to get approval from each Registry to actually be able to deal in their domain.

So once you are a Registrar, that still doesn't mean you can make any domains available to anyone unless you have agreements with specific registries, and some have agreements with select registries, some have agreements with many registries. Moreover, a Registrar does not have to actually deal with the public themselves. They can have Resellers who act as agents for that Registrar and in fact, Resellers can have Resellers, and a Reseller who is a Reseller of a Reseller, can have Resellers.

So the tree structure can go quite far down. Prices are set by the resellers and registrars, there are no price limitations set by ICANN, per se. And registrars and resellers compete with each other based on price, based on services they offer, and most registrars will offer some level of service, many will offer websites, many will offer privacy services, we'll talk about privacy a little bit later, and things like DNS servers. Next slide.

So, let's say you want to have a name of your own. This discussion is primarily related to gTLDs; ccTLDs all have comparable processes, but they each are decided on by each ccTLD and they don't necessarily follow the same type of rules as we do here. Some of them, but some of them do not. Next slide.

So, the overall process is, if you want a domain, first of all you have to decide what top-level domain do you want, and what second-level domain do you want. Then you have to select a registrar or reseller, you have to check the availability of your choice, decide how long you want to register it for, and then you have to complete the process, including payment, of course. And recognize a domain name is just a name, it doesn't provide email, it doesn't provide web services, although any given registrar may bundle those services together, depending on who you select. Next slide.

Okay, Top Level Domains, we talked about them a little bit. We have .com, .net, .org which were the original ones that were available for registration essentially by anyone. There were a number that were put in place by ICANN in the early 2000s, examples are .biz, .info, .aero, .travel, .museum, .asia, there are a couple of others. And then in the

2012 round there were about 1200 new TLDs authorized, and there are examples on the slide.

Plus, you have ccTLDs and you have IDN TLDs which might be cc or they might be the generic top level domains. IDNs are Internationalize Domain Names, which use character sets other than simple Latin characters to create the name. Again, we'll talk about that a little later. The rules vary for each one, there may be rules associated with who can register in a top level domain, there may not be. And the prices, of course, can vary all over the map. Next slide, please.

So, if you're going to register your own name, the obvious question is what is it? Is it named after you? Is it your proper name? Is it named after your company? Is it a product? Is it the name of your club or association that you want to have a website for? You have all sorts of options and people pick different ones to try to make their domain name memorable, because very often that is going to be a key issue, will people remember you? Is it catchy? Is to long and complex that people will never type it in. There are all sorts of questions you must ask about just what name to you want. Let's say you pick one, though. Next slide, please.

The next step is to figure out, who are going to deal with? There are big, big companies that are registrars, the largest registrars have a very significant percentage of all the domain names on the internet, and there are other ones that are very small and specialized. Many registrars have target audiences, so there are registrars that target their business at At-Large corporations, for instance. They offer services that are particularly useful to those corporations. There are others that

target individuals, they may offer Web services and things like that, that a large company doesn't need, but an individual might need.

And, of course, there are resellers who also have similar sets of offerings. And to mention it once more, and I'll mention it again later, prices vary. There may not be a lot of sense why one domain at one registrar will sell for $10 USD, and the same domain from someone else might be $100 USD, but it's up to you as the consumer to pick someone that you feel will do a good job for you at a price that you think is reasonable. Next slide.

Okay, let's say I decided I want blahblahblah.com. For one reason or another I've decided this is the name I really want. So, we need to check, is it available, or has someone else already registered it? And there are a number of ways you can go. You can go to your own registrar or reseller, they probably will have a WHOIS service, usually on their home page, where you can type an address, a name, and find out, is it available or not. There is also a server that is on the ICANN website that will tell you who owns a given domain, if indeed it's owned. Next slide.

So, if I enter blahblahblah.com, I'll find it does exist, someone has registered already, it happens to be owned by Condé Nast...

YESIM NAZLAR: Alan?

ALAN GREENBERG: Yes.

YESIM NAZLAR: I'm so sorry for interrupting, once again we have the same Adobe Connect issue. Please bear with me.

ALAN GREENBERG: Then we'll take a pause.

OLIVIER CREPIN-LEBLOND: For those people that are on the dial up, it's Olivier speaking here, for those people that are on the dial up, we had the same problem yesterday and we ended up being cut, I think each of us, twice, so Alan is now on 2, I'm on 1, so he's taking the lead. We'll see if I get cut off in the future, as well. But is is a little annoying, sorry about that, everyone.

ALAN GREENBERG: I'd be willing to make a bet that you're going to be cut off at least once, Olivier.

OLIVIER CREPIN-LEBLOND: I definitely will be, every 20 minutes or so, it cuts off. And there are a number of questions in the chat, we will answer either on the chat or afterwards, when we'll be able to answer questions, so we'll take note of the questions in the chat that haven't already answered.

YESIM NAZLAR: Sorry, it's taking a bit longer than expected this time, I'm still working for Adobe Connect to reconnect the audio back.

ALAN GREENBERG: Are we good to go?

YESIM NAZLAR: Yes, okay, audio is back.

ALAN GREENBERG: Alright, then back to Slide #28. We see that blahblahblah.com is in fact already registered, it's registered by a company that publishes magazines. Why they have that as their domain, we don't know, but that doesn't really matter, it's not our business, but it is not available. Next slide, please.

Now, let's say you really want it, well, you may find among other things that although it's registered, it's not used. There are many, many domain names that are registered on the internet and are not actively being used, many of them, in fact, are registered by speculators, by people who are in the business of buying domain names and hoping they can get someone to buy it from them, obviously at a price higher than they paid, and make a profit on it.

So, the domain name you want may be available from somebody, and very often if you just go to the name, it may tell you, you can buy it, sometimes it will give you a price, sometimes you have to negotiate it. You can also, there may be a name which looks like it's not being used

because it doesn't have a web server on it, but it is being used for email, for instance. So you can always try to buy it from the owner. That can be very expensive.

There was a case reported in the Washington Post yesterday of someone who decided they really, really wanted a domain name and approached the owner at gunpoint and forced them to transfer the domain. I don't recommend that methodology, that person is now in jail. But you can see to what extremes some people go to get the name they really want. Next slide.

Let's say you can't buy it, or you choose not to go to those extremes, then you can change your mind. You can pick another name, and hopefully it is available. You can also take blahblahblah and say well, I don't really need .com, I'll use .cloud, or something else, and assuming there are no rules associated with stopping you from buying a .cloud domain, you may solve your problem that way. Next slide.

In this case, if you check blahblahblah-today.com it is available, and you can proceed and register it. Next slide.

And the registration process is pretty simple. You have to provide your contact information, so they can find you, you have to decide how many years to register a domain and a generic TLD you can register for anywhere from 1 to 10 years. You have to pay for it, and it's yours. And you are not officially a Registrant.

And lastly, one more slide, and we'll talk about prices again, because it's one of the subjects that confuses people most. Why do prices vary so much? And the answer is they vary because registries pay have policies

on what their domains are, registrars and resellers have practices, if a domain name sounds like it's worth a lot, it may have a higher value, depending on who is selling it, and what services the registrar or reseller provides along with the domain name, may vary heavily.

In fact, there are many places that advertise websites, and for several dollars a month, you can get a website and they will provide the domain name for free the first year, and after that, of course, you will have to continue paying for it yourself. So all sorts of things can change price, and it's up to you, the consumer, to decide what value these things have. And I believe I am now transferring this back to Olivier.

OLIVIER CREPIN-LEBLOND: Thank you very much, Alan, Olivier Crepin-Leblond speaking. By now you must have all noticed that Alan always gets the parts which are fun to talk about and the positive stuff, and I constantly have to talk about the negative things, or potentially negative things. But anyway, alright, let's go to the next slide, please. When you register a domain name you have to provide personal Information about the registrant, of course, contact information to register the domain, and that's quite important, of course, in the whole overall thing, because they need to be able to get in touch with you if something goes wrong, and so one.

The WHOIS database was open for everyone to be able to consult for a very long time, so all of the information you were giving, whether it was your name and address details, telephone number, email address, and so on, used to be all displayed publicly. And since the European General Data Protection Regulations (GDPR), I know that in French the acronym

is RGPD, these have now made it that the amount of information that is displayed is greatly reduced.

We are in the middle of the work of the working group that deals with this general data protection regulation for ICANN, they have already worked in the first phase on what information should be in the database. They are now working together, they're just starting the work, to find out the different types of access that one is going to have, so the qualifications or accreditation that would be needed to be able to access such and such, and information about the owner of a domain name.

In the meantime, there are proxy services that are available, which have always been available, which for a small fee are able to act as a go between, between you and someone else, so they would have an email address that would basically forward any email over to you without giving your details and they would cover the information about you, any personal information about you. These are still in place, and are still being shared there.

Now, of course, that means that you can be contacted, and if we go to the next slide, you will find out that if you do have a domain name, you do open yourself to all sorts of domain name scams. Messages that you will receive, that will tell you to renew your domain name and of course these things are renewable yearly or sometimes after five years if you register it for several years at the same time, you don't really remember who your registrar is and so they try and play with us.

If it's from your registrar of course this is legitimate it's a legitimate renewal request, but if it's from others, it's probably a scam. It probably is just trying to either get your transfer that domain name to them one way or another, or something where they just basically take your credit card details to pay for another year or another five years, and they don't renew your domain name at all, they just pocket the money and run away with it. This sort of stuff exists, unfortunately, on the internet and there is a lot of it.

And I can tell you from experience, the number of emails I receive about renewing some of the domains that I own, my personal domains, is quite ridiculous. There are also messages that you would receive about search engine optimization, making it sound like if you give them money to optimize the search engine placement of your domain name, you end up with something that is going to absolutely beautiful, you will be on the first page of Google, and so on.

But of course, if they tell everyone this, then how in the world is everybody going to be on the first page of Google. So it really makes it sound like it's something you must do, but it's not something that you must do, as such. And then, of course, you also will receive some emails telling you about other extensions, other domain name extensions that you could have, so if you own alangreenberg.org, of course, you would be interested in alangreenberg.stuff, and alangreenberg.com, and alangreenberg.info, and alangreenberg dot pretty much anything else in there.

And this again is something that you would receive. And there are tons of other scams, as well, out there, unfortunately fraudsters have this

amazing ability to think of new ideas much faster than most of us. So that's the sort of thing that you open yourself to. If we go to the next slide, please.

Now, let's talk about something a little more fun, and that's Internationalized Top Level Domains. Alan mentioned it a little bit earlier in that you were looking at the top level domain with Chinese characters saying 'restaurant.' So, these are effectively, until I would say about 10 years ago, a bit less than 10 years ago, all the domain names in the world use to be in the Latin character script. So, we're talking the alphabet, a, b, c, d, e, f, all the way down to z, and 0 all the way down to 9, and that was it. You couldn't type in any other languages than in this Latin character set.

And of course, as we know, the internet has become so international these days, that a majority of people are using other character sets now, not just Latin, but you've got Chinese and Cyrillic, and thousands of different scripts out there. And so there was a real push to get both some country code top level domains to be in Chinese, and also some generic top level domains to be in Chinese.

There are two ways to display those. There is what we call the U-label, which is the actual that you see here in the actual native character set itself, that would actually be displayed usually on the web browser or in your email addressing system. But then there is the actual technology behind things, and the technology being quite a few years old, actually still runs in this standard Latin character set, using these xn-- labels; that's the A-label.

So, each one of those new labels has got a corresponding label in the Latin character set, you don't see that, this is where the technology works, and the whole system is coded using a system called Unicode, that was developed by the Internet Engineering Task Force and also the Unicode Consortium, and they came up with the whole coding of all of these character sets, and there are many, many different types of them. Let's go to the next slide to get a few examples.

So, here for example, you've got räksmörgås.josefsson.org, so you can mix Latin character sets with non-Latin character sets. Here we have a Swedish script and oops, I just pressured the wrong button. What happened there? Did I just crash? Sorry about that, well, I'll continue. So, you've got the Latin character set first, räksmörgås.josefsson.org, then you've got one which is in Chinese character set, under .asia, and you've got one which is in Hindi script, that is along here -- let me try, I'm just trying to re-log in when I'm here, because for some reason I was logged out. And then you can also have a mix between Latin character sets and the Hindi character set, and you can click on any one of these, by the way, they all work, they all work really well. There are things called variants. If we go to the next slide, please.

You will find that we have things called Variants. Now in some scripts, such as the Latin script, there actually is no difference between using uppercase and lowercase letters. So .org all in lowercase is totally equivalent to .Org with an uppercase O, or .oRG the other way around, or everything in uppercase. But in some character sets like for example Chinese, you could actually write the same word in two different ways. You can see here being .restaurant in Simplified Chinese character set and Traditional Chinese character set.

And in this case, the DNS actually treats them differently. It's not the case for all those Variants. In some cases the DNS treats them the same. And that's where you get this problem of Variants and there are some tables which have been created for each one of those character sets to find out which ones actually are equivalent and which ones have to be treated differently, whether it's in Chinese, Cyrillic script, or other script.

If you're interested in this, there is actually an interesting link and it's on the page here, https://www.iana.org/domains/idn-tables, and you will see the work that is taking place, and many people in our community have taken part in this work by working with linguists and with the ICANN department in charge of internationalized domain names to be able to extend those variants and work with the different character sets. I think some of the more recent ones, the Greek script, there was also a very recent one, we're talking about a matter of weeks, was the Hebrew script. So it's all growing and it's still history in the making. So, if you're interested in this stuff, then please do check it.

Alan has actually written also the thing with regard to variants, and maybe he'll be able to talk about it in a second. But that's effectively the whole thing about IDNs, and there is a lot more to be talked about and we could have a whole webinar about them. But we thought we would touch on these because they're quite important. Alan Greenberg, you have the floor, you can take over, now we've gone into some nice stuff, agree. And now we might have lost Alan.

YESIM NAZLAR: This is Yesim, I'm just double checking that Alan is unmated. Alan, you should be able to speak now.

ALAN GREENBERG: Alright, can you hear me?

OLIVIER CREPIN-LEBLOND: Now we can hear you.

YESIM NAZLAR: Yes, we do.

ALAN GREENBERG: Alright, I didn't do anything, someone did magic. Alright, what I was saying is just finishing off on Variants, Variants were not considered when the new TLDs were first released and they were considered different languages.

As a result, you ended up with some rather interesting anomalies that it is conceivable in some domains to register two variants by two different people and so essentially we have the same name, perhaps written in traditional and simplified Chinese, or in many other languages they have Variants, but they both can exist in parallel and for different purposes, and that could certainly be rather confusion. There is a lot of work going on right now to address that. Next slide, please.

Olivier said I only do the fun parts, I don't think these are the fun parts, but we may...

YESIM NAZLAR: Alan, sorry for interrupting, the audio is gone again, unfortunately.

ALAN GREENBERG: Alright, I will pause.

YESIM NAZLAR: Thank you.

OLIVIER CREPIN-LEBLOND: We're still waiting for the audio to be connected. Testing now. Does it work? I think it works now.

YESIM NAZLAR: Olivier, yes, the audio is back.

ALAN GREENBERG: Thank you very much. It is Alan Greenberg and we'll try again. Olivier I think I'm winning in terms of the number of failures during each of us talking. I'm not sure I want to win this one. Alright. We're on Slide #39 for those who are watching their own slides. Is there a problem?

YESIM NAZLAR: No, Alan.

ALAN GREENBERG: I guess not, okay. As a registrant you have a number of rights. Once you register your domain name, you can use that domain name subject for pretty much anything you want, subject to the rules that any given TLD may have, many TLDs have no such rules, others have very specific rules, and subject of course to applicable laws. For gTLDs you can expect to be notified when your domain is going to run out, and that presumes of course you gave valid contact information and you can presume what the price is, a registrar is required to post on their website what the renewal price is, not always easy to find, but it must be there somewhere. But of course, over time it can change, and very often the price they charge you for the first year or years is not the same as the price for successive years. Next slide, please.

Along with rights, you have certain obligations. You must provide accurate contact information. Now, certainly pre GDPR there is an inclination of some people to provide false information so that the information displayed is not real, and they can't be bothered. There are proxy services that will hide the information for you for a price, but some people have chosen not to provide information. But if you are known to provide false information, your domain can be taken from you. And moreover, you must keep it up to date.

If for instance the email address you gave was valid at the time you registered, but you have now changed your email address, something people very often do, you are obliged to notify the registrar and keep it up to date, and that's regardless of whether it's public or not, you must tell the registrar. And of course, the penalty for not doing that is you may not find out that there's a problem with your domain. You may not find out that your credit card is no longer valid, or for some other

reason your domain is going to disappear. And of course, you can't use it to defraud or impinge on other intellectual property rights. And lastly, despite the fact that you should be notified of when your domain is about to renew, you should keep track of those dates yourself, because the problems of not keeping track is you could lose the domain name. Next, please.

And that brings us to Domain Renewal. You should renew a domain prior to expiration. For gTLDs, if you don't, there is a 10-day period in which the domain will stop working, but you are still able to renew it. The price may be different than it would be before renewal, those prices must be posted on the registrar website and it may be different than the pre-renewal price, but after that period of time, for gTLDs, the registrar and registry may give you more time, but they may not, and could easily lose that domain with absolutely no recourse to get it back. And if you're running a business on that, that obviously can have real implications. So name renewal is a critical issue to consider if you are going to become a registrant. Next slide.

We spoke a lot before about selecting your registrar. Well, once you have registered a domain name, you can transfer it to another registrar, there is no fee for doing that, but you must add at least one year onto the registration if you do that. There are some restrictions that apply for when you can do a transfer, you can't do it necessarily too early or too late in the domain name's life, but in general you can transfer.

Moreover, you can sell your domain to someone else. If you have acquired a domain name then you have the right to that until it expires, and you can sell that right. There are services that will auction it for you

and essentially that's just a private transaction. And as I mentioned, there are people who specifically acquire domain names just to sell them and hopefully make some money on it. And I'll turn it back to Olivier now.

OLIVIER CREPIN-LEBLOND: Thank you very much, Alan, Olivier Crepin-Leblond speaking. We just got a few more slides to tell you about domain names, and yet again, I have to take you to some problem that you might be faced with when you have a domain name. Let's go to the next slide, please. This one is talking about Intellectual Property issues. You do have a lot of domain names that are registered out there with the intent to possibly take unfair advantage of trademarks, or intellectual property rights.

So people that basically try and get the traffic from those, either try to gain the traffic from those domain names, or make it look like they are from those companies to commit fraud, or whatever, and you've got some examples here, face-book.com, for example, with a dash between face and book. This one is quite obvious, obviously most people wouldn't use the dash between face and book, but look at the next one, g00gle.com, this is one with the two o's of Google actually being zeroes, and it is very difficult to differentiate between the fake G00gle and the real Google. A

nd the next one that is even worse, and I think Oksana spoke about this. Oksana Prykhodko wrote something in the chat about that and said what about the mix, when you start mixing Cyrillic characters with Latin character sets, there is a danger of fraud on this, and indeed, in this

case, the k, looks a little bit funny in the script, but they are Cyrillic script because all the foreign letters are Cyrillic, it looks like the word "coke" but it is not the word "coke." So, they would be able to register this domain name and make it look like it's the real thing, but in fact, it's not the real thing. Let's go to the next slide, please.

For this type of problem, there are a number of systems in place in ICANN to have a prompt resolution process. The first one is the Uniform Dispute Resolution Process (UDRP) and that is a process by which you can file, if you are an intellectual property owner, so you own a domain name and you've got the intellectual property rights to that domain name, to that string, you can then file a UDRP, Uniform Dispute Resolution Process or if you don't own that domain name and somebody else registers a domain name that allegedly infringes on your intellectual property rights, then you can file a Uniform Dispute Resolution Process and you also file for a Uniform Rapid Suspension (URS).

So, these are internal systems in ICANN with an external panelist that will look at they will be dealt with quite fast. But they are really designed to avoid such problems, and in an international manner that we have today, having to go to court and so on might be very difficult, as you know, there is no international court for this sort of thing. But this is kind of internal processes to help out with that.

For new Generic Top Level Domains there is also a thing called the Trademark Clearing House (TMCH) and that allows for trademark owners to register their name and get priority access to the names themselves. So, when somebody decides to register a domain name

under that top level domain that might infringe on your trademark, you will be notified as the trademark owner, you would be notified that somebody is registering something under that name, then they would also be notified that by registering this name, they might be infringing on your trademark. I'm saying 'might,' because there is a big difference between domain names and trademarks.

As you know or you might not know, trademarks are actually quite restricted. They work in a class, so you would have a trademark that is by activity, you could have a trademark for a company that sells cars, that is restricted to just trademark for selling cars, and then somebody else would have a trademark for selling apples, and they would be the same name, the string as your trademark, but that would be restricted to just selling applies, and that is actually entirely impossible.

But there is also a second thing, in that trademarks also have geographic delimitation. Which means that somebody could have a trademark registered in the United States, and another person could have a trademark registered in German, it could be the same trademark. If there is no trademark extensions, you would have those trademarks only specific to some countries. And unfortunately the internet, being what it is, domain name do not have boundaries. They are all global, so a string as such could infringe on trademarks in any number of countries, in fact multiple numbers of countries. And I see there is no sound again, is it working?

ALAN GREENBERG: Olivier, it does seem to still be on.

OLIVIER CREPIN-LEBLOND: Okay, thanks, I was getting worried that I was going to catch up with you. So that's what you get for trying to help out with intellectual property issues, and there is a lot of that going on. And if we got to the next slide, please.

We're soon reaching the end of this discussion and in fact this is quite a complicated field altogether, between the trademarks, the fraud, all of that, and of course the way the whole system works. So, if you want to register a domain name or you've already registered and you've got a problem with anything, any questions, of course, your first point of questioning would be your registrar's help desk. Hopefully you will have purchased it from a registrar that has a help desk. They should have all sorts of good information for you.

There is also ICANN's website. There is whois.icann.org, and I've just noted that we've forgotten one slash here, there should be two back slash after https. That's available in multiple languages and that's the database by which you can find out who the owner of a domain name is, and who the registrant of a domain name is. And then you've got a link to the compliance department.

If you find a problem with a domain name, you have a complaint to make about the domain name because it either infringes things or there is something wrong with it as such, then you have a form that you can fill in for the ICANN Compliance Department, the link is there. If you have a problem with a Registrar, I would suggest that you read that

announcement from all the way back to 2007, it's a link to this information, very helpful, indeed. If we go to the next slide, please.

You'll get some more links in this last slide, other useful resources. There is a link to the Australia's Competition and Consumer Commission, they have a whole section on domain names and registration of domain names, and so on. There is the eConsumer website at http://www.econsumer.gov/ which is very helpful, as well. Obviously, there is the ICANN website which has a whole section on being able to help you out. We've got the At-Large website, the United States Federal Trade Commission also has some web pages that relate to domain names.

And I also wanted to let you know that this presentation that we've just done here is actually based on the ICANN Learn course, the corresponding ICANN Learn called Domain Names Demystified. So if you're interested and you would like to learn a little more, there is actually more in the ICANN Learn course. There are a few videos in there, there are a few more things, so that's one thing.

And the whole ICANN Learn course was actually based on printed material that was the Domain Names Beginner's Guide, that was written in 2010, if you're interested printed material, then you can go in that section and check it out. So, that's it, I guess, for this webinar. But we have time for questions and there are several questions that we've collected in the chat.

There was one which was, "Who decides to set up a resolver? Is it a company or an ISP? Alan? What do you think?

ALAN GREENBERG: Well, the answer is anyone can set up a resolver. If you run Windows, you have a stub resolver, which is not a real resolver, but relies on the next one down the chain, but you could install a real resolver into your machine. You could install a real resolver that does DNSSEC checking. So, such things are available.

If you're running an ISP, you pretty well have to install a resolver that will provide services to your users. There is no restriction on who provides resolvers and if you were around when we changed the DNSSEC key a few months ago, one of the problems was it's not possible to know exactly who is running resolvers and who is running DNSSEC resolvers. So one of the problems with the overall thing is it is distributed, anyone can do it, and there are no rules on it.

OLIVIER CREPIN-LEBLOND: Thank you, Alan. The next question also in the chat was, "How are abuses by ccTLD registries handled by ICANN, IANA, or the internet community?"

ALAN GREENBERG: Basically ccTLDs are on their own. So if the abuses are things that effectively break the internet or violate the few rules that ICANN has, presumably ICANN could try to take some action, I'm not quite sure what action could take legally, and there certainly aren't a lot of instances of these kinds of things happening, so I don't have a lot of history in it.

But, abuses for things that are not against the rules and don't break the internet, it's up to each ccTLD to enforce their own rules, and indeed, some have rules that others might consider abuses, but are in fact within their rules, and they're not technically abuses. So, the ccTLDs are to a large extent a world unto themselves. ICANN does have some authority if a ccTLD must be re-delegated, that is, must be transferred from one entity to another.

YESIM NAZLAR: Alan?

ALAN GREENBERG: Yes?

YESIM NAZLAR: I'm sorry for interrupting, it's the Adobe Connect audio issue again.

ALAN GREENBERG: Alright. If the interpreters could please announce in the other languages that we're working on a sound problem.

YESIM NAZLAR: Okay, it's back.

ALAN GREENBERG: And I have absolutely no recollection of where I was in the question. Olivier, did I finish answering your last question?

OLIVIER CREPIN-LEBLOND: Thank you, Alan, Olivier Crepin-Leblond speaking. The question was based around abuses by ccTLDs and how they're handled by ICANN, IANA, or the internet community.

ALAN GREENBERG: If they are things within their jurisdiction, then we handle them, although I'm not sure what tools either ICANN or IANA has, but there are in general very few abuses that break the internet or violate the rules that apply. Most things that would be perceived as abuses are indeed things a ccTLD has within its own jurisdiction.

OLIVIER CREPIN-LEBLOND: Okay, thanks Alan. Now, there is another question, I'm reading the questions at the moment and going through them. The next one is about the mix of Latin and non-Latin scripts in one domain name. That creates a lot of cyber security risks as we've seen, what are the possible solutions for this problem?

ALAN GREENBERG: Well, certainly mixtures between with different levels are perfectly valid. Mixtures within a second level, I'm not quite sure what the current status is, to be honest. Olivier, we had a private discussion the other day on whether those are in fact allowed right now or not, and I'm not 100% sure of the answer.

OLIVIER CREPIN-LEBLOND: Okay, thanks. Next is a question from Bakary Kouyate, and I know that Bakary is online, I don't know whether Bakary is able to speak.

ALAN GREENBERG: I can hear someone very quietly saying hello, but you have to continue.

YESIM NAZLAR: I think it's a loop from Bakary, we're trying to locate it, apologies for that.

OLIVIER CREPIN-LEBLOND: Okay, let's continue, then. There are some other questions that are in the list at the moment, so let's go to Amal Al-Saqqaf, and Amal Al-Saqqaf, asked, "Who is responsible for observing and making sure the registrants obligations are being followed?"

ALAN GREENBERG: The answer is if someone reports that a registrant's information, let's say, if it's in the public WHOIS and they report the information is invalid, then ICANN will contact the registrar and the registrar will be obliged to make sure it's fixed, or the domain may be de-authorized. So, it all depends on exactly what the problem is, but in general, if a registrant has an obligation under the contrast, then it's up to the registrar to get it fixed with the registrant, and it's up to ICANN to work with the registrar to make that happen.

OLIVIER CREPIN-LEBLOND: Okay, thanks for that alan. The next question was from Bakary, who wrote down the question, "Does it make sense to implement DNSSEC in the root zone without actually having a validation service?"

ALAN GREENBERG: Do you want to answer that? Or do you want me to?

OLIVIER CREPIN-LEBLOND: I would say that without one, I mean, it's always good to have DNSSEC in the root zone, I'm all for it, that's my personal feeling, that all zones should be DNSSEC signed. The problem is having enough organizations that are convinced to actually implement validation for it.

ALAN GREENBERG: I think the first part of the answer is someone has to start, and there is no point in having a validating query tool if nothing is signed. No one is going to put validation in if there is nothing signed. So, someone has to start, and we started by signing the root. Many TLDs are signed, all new TLDs are signed, and a fair number, but not a lot of individual domains are signed. So, that's the start. Now the question is do enough people care to put resolvers in that verify the DNSSEC signatures. So, you have to start by putting in the security, and then hopefully people will use it. So I don't think there is any other order in which to do it. Thank you.

OLIVIER CREPIN-LEBLOND: Thanks, Alan. The next one is from Amal Al-Saqqaf, and the question is, "Who is responsible for observing and making sure the registrant obligations are being followed?"

ALAN GREENBERG: I think we just answered that.

OLIVIER CREPIN-LEBLOND: Okay, and when you said ICANN is the managing, so that's from HKhatib2000, when you said ICANN is the managing ICANN.org, is it because they own it or in general they're managing second level domain names?

ALAN GREENBERG: Well, the word 'own' is not technically correct, because domain names are not owned. You acquire the rights to use a domain name as ICANN has, so ICANN has gone to a registrar and paid for ICANN.org, and at the that point they are now responsible for anything that comes under ICANN.org, just as I am personally responsible for anything that comes under alangreenberg.org, because I happen to be the registrant for that. So the fact that ICANN also oversees rules associated with GTLDs is unconnected with the two things. From the perspective of ICANN.org we are simply another registrant.

OLIVIER CREPIN-LEBLOND: Okay, thanks Alan, Olivier Crepin-Leblond speaking. We have Omar Shuran on the line, let's see if we can hear from Omar.

OMAR SHURAN: Yes, can you hear me?

OLIVIER CREPIN-LEBLOND: Yes, we can hear you, welcome.

OMAR SHURAN: Yes, I'm just pointing to the whole, as they say. Alan just said that the data is displayed, there was a case where I couldn't find data for a domain owner. Is it illegal to hide the data for the owner of the domain?

ALAN GREENBERG: Prior to GDPR being implemented, there was a requirement that whatever information you provided has to be displayed. Now, you're allowed to go deal with a proxy service which will their put their information instead of yours, but you were not allowed to put false information in or simply put no information in for a domain name. That would be in violation of the rules, and if someone had made a complaint it would have been resolved.

Now with GDPR, the rules have been changed, and under certain conditions, fairly wide conditions, registrars and registries are allowed to mask the information on who you are, and we are in the process of refining those rules, but that's not likely to change in general. So, certainly for individuals, for people that are subject to European GDPR, then that information will remain masked.

It remains to be seen whether that will be the case for companies or for those who are not resident within the EU, that's still being discussed right now. But that doesn't mean that the information you're providing is false, it just means it's not publicly available. There will be situations under which those who have appropriate authority can get information even if it's not public. That will not apply to you as an individual, though.

OLIVIER CREPIN-LEBLOND: Thanks for this, Alan. And I'm not seeing any other questions now. We might have reached the end of this webinar, I'm not quite sure. Are there any other questions anybody has regarding domain names? Are you all now demystified?

ALAN GREENBERG: We are 4 minutes over, and we're going to run out of interpretation in a few minutes, in any case. So, if there are no more questions, perhaps we should thank everyone for their participation and turn it back to Joanna.

OLIVIER CREPIN-LEBLOND: Thank you, Alan, and I was just going to repeat again, as we said, this webinar will be taken into account with regard to participation in the ICANN Learn program for ATLAS III and of course one doesn't stop the other. So, if you're interested in this, I would suggest you also have a look at the ICANN Learn course. It is in English, unfortunately, and this webinar was done for people who are not that confident in English, but

it's got further videos about DNSSEC, about various aspects of we have spoken today, and it will go a little bit deeper than what we've done today. I hope you've all enjoyed this, and thank you again to Alan for having helped out and put those excellent slides in. I hope now that we Joanna back on line, because she did write that she had dropped of.

JOANNA KULESZA: Yes.

OLIVIER CREPIN-LEBLOND: You're back. Over to you, Joanna.

JOANNA KULESZA: I'm back, thank you very much gentlemen for yet another wonderful presentation. Thank you to everyone who participated, I hope you have found this helpful and informative. I am certain the At-Large community stands by, should you have more questions feel free to reach out. The presenters themselves will be happy to support you with any additional information that might be needed. Having said that, this is the first in a series of five courses that will be held twice with due respect for various time zones.

I am sharing in the chat box now a link to the agenda of those training courses. Our wonderful staff will be sharing more information. Thank you very much for putting that into the chat box as well. Our wonderful staff will be sharing more information on the upcoming webinars and the next one will be on GNSO, it will be hosted on April 30th at 2100 UPC. It will be presented by Marika Konings and Steve Chan, or Caitlin

Tubergen, who we'll see how their availability will look at that point. We will keep you updated.

Those webinars will also be a part of the mandatory program for your participation in ATLAS III and as Olivier rightfully pointed out, they will also be provided with simultaneous translation, and as I already mentioned, all the webinars are recorded and you will be able to view them afterwards, should you find the need to come back to the information that was shared here today.

Thank you very much to the interpreters who agreed kindly to work overtime. Thank you very much to staff who have been wonderful and have been doing their best to provide us with the best IT service that is available. And last, but not least, thank you Alan and Olivier for yet another exciting presentation. Thank you very much everyone, enjoy your day, and I will see you or hear you during the next webinar.

ALAN GREENBERG: Thank you, Joanna. By the way, if we have to do this a third time, you are now fully trained to give the whole webinar.

JOANNA KULESZA: I will be happy to support you guys, that was wonderful, thank you so much. Bye everyone.

YESIM NAZLAR: Thank you all for joining today's webinar. This webinar is now ended. Please don't forget to disconnect all your lines. Have a lovely rest of the day. Bye bye.

[END OF TRANSCRIPTION]