CLAUDIA RUIZ: Good morning, good afternoon, good evening to everyone. Welcome to the eighth At-Large capacity building webinar, on Internet of Things, taking place on Monday the 7th of December 2020 at 19:00 UTC.

We will not be doing a roll call as this is a webinar, but attendance will be noted on the Wiki page. I would like to remind all participants on the phone bridge as well as computers to please keep your microphones muted when not speaking to prevent any background noise and to please state your name when taking the floor, not only for the transcription but also so the interpreters can identify you on the other language channels. Please speak slowly to allow for accurate interpretation. We have French and Spanish interpretation on today's webinar. Our Spanish interpreters are Lilian and David, and our French interpreters are Aurélie and Jacques.

Once again, I would like to thank you all for joining, and I will now hand the call over to you, Hadia.

HADIA ELMINIAWI: Thank you so much. We will try, through this webinar, to explore the impact of the Internet of Things on communities and end users and how this relates to the DNS. We shall also explore the interplay between the domain name system and the Internet of Things.

For that, I will be presenting a short presentation about the impact on end users, and then Sarah Kiden will be presenting about the impact of Internet of Things on communities, and Andrei will be talking to us

about the interplay between the domain name system and the Internet of Things.

So let's start. As I said, this is my presentation and I will be talking about the impact of the Internet of Things on end users. Next slide, please. I will start with a definition, and then I will briefly talk about the impact on users and the economy. I will also touch on the Internet of Things constraints, and then I shall briefly discuss the relation between the DNS, the Internet of Things and users. Next slide, please.

Thank you. So, many definitions of Internet of Things were presented by researchers. However, I chose the one that stems from the semantic origins of the expression. So the Internet of Things means a worldwide network of interconnected objects, uniquely addressable, based on standard communication protocols. The Internet of Things-allows people and things to be connected anytime, anyplace with anything and anyone, ideally using any path and any service.

So, what is the number of connected devices? A prediction made by Gary Davis of McAfee Inc., 50 billion devices. This should include all sensors, devices, computers existing in our world.

Another prediction says around 31 billion. This is by Security Today, and 35 billion are expected by 2021, a jump of 4 billion in one year. Martech Advisor says by 2030, this figure is expected to jump to 125 billion, where every customer of Internet of Things devices will own around 15 connected devices. Now, the future is connected, definitely, from what we see. Next slide, please.

So, what's the impact on users and economy? The potential economic impact of the Internet of Things in 2025 is estimated to be something between $3.9 trillion to $11.1 trillion. This potential impact was estimated by extrapolating from current and emerging users and estimate adoption and growth in the industry. .This was done by McKinsey.

So if we look for example at different settings, like devices attached to or inside the human body, home, [inaudible] where people live, retail environments, worksites, [custom] production environments, urban environments, those are all possible settings for the use of the Internet of Things and the growth in economy that is associated with that.

Users [could get enormous amounts] of data about themselves and their surrounding environments. However, security is always a concern, and they need to take care who they share this information with and how to get engaged with their environment. So there needs to be this kind of balance between the benefits and the privacy concerns. Next slide, please.

So this is a quiz. We haven't talked about this yet, but I thought maybe I would put the quiz before we talk about it. So, which of the following could be seen as an IoT constraint? Technology, interoperability, privacy and confidentiality, security, intellectual property, organization and talent, public policy, all of the above?

CLAUDIA RUIZ: Hadia, I'd just like to let everyone know that they are able to answer the question in the poll.

HADIA ELMINIAWI: Yeah. Please go ahead and answer the question, and then submit.

EDUARDO DIAZ: I cannot submit the poll.

HADIA ELMINIAWI: Yeah, “submit” is not working for me as well.

EDUARDO DIAZ: It works if you scroll down.

HADIA ELMINIAWI: Okay. Thank you.

CLAUDIA RUIZ: My apologies. It looks like the second one, [inaudible].

HADIA ELMINIAWI: For me, it’s not working. I have to answer the second one in order to submit both, right?

CLAUDIA RUIZ: It looks like it. I'll see if I can fix it.

HADIA ELMINIAWI: Yes, that's what we need to do. We need to answer both.

CLAUDIA RUIZ: Hadia, are you able to see the results? It looks like the majority are picking all of the above.

HADIA ELMINIAWI: Yes, 63% are saying all of the above. And certainly, all of the above is the correct answer. Next slide, please. So there was a research conducted by Consumer International and the Internet Society which gives insight into what consumers know and feel about the privacy and security aspects of the Internet of Things.

63%% finds connected devices creepy. 50% of the people know how to disable data collection. 75% distrust the way data is shared. So the research also shows that security and privacy concerns surpass cost as the primary barrier to purchasing IoT devices. So the research conducted definitely shows that privacy and confidentiality and security are all major constraints when it comes to the Internet of Things.

Technology is also a constraint for the widespread adoption of the Internet of Things, the cost of hardware, connectivity, data storage, [inaudible] boundaries, all of this needs to drop. I won't be touching much on the technical aspects, I will be mainly focusing on the social aspects.

Interoperability, this is definitely required for Internet of Things devices and systems to work together. It is estimated that 40% of the benefits of the Internet of Things are realized by devices and systems working

together. Privacy and confidentiality, and again, IoT cannot be widely accepted and deployed unless users accept it. People could see Internet of Things as a technology putting their security and privacy at risk, which ultimately translates in distrusting the Internet and preferring to be offline.

And trust comes from two things. One, you need to have control over your information, and second, to trust the security of the network over which your information is flowing. Intellectual property, this is also an issue or constraint. A common understanding of ownership is required, like rights to data produced by various connected devices. For example, if you have a medical device implanted in a patient, who has the right to the data? Is it the patient, is it the healthcare provider, is it the manufacturer of the device? So definitely, ownership here is an issue.

Also, organization and talent. People need to learn how to deal with all this flow of information, and organizations need to adopt data driven solutions and start relying on data in decision making and predictions. Also, public policy and regulation is a big issue. So regulations and policies in relation to data and privacy, when it comes for example to self-driving vehicles. So lots of regulations are required in order to enable the Internet of Things to evolve. Next slide, please.

So here I'll be touching on the DNS and the Internet of Things and users. Definitely, with the Internet of Things, more devices will be connected where we have seen estimates suggesting 50 billion connected devices and predictions to reach 125 billion devices by 2030. Predictions also say 70% of IoT devices are not securely deployed and vulnerable to different attacks. For that, the name service must be robust and secure

enough to support stable and trusted name resolution for the huge number of connected objects.

So to address the question, will the current DNS be able to support the name resolution of IoT objects, we need to think about the Internet of Things' name service requirements. Security is certainly one of the requirements. The trust opportunity research of Consumer International and the Internet Society shows that user security and privacy concerns surpass cost as the primary barrier to purchasing IoT devices.

So the DNS was originally designed with limited security and thus was vulnerable to attacks like denial of service, redirections, among others. The security of the DNS was enhanced with DNSSEC protocol, but DNSSEC may increase the size of the data packets and also involve additional [inaudible] to fetch the key information. All of this affects the query time, which is a limitation to a lot of IoT real-time applications.

So a security model other than DNSSEC is needed for IoT name service. Also, DNS still transmits DNS data without privacy protection. Yes, there are mechanisms under development to provide confidentiality between DNS users and the resolvers and between the resolvers and the authoritative servers, but we're not there yet. So the integrity of the DNS data as well as its confidentiality may not currently meet the IoT requirements.

Mobility is another concern, so limitations in relation to mobility is an issue. According to the DNS protocol, the update of the data does not need to be executed immediately, and this is especially when multiple

[tasks] need to be updated. For IoT, the name information must propagate as fast as possible, so again, this is a limitation.

Also, the time to live in caches for resolvers needs to be set to zero, which degrades the efficiency of the name resolution. So modifications to support efficient mobility management should be proposed.

The usage of IDNs will definitely help in supporting the Internet of Things where they can be used in localized Internet of Things applications.

So to summarize, the DNS was not designed for IoT applications which have stricter requirements in relation to security, efficiency, mobility. Therefore, definitely a smarter DNS will be required in order to accommodate the Internet of Things and to accommodate the Internet of the future. Next slide, please.

So that was the quiz. The second quiz question was the current DNS must become smarter to accommodate IoT applications. So yes, no, maybe, don't know. And here we have it again. So Avri is saying, "What does smarter mean?" Okay, so maybe smarter is a little vague expression, but actually, what that means, I've explained. It needs to face limitations in relation to mobility, for example, in relation to security. For example, to be more precise, if we are talking about DNSSEC as the security now existing in DNS, would that be sufficient for the Internet of Things? Well, the answer is no, because DNSSEC requires bigger packets. You won't be able to use UDP, you need to use TCP. Also, the tasks involved in fetching the key information, all of that will affect the latency of the DNS query, and thus it's not suitable for IoT.

And for IoT, we need to find different security solutions. Also, in relation to mobility, we need to have modifications to support efficient mobility management, modifications to the existing DNS. So by smarter, it's tackling the technical issues that exist now that won't be able to accommodate IoT. But I used the word "smarter" because I know many of the attendees are not actually technical people and I just wanted to get the concept through rather than the technical aspects of it.

Additional functionality, Avri is saying. No, it doesn't need artificial intelligence capabilities. It just means it needs more different technical solutions to the existing problems.

So I'll finish here, and I thank you a lot. I'm open to questions.

JABHERA MATOGORO: Yes. Thank you for a very good and [wonderful] presentation. Is it necessary to wait until we have Internet connectivity and then we start talking of Internet of Things, or we can even do Internet of Things without Internet connectivity? Thank you.

HADIA ELMINIAWI: Okay. Well, definitely, we can work on research and deployment, but how will Internet of Things work without connectivity? The basic idea is actually to have devices talking to each other, to have devices talking to people, to have ... So you need definitely to have connectivity, any kind of connectivity. But that doesn't mean that we cannot start deployment, research. By the way, it's estimated that deployment in developing countries will be more than the deployment in developed

economies. However, the economic impact of companies in developed companies is expected to be more. So yeah, I don't know if I answered your question, but yes, we need connectivity.

ANDREI KOLESNIKOV: I can add to this. You can use mobile networks or you can deploy the low power wide area networks, which is really cheap, and you can do it by yourself.

HADIA ELMINIAWI: Olivier, please go ahead.

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Hadia. A question on he number of devices that you mentioned. I'm looking at your slides, and you say by 2030, there would be 125 billion devices, and there's 35 billion IoT devices by 2021 installed around the world.

Now, when you mention 35 billion IoT devices installed, what you mean by installed is they'll be connected to the Internet around the world? That's question one. And question two is whether they all need to be using DNS or whether some of them would be just using other types of addressing? Thank you.

HADIA ELMINIAWI: Thank you for your questions. So yes, they don't need to all use the DNS for sure, and definitely, there are other schemes. Object resolution

rather than the DNS, because the DNS actually makes the resolution between mainly websites and IP addresses, but with the devices, it's different. So yes, we could have different types of resolution, and by connected, yes, I mean connected to the Internet.

But the estimates differ depending on who produced those estimates. But I think mainly part of the estimates is that some of them for example house all the chips or computers present in one device, so instead of counting it as one devices, if you have for example two computers, then you count it as two instead of one. So that could be one reason for the different estimates, is what exactly do you count?

OLIVIER CRÉPIN-LEBLOND: Thank you.

HADIA ELMINIAWI: Sarah, please go ahead.

SARAH KIDEN: Thank you, Hadia, and thank you, everyone, for inviting me to this webinar. My name is Sarah Kiden. I'm a technologist and design researcher currently on a project called OpenDoTT, Open Design of Trusted Things, which is a joint project between Northumbria University and Mozilla, exploring how to do a more open, secure and trustworthy Internet of Things. Next slide, please.

My presentation is also going to take a design and social science approach, so less technical talk and more on the end user or community

side of things. I'm sure Andrei's presentation will be more technical. So even if I have a technical background, I've always been very interested in the end user side of things.

My research sits at the intersection of the Internet of Things or objects and communities, because now we have increased [inaudible] do it yourself platforms that place IoT within possibility for grass roots communities or makers and activists at local scale.

For example, it's now a lot more affordable and easier to buy sensors, boards and other objects that you may need to deploy or build your IoT device for your home or your city. So we seek to use aspects of co-design to develop locally relevant IoT solutions, to support charities and community-based initiatives. We seek to harness the skills that communities already possess to customize and build technologies.

For example, in our communities, we already have people who do [things,] they prepare our radios, our TV sets, our bicycles, motorcycles, boats and so on. In Swahili, a language that's spoken in a lot of sub-Saharan African countries, there's a word for that, [inaudible]. Sometimes they are self-taught, they learn on the job, or many of them don't even have formal education. So we hope to harness these skills and repurpose them for building community technology solutions. And finally, we seek to compare and contrast IoT deployments in rural and urban, developing and developed country perspectives. As you are aware, these differ a lot. Next slide, please.

Before I say more about this slide, I just wanted to say that co-design is an umbrella term for design processes that are participatory, so they

are co-created, they are open. This means that instead of developing something for a particular group of users, you are actually developing it with this group. Not for, but with, hence aiming for IoT solutions that are relevant to a particular group's needs.

I would like to share this example. Being part of the At-Large community, we might learn interesting ways for us to engage with everyday users in topics such as DNS abuse, which sometimes feel very complex and yet they affect basic everyday users. And I don't intend to start a religious discussion at all, this is just an example of one of the most basic and interesting uses of IoT for everyday users that I have seen. This is not my project, but I'll be telling you about my project shortly.

This is prayer companion, which I highly recommend that you read this if you have some time. It's a device that was developed by design researcher William Gaver and others as a resource for the spiritual activity for a group of nuns in northern England. It basically displays a stream of information served from RSS feeds and social media sites to suggest possible prayer items for the nuns.

I don't know if many of you are aware, but nuns normally live in convents or homes specifically meant for them. Their way of life revolves around meditation and prayer, and many times, they have very minimal interaction with the outside world.

What I like about this project is that the IoT device which is that wooden object that you see in both images, it's the simplicity and ease of understanding. Already, these nuns because of how their activities are

planned, they don't spend a lot of time using technology or social media sites for news stories. In this example, you see that most of their news was on a notice board.

So I like this prayer companion because it just displays the prayer items on that wooden thing which was designed to almost mimic a cross because in the convents or in such places of prayer, you'll find a cross, so they tried to mimic that cross and make it integrate with the lives of these nuns. And the other nice thing is it doesn't change their way of life very much. They don't have to go looking for news stories or news feeds, they don't even have to interact so much with the IoT device. So it's very simple, it's interesting, and it's a very interesting way to introduce technology to basic users without them feeling overwhelmed. And as the At-Large community, such simplicity should interest us.

Next slide, please. Now on to my project. Just to note that this project is funded by the European Union. I have spent the past year volunteering and working with the Dundee West End Community Fridge in a bid to understand the workings of community-based initiatives. So the case study was selected as a model of community-based initiatives, and the main aim was to understand how Internet of Things can support charity organizations and other community-based initiatives.

For those of you who are new to the concept of community fridges, they're just like the fridge you have in your house, but instead, they are placed in public spaces and used by the community to reduce food waste. So donations come from supermarkets, food businesses and individuals who share the food instead of sending it to landfill.

We worked with this community, we interviewed some participants to understand their perspectives about using the service [inaudible] such organizations and how they think the IoT can support their work. And due to the COVID-19 pandemic, some of our activities were interrupted, so the true aspect of co-design where you work directly with participants was replaced with online activities, interviews, conversations and other activities. We also talked to other organizations like Hubbub in London which is a network of such community fridges. We talked to the People's Fridge in Brixton, also in London, UnshelteredTV in California. UnshelteredTV does a lot of community projects around behavior change and things like that. We talked to Kijiji Yeetu in Nairobi, Kenya, and they do a lot of projects around ... they're aiming to build smart villages, basically, and then Zuri Foundation in Limpopo, South Africa. We also talked to some people who fund this project, [inaudible] and other leaders in this organization. Next slide, please.

So some of the emerging themes from this work were things like sense of belonging. So we were talking to the community and asking them what does community mean to you, and participants expressed what it means in our individual and our collective life. So this first theme, sense of belonging is about belief, faith, openness, caring, sharing and helping one another, and understanding this social cultural concept helps designers and researchers to understand expectations that people have for their own behavior, for other people, and what happens when those expectations are violated, and it helps to bring clear value to [inaudible].

It's also important to note that it's not always [inaudible]. A lot of the participants are telling us that sometimes, [inaudible] when you're living

and working with other people. For the case of the Dundee West End community fridge, they were telling us this story about how when they decided to put that community fridge, the local businesses were not very happy. They thought that maybe their businesses are going to be taken away and things like that. But now they've grown to like the project and actually contribute to it.

Another theme was around community building, which explores the conscious effort needed in order for community projects or projects intended for everyday users to succeed. It's again worth noting that sometimes, technology is not the solution to every problem, especially if the foundation has not been laid. When we talked to our participants, I was wearing my technologist hat and I was telling them we could do this and that, we could build this and that solution to solve this and that problem. And some participants told us a few things. To quote one of them, they just said, "There are quite a few things that you need to address before we can move on to the tech bit." They [said that] it feels like a lot of the time, the tech stuff is nice to have but it's not essential. So, what does this tell us? That we need to understand community or end user needs and priorities in our endeavors.

Another theme was around social inclusion and exclusion and the unseen. Many times, we are quick to judge a community or an end user just by looking at them. For example, we just assume that people who live in affluent neighborhoods or people who come from a particular country are "well off," which may not be the case. We cannot determine community needs just by looking from the outside.

So other themes emerged around ecological stewardship, low and high tech, the impact of technology on our health, leadership, partnerships, funding and support, efficiency, privacy and security, among others. Next slide, please.

So, what are the next steps for this project? The process we followed was participatory. So we did a lot of things. There was observation involved. There was shadowing where we were following the people as they connect the donations from this community and bring them to the community fridge. We volunteered at the community fridge to actually have that direct experience of what it means to volunteer and work directly with the community.

We also did the interviews, and after that, we came up with a few sketches that we shared with the community for feedback. In normal times, these sketches would have been done b yes the communities or the participants themselves, but the pandemic did not permit that. And once they gave feedback, we just went through a process where we would draw sketches, share with them, give feedback and [would keep iterating with them,] and some concepts were developed. So we are going to explore this concept further and try to prototype them using open hardware, and Internet health considerations, which I'll talk about shortly, will be considered through [inaudible]. Next slide, please.

So as I mentioned earlier, Mozilla is an equal partner in this project, so we want to ensure that Internet health considerations are followed. As we develop these community solutions, we need to ask some questions before and during the framing, and not just as an addon once the projects are deployed. I think one of the challenges with IoT right now is

things like privacy and security are an addon, like the product was developed, it was deployed, and now we say, “Okay, we need to add security to this.” So we need to think about these things before or during the process. We need to ask in terms of privacy and security, is the technology solution safe? What are the privacy concerns? How open is it? Is it open in a way to allow diverse contribution from different stakeholders. In terms of digital inclusion, who is welcome? As you may know, even open spaces sometimes are not welcome. So, do we have to extend an invitation to have more voices on the table? Do users even have a voice once they come to the table?

In terms of web literacy, who can succeed? Do our users have the right skills to actually develop and deploy this solution? In terms of decentralization, who holds the power, who controls this whole process, who is the ultimate decision maker? And this is one part that I feel that as design researchers, we can learn from the growth of the Internet and from bodies like ICANN and the IETF.

I actually wrote a blog post about lessons that design researchers can learn from the growth of the Internet and from Internet policy. So for more information, you can take a look at the Mozilla Internet health report, and the one other resource that I didn't put on the slide but I will edit it, and then I think the final slides that will be uploaded will have another link for a report called privacy [inaudible] included, by Mozilla as well. It rates your IoT devices from creepy to less creepy or not creepy, so you can actually go to this website and see how different IoT products on the market have been rated. I think many of you will find this very useful. Next slide, please.

So I feel like this is Andrei's section, but as I noted, I'm giving design and social science context, but just briefly to highlight, as Hadia already mentioned during her presentation, there are billions of new devices on the Internet, and because of this do-it-yourself and many people now doing this on their own, the number is going to become bigger. So for example, these communities that I'm working with are potential new IoT devices on the Internet. And also, I feel like we are [inaudible] in terms of Internet access and things like that, and I've seen a few questions in the chat about that, but the growth of community networks and lower costs of connectivity means that more devices are now connected and more will continue to connect in the coming years.

Perhaps the thing I need to emphasize is that new entrants or end users are not security experts. And we should not require new entrants to be security experts. They don't even know [inaudible]. They're not concerned about DNSSEC, DNS over HTTPS, DNS over TLS, or whatever fancy [inaudible] something that we'll come up with. What end users need, and what we as At-Large need to advocate for, is an easy way to include security, to update, to deploy.

We should know that if it requires an extra effort on the part of the end user, they will just ignore it or ditch it altogether, and that means we have created a wonderful thing, beautiful framework on paper that [stays] something beautiful, but in someone's lab somewhere or someone's computer.

And the final question would be, how do we ensure that nontechnical people, as they build their own technology, like the communities I worked with and really basic users, and we'll see the growth of

community networks, community [radios,] how can they make proper use of IoT devices, embedded with security and other services that we offer? Next slide, please.

And I've probably already hinted at this earlier, but to emphasize that one size does not fit all. this illustration is an artist's impression about our project as we connect people and we give people access to technology, to IoT, to Internet, we have people from all walks of life, so we have basic, intermediate and advance users, people with office jobs or they do manual work, they till their land to earn a living, people who drive to work or use public transport, they live in urban or rural areas, people who speak English or English is their first language, some people don't even have English as a language option at all.

So the challenge to Andrei and to the tech and to us as the At-Large community is to think about these issues. Next slide, please. I just want to end with this quote that I found in one of my readings. I'll just read it out for [inaudible]. "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." So this quote is from 1991, but it's very much applicable today. Next slide, please.

So this is really an invitation. As this is very much work in progress, I welcome any feedback, comments, recommendations, questions and collaboration to continue supporting IoT at community level, and most importantly, communities of the most basic users whom the At-Large Advisory Committee seeks to represent or work with. I know that represent maybe right now is not the right word to say.

And I've created a GitHub page for the project, to collect examples and share resources for Internet of Things at community level. Thank you very much. I'm happy to take any questions. I believe there is one pop quiz [inaudible]. So that's the question. Co-design is an umbrella term [of which processes?] Participatory, co-creation, open design, all of the above?

So I see 71% have selected "all of the above," and that's basically what it is. Co-design basically means you're working with the community and not for them. You're co-creating, your process is open, the design process is open, and all those things. So, thank you very much for listening to me and thank you for inviting me to this webinar.

HADIA ELMINIAWI: Thank you so much, Sarah. Are there any questions to Sarah before we move to Andrei? Sarah, this was really good, great work, great initiatives, and I assume great impact as well. And as Herb says in the chat, quite inspiring as well.

JABHERA MATOGORO: I wanted to ask Sarah a question. I posted it on the chat. Sarah mentioned about community network as an alternative solution to connect the unconnected, but most developing countries, especially in Africa, do not have policies and the regulation [favoring] community networks. I was just asking Sarah, do you think IoT could be another angle to push for policy and regulation for connectivity in Africa? Thank you.

SARAH KIDEN: Thank you, Matogoro. You are very right that in Africa, we don't even have the right policy to support community networks, but I think that is changing. If I can give you an example from Uganda, I think around 2018, there was a call by the regulator developing new regulation for connectivity, for Internet service providers and things like that. And as a group of people, we didn't even think it was going to [come up with anything,] but we basically just wrote and gave feedback and used the example of one of the community networks in Uganda, BOSCO Uganda, and said that this community network is connecting this number of people and they don't have a license to operate as an operator.

And to our surprise, towards the end of last year, basically when they published the new guidelines, there was one community network regulation. So basically, right now you can operate as a community network in Uganda. So what I'm saying is that we are not yet there, but we are making progress and now we can continue to push and give these examples of things to advocate for better policy. Thank you.

ANDREI KOLESNIKOV: Hello everybody. My name is Andrei Kolesnikov. I'm from Russia, and my day job is to run the Internet of Things Association here in Russia. Also, I'm a member of SSAC, Security and Stability Advisory Committee. Next slide, please.

I should say a few words about SSAC. It has 39 members all appointed by the ICANN Board, and the role of the SSAC is to advise the ICANN

community and board on matters relating to the security and integrity of the Internet naming and address allocation system.

Our group published 113 publications since 2002. It is an expert group, and its expertise is addressing and routing, domain name system, of course, DNSSEC, domain name registry/registrars operations, DNS abuse and cybercrime, internationalization of domain names and data, and Internet service/access provider, and also ICANN policy and operations. Next slide, please.

So, how does it work? ICANN's mission and commitments are here on the slide. To ensure stable and secure operations of the DNS, and preserving and enhancing the operational stability. So SSAC does its job by issuing advice documents, send it to the board, board acknowledges, studies the advice and takes actions, [inaudible] take it or drop it. In order to publish advice, SSAC usually forms work parties. Next slide, please.

This novella is based on SAC 105, which is a document released last year. It's called DNS and the Internet of Things, opportunities, risks and challenges, and also, this paper was adopted by IEEE as a manuscript. Here you can see the list of authors. I should [inaudible] Cristian Hasselman who's the chair of the work party. He did a great job. [inaudible]. Next slide, please.

So it was an interesting document because it's a different kind of SAC report. It has no written recommendations to the ICANN Board, but it's a tutorial-style discussion intended to trigger and facilitate dialog among the broader ICANN community. Now we have the broader ICANN

community right here, right now, so I've decided to ... with this presentation, I'll also ask a couple of questions which I saw on the chat recently, so let's move to the next slide, please..

As already mentioned, I will do this fast scroll through the slides because there are a couple of definitions of the Internet of Things, but it has the same meanings. I like Wikipedia much better than the ISOC one from 2015. It's a network of physical objects that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices.

It's interesting that the term "Internet of things" was born in the late '90s by a guy who was selling RFID cards, radio frequency identification. So it started with a simple thing and grew up into a huge world.

So differences with traditional applications. IoT continually senses, interprets and acts upon the physical world. It means that IoT connects the physical world with the digital world and it's the main function of the IoT.

We can argue about the numbers, but let's go to the next slide and see the recent numbers from Omdia. These numbers were presented at the IoT world conference, which was virtual for the reason we all know.

So let me put it like this. There are a lot of IoT devices. You can see on the screen, it's M2M market, which is devices which utilize the mobile networks to connect the devices to the network. So it's a connected device.

But there are billions more not connected to public networks. I should say that when we talk about the IoT, we talk about a huge and broad spectrum of devices, because this huge number, these billions on the slide, only shows you M2M, but there's also a world of [inaudible] IoT which has wires and private networks which will never be connected to the public networks, and probably even bigger than M2M world. But still, it's IoT devices.

Also, as you can see on the slide, China completely dominates. It's complete world domination with M2M devices. So three largest mobile providers for IoT devices are China Mobile, China Unicom and China Telecom. [Phenomenal results.] Next slide, please.

Again, the trends are important. The growth is important too, because it gives you the idea on how this ecosystem [inaudible], how it should evolve. And it will evolve to a lot of devices, basically. 20 billion devices just in the M2M sector. Next slide, please.

I should say a couple of basic things before we go in depth into the DNS and other stuff. This is a simple view of the IoT architecture. On the bottom, you see things, then you have a communication layer, then you have a computing core with algorithms, which is called IoT platform, and on top of it, you have data and applications which basically run out of past, out of present and out of future, because AI is a huge part. You can collet a lot of data, learn the patterns and predict how things will work if some circumstances will change. Also, the vertical layer is security which goes from the bottom to the top. Next slide, please.

This is a colorful diagram. I drew it myself. So basically, what are the things? Sensors, actuators, machines, meters, triggers, door locks, [inaudible], cars, etc.

Then you have a network level. You have to connect your device with a network. This is an important part. Maybe I'll have time to talk about it at the end answering the question on how to [first start] IoT projects in certain areas of the world where you don't have infrastructure ready for that. Believe me, it's easy and it's doable.

So bascialyl, you have a network level, and it's tons of protocols which connect to the different devices for different purposes to the IoT platform. It does three functions. It manages the things, the IoT devices. It collects the data, and it runs the data analysis and management. And it also sends the signals to the devices back to execute some certain job.

On the top of it, you have the applications, which can be related to the smart village, transport, security, industrial, health, you name it. All modern industries in the world somehow use IoT technologies. And if you look at the arrow which goes down, up, it's value. It's how people and corporations make money.

So the Facebooks and Googles and Amazons harvest the value because they run the applications. There are some guys on the bottom who manufacture the things. That has a little value, but if you consider the size of the market, the number of deployed overall, it's also very valuable business. Next slide, please.

So this diagram is from the SAC 105 document. What you have on this diagram is people at home or in the city, you have a combination of

devices, devices with IP stack, devices which are connected, support the IP stack [inaudible] connectivity, and devices without the IP stack which is the majority of devices in the telemetry networks, because there is no reason to connect them to the Internet.

But they're all connected to the gateway, and the gateway talks to the service provider, of course. And usually, what it does is calls up the DNS to resolve the service provider and at the end of the day, in your network, for example, you have a smart bulb or you have a smart switch in your house, they do not talk to the DNS. But they do talk to your home switch, and your home switch talks to the DNS.

And of course, there are always bad actors. [They're always red lighted,] [inaudible] the picture, but they try to do some tricks to basically get access to your devices, to your house, to your city, to your village, and to do their bad business. Basically, the DNS [is used,] but not by the devices most of the time but the gateways which control your devices. Next slide, please.

IoT and the DNS. This is a core slide, actually. Remote services, cloud services, platforms, they assist devices in performing various tasks, for example, combining and analyzing data from multiple sensors. Also, devices calling DNS to perform their firmware updates and locate remote services. For example, if you have [two smart hubs] in your home, the smart device usually updates its firmware and they call the GNSO to retrieve the address of the update.

Also, IoT applications use DNS to locate service platforms. If you have an IoT application on your smartphone or computer, it uses DNS. So bascialyl, we have opportunities, risks and challenges.

Let's start with challenges. DNS and IoT industries can seize opportunities and address risk. If you scroll the Internet or you google it, you can see a lot of publications about DNS and IoT security. [inaudible] previous presentation asked the question, should DNS be smarter? I would say no. The IoT devices should be smarter and utilize DNS in appropriate ways, because there is a risk, because IoT stresses the DNS, accidentally. For example, large number of devices coming online simultaneously after a power outage, or on purpose because there is a DDoS attack. I will talk about this a little bit later.

Also, opportunities. DNS helps fulfill IoT's more stringent security, stability and transparency, because DNS is a utility for the IoT. DNS is a part of infrastructure services served by IoT. Next slide, please.

So, what does it mean for the end user? I'll just mention of course the botnet superstar, which is Mirai, responsible for DDoS attacks involving 600,000 devices, and Hajime botnet in sleeping mode because [it was never was in execution,] but 400,000 infected IoT devices.

And important is that these zombie devices utilize direct connection to the Internet. They use direct IP stack. So it's one of the vulnerabilities of the devices with a direct IP stack, connection to the Internet.

Also, there might be unintentional DDoS attacks, for example, software updates for a popular IP-enabled IoT device that causes the device to use the random lookup to check for network availability. And I say hello

to the Chronium, which [checks] the performance of the Internet by addressing the random lookup, which is a huge load on DNS infrastructure, ongoing currently, right now.

However, the most dangerous object—this is my personal opinion—for an end user is this. No brand remote control power switch sending data. Sending data is okay, but executing your commands through some unknown cloud service. This is a real dangerous thing. Next slide, please.

And I can say a couple of simple recommendations. Evaluate the convenience of IoT adoption at your home. This is probably not for Africa, but for the European, American and other communities. Do you really need cloud-based kettle to boil water? This might be a fun thing to do, but in two weeks, you'll forget about it. A lot of people buy smart things and just throw them away because it’s fun and it’s cool, but you really don’t need it.

Also, a separate recommendation from me, from Andrei, is be accurate in selecting an IoT service provider. Do not rely critical home appliances on some unknown stuff. You can buy some cheap thing with a cloud service that’s bundled to this device, but just make sure that this cloud is safe and you know who [it’s sending data.]

Also, be suspicious with open IP stack devices. Do not connect your video camera directly to the Internet. Connect it to the home recorder, and access through the recorder, do not access through the IP cameras, because might be a sort of DDoS attack [inaudible].

Also, very important thing to say, and this is from my practical experience. Your M2M device, [inaudible] security most likely is

appropriately managed, because mobile providers have some budget and they do manage their security. However, if you experience paranoia, remember, all your data is collected, used, processed and sold. Next slide, please.

And this is thank you. If I have time, I can answer some of the questions which I saw previously. Is this okay?

HADIA ELMINIAWI: Thank you so much, Andrei. Yes, please go ahead. And if we have more hands up, you'll be answering those as well. Go ahead, please.

ANDREI KOLESNIKOV: Okay. So a couple of questions on how to start an IoT project. First, go and check your telecommunication regulator to see if you have what we call the [ISM] band frequency. This is a free to use radio frequency which you can use through your wide area network devices. One of the protocols, take a look at the LoRa protocol, check the [inaudible] because there are a lot of devices available. So basically, [inaudible], what you can do in your village, you can connect for example all your power sources, all your grids with the smart meters, collect the data to the local cloud to build a local dispatcher, dispatch cloud service. It’s a very easy [chip,] it runs on two computers, it manages all your devices, it runs on a free frequency. But make sure those devices are appropriately set up to use your country permissible frequency [inaudible] lot of examples [inaudible].

So I spent about a year, we just finished in October, big work in IoT in agriculture. So if you're interested in this, you can contact me through the At-Large staff. I pasted my e-mail address to the chat so you can send [inaudible] e-mail. [inaudible] answer all the questions, because agriculture is so important everywhere, and IoT in agriculture is one of the fast track projects which basically pays off your expenses within one season. This is the only industry where your IT implementations can pay off the budget quick and effective way. Very cool. Believe me.

Also, another question. DIY. DIY works. Again, you can google a lot of examples on Internet and install it for yourself. Also, some of my recommendations would be if you manage something with IoT, make sure that if it's a critical application, for example if you can control your power grid or some of your critical infrastructure like water supplies or gas or whatever, make sure it's appropriately installed, managed and secure. It's very important. Or better have a human execute the commands. Do not trust the IoT cloud to execute critical functions.

Also, I should say a couple of words about [inaudible]. This is very important. If you look at the economy of IoT, [you can see the] growth of the cloud services and the drop of capital expenditures, because a lot of companies [inaudible] their capital investment projects like building infrastructure, and more and more companies rely on cloud services because you pay for the service, you do not pay for the infrastructure. It's one visible trend you can see right now. So go and read SAC 105. It's really easy reading.

Most important to say about the packet size, it's a [inaudible] device which runs on battery. The packet size of the [valuable] data is very

small. It’s like 100 bits. Not bytes, bits. Half of it is basically the [negotiation] data and [inaudible] and the valuable information within this packet might be two or three bits. So this is one of the interesting phenomena of the IoT for the [autonomous] devices. And there's a lot of them all around.

That’s basically it. Thank you.

HADIA ELMINIAWI: Thank you so much, Andrei. That was a very interesting presentation, and thank you for all the advice. Here's your quiz question. Would you like to read it?

ANDREI KOLESNIKOV: Yeah. Which of the following is IoT? I will answer with you because I'm not sure that ...

CLAUDIA RUIZ: I’d just like to let everybody know that you are able to select more than one option.

JUDITH HELLERSTEIN: It disappeared before people were finished.

ANDREI KOLESNIKOV: No, mobile phone is not IoT device. [inaudible].

JUDITH HELLERSTEIN: I had it disappear before I hit submit. So next time, can you wait a few more seconds or let us know? But I did have my three top choices as being the top ones, so I'm an additional one on smart TV, Tesla, and smart door lock.

ANDREI KOLESNIKOV: Yeah, you're right.

JUDITH HELLERSTEIN: Sorry.

ANDREI KOLESNIKOV: It’s okay. It’s fun. Which device uses DNS? If you hear my presentation, you probably can answer this one. That’s two out of four. Claudia, I have a question. If I press “close quiz,” I'm not closing it for everybody, right? I close it for myself?

CLAUDIA RUIZ: Just for yourself, Andrei. Correct.

ANDREI KOLESNIKOV: Okay.

CLAUDIA RUIZ: Okay, I see about 50 people have answered. 50% of the attendees have answered. I'm going to stop it now.

ANDREI KOLESNIKOV: Let's see the results. Yeah, smart bulb and smart door lock do not use DNS. They address their system to the local hub. But Siri assistant and Amazon Echo hub uses DNS. If your smart bulb using DNS, you're in danger because it means that your smart bulb has open IP stack which can be used for DDoS attacks. This is fun.

CLAUDIA RUIZ: And here is the final one. Andrei, we're not able, the way Zoom is set up, to have anyone put them in order. So if they would like to note—

ANDREI KOLESNIKOV: Well, pick one.

CLAUDIA RUIZ: Okay, we can do that. Okay, again, about half the attendees have answered. I'm now closing the poll.

ANDREI KOLESNIKOV: [C?] Exactly. 41% said IP camera. It's a source of the Mirai botnet. Also, smart hubs are kind of a danger. That's absolutely right.

JUDITH HELLERSTEIN: I thought you would have put a printer as well.

ANDREI KOLESNIKOV: I forgot how printer looks like in this COVID isolation. Who needs paper? I can do my documents electronically.

JUDITH HELLERSTEIN: [Printer is very successful for people who have] home printers because they can get hacked so easily.

ANDREI KOLESNIKOV: I don't know about printers. So, thank you very much.

HADIA ELMINIAWI: Andrei, I have a question for you. the applications that you put, yes, most probably, for example when you say, would this use the DNS or not, most probably yes, it would go exactly as you said, but that's not necessarily. And in the future also, we don't know how those things will be used and if they would require a kind of name resolution. Not necessarily DNS. So I don't know, what's your thought on that?

ANDREI KOLESNIKOV: Thank you for the question. [inaudible] first. First of all, when we talk about the applications, people think about humans touching the smartphones or running the application out of their computer, or have some smart hub in their home or smart tv where they control their house.

Most likely—and I believe I'm right—the applications will be other informational systems. Within three or four years, not only IoT devices

will be connected to the network, but the information systems by themselves will be connected. So they will talk to each other without human participation to make our lives easier. For example, the traffic lights are already talking to the cars, cars are talking to the gas stations, gas stations are talking to the banks because they can automatically charge you. The marketing companies get the data from the [car spare part] warehouse, etc. There will be less and less human participation if we talk about the automated world.

So when we talk about the applications which call on the DNS, yes, they will keep doing it, information systems talking to other information systems will still most likely use the DNS.

HADIA ELMINIAWI: Thank you, Andrei. So, do we have any other questions? Seeing none, Andrei, I would like also to ask you another thing. So what I understood that you say that the DNS as is does not need any kind of adaptation to meet the IoT requirements. And let's forget the word "smarter" because smarter sometimes implies artificial intelligence. But I think still that the DNS would need some kind of technical adaptations in order to move towards being object oriented, because we are moving towards object connectivity rather than people connectivity. So, what do you think?

ANDREI KOLESNIKOV: Well, [the good DNS is still good] for the IoT, but yes, [they'll] need some adaptation. For example, the concentration of the DNS traffic follows the concentration of IoT devices. As I said in the presentation and in SAC 105, for example, the firmware update of certain devices, or

if the whole things go offline and then come back online, which might cause a huge burst in DNS traffic.

But this [inaudible]. This is a provision of the DNS which must follow the traffic like it does today. The DNS today is a huge system adapted to the traffic levels. Basically, IoT just adds some kind of traffic level to the DNS and DNS should follow the IoT traffic level.

In regards to the object resolution system, it's another technology that has nothing to do with the DNS. There are a couple of things now being used in, I call it the upper IoT world. There are huge cross-industry initiatives talking about the new standards where informational models can talk and understand each other, how do you mange this informational model, how do you manage data schemas of the digital object? How do you identify these schemas? How do you run the unique identifiers [of these] schemas? But it has nothing to do with the DNS, because it's upper level, it's the level of the information exchange and artificial intelligence and predictable models, and data exchange between the data [platform,] manufacturing or industrial informational platforms. So this goes on a different level of the communications, it's not on DNS.

HADIA ELMINIAWI: Okay. But if you have an IoT device using the DNS, let's say a real-time IoT application using the DNS, do you think that the current DNS could actually meet its requirements? And taking into consideration for example that you need some kind of security, so, if you apply DNSSEC, would that meet the requirements? You need to take into account of

course the latency that would be [inaudible], and also that you might be using for example TCP instead of UDP. Will the current DNS meet those requirements?

ANDREI KOLESNIKOV: It's a direct answer. Yes.

HADIA ELMINIAWI: Okay. Maybe.

ANDREI KOLESNIKOV: Yes. [It will.]

HADIA ELMINIAWI: Also, when you talk about the mobility as well, that could be an issue also when you're talking about real-time IoT applications.

ANDREI KOLESNIKOV: Okay. Real-time IoT applications run on a different level. [inaudible] protocols which connect the [cars] with the infrastructure and [inaudible] completely different technology. It runs on 5G, for example. And 5G itself is a protocol with low latency, low delays, high bandwidth, and it's not utilizing the DNS as we as users call it. It uses a little bit different [embedded] addressing system in order to send packets back and forth in a quick way, 3-5 milliseconds, because if you have a moving object, moving car, everything must be really fast. And it's not DNS.

HADIA ELMINIAWI: Thank you, for sure, Andrei. So, we have no more hands up. Thank you all for attending today's webinar. Thank you for your interest and for your engagement and for your questions. Thank you a lot, Sarah, for this inspiring presentation and thank you, Andrei, for your technical expertise. And thank you to our staff and thank you to our interpreters. I think we have a survey still, correct?

CLAUDIA RUIZ: Sorry, Hadia, I'm having trouble with that survey. I can send it out to people after this.

HADIA ELMINIAWI: Okay. So we don't have a survey with us today. I thank you all again, and see you in our next webinar. Bye.

[END OF TRANSCRIPTION]