ICANN68 | Virtual Policy Forum – At-Large Policy Session: DNS Abuse: COVID-19 and End-user Issues
Monday, June 22, 2020 – 10:00 to 11:30 MYT

CLAUDIA RUIZ: Hello, Joanna. Are you ready to begin? We are currently only missing Marita, who will also be presenting.

JOANNA KULESZA: Yes, Claudia. I think we're good to start. We have our two first presenters and I will be doing an intro. I'm going to act under the assumption Marita will join us during the course of this call. So, I'm glad to start for us not to start off behind schedule. Thank you.

CLAUDIA RUIZ: Okay. Thank you very much. One moment. This session will now begin. Please start the recording. Good morning, good afternoon, and good evening to all. Welcome to our At-Large session of the ICANN 68 Virtual Policy Forum on Monday the 22nd of June at 02:00 UTC, on DNS Abuse: COVID-19 and End-user Issues.

My name is Claudia Ruiz and I am the remote participation manager for this session. Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior. We will not be doing a roll call during ICANN 68 but we'll note attendance for the following sessions.

During this session, questions or comments submitted in chat will only be read aloud if submitting in English, using the proper form as I've

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

noted in the chat. I will read the questions and comments aloud during the time set by the chair or moderator of this session.

If you would like to ask your questions or make your comments verbally, please raise your hand. When called upon, staff will unmute your microphones and you can take the floor. Please state your name for the record and the language you will speak, if speaking a language other than English.

Please note, this session includes interpretation in French and Spanish. To hear the interpretation, you will need to download the interpretation application. More information can be found in the session details on the events schedule. And instructions are in the chat.

We have also posted all the details on the At-Large ICANN 68 wiki page. The link is posted in the chat as well. And a kind reminder to please speak clearly and at a reasonable speed to allow for accurate interpretation and again to state your name each time you take the floor. Thank you very much. And with this, I hand the floor over to you, Joanna Kulesza. Thank you very much.

JOANNA KULESZA: Thank you very much, Claudia. Thank you, everyone, for joining us at this very first At-Large policy session, which we like to look at as an opportunity, also, for capacity building, as you can see here on the slide.

Now, we're trying to develop an angle to this discussion we've been having around DNS abuse in times of pandemic. I am thrilled to be joined today by our speakers. If we could move on to the next slide, that will have a very brief introduction. You can see that also in the session description.

We are joined also, as you will see in the session description, by my good friend and colleague, Alexandros Kargopoulos, who's working from the Fundamental Rights Agency and has kindly accepted our invitation, as we would like to look at legislative efforts around the pandemic that might have impacted end-user issues. Because the pandemic has caused us all to be working from homes, ICTs have become an important part of everyday lives. With that, we would like to look at specific efforts that have been taken on by governments, through legislation, that might impact end-user issues.

On behalf of the community, Yrjo Lansipuro and Marita Moll have kindly agreed to accept my invitation to speak and try to look an DNS abuse from this very specific angle. So, I welcome Yrjo Lansipuro, who's our At-Large GAC liaison, who has kindly agreed to report on the stance that governments have taken towards this pandemic.

We will also hear from Marita Moll, who has kindly accepted the challenging task to try and look at how the multistakeholder model might have shifted because of the pandemic, when we are granting forevermore trust and power to legislation that is targeting this specific challenge.

And as already said, I'm thrilled to welcome, also, Alexandros Kargopoulos of the Fundamental Rights Agency, who will provide with an insight on the activities that were taken by European states when targeting the pandemic.

If I could have the next slide, that would provide is us with a scoping question. Thank you. What we are trying to pursue during these 90 minutes is a freeze frame of legislative processes and the events around them that might have impacted the shifting multistakeholder model. So, the reason why we are here, regardless of where you are in the world, is to try and make the multistakeholder model better—to make sure that end-user interests as well, as business interests and governmental powers, are equally represented. Trying to achieve that aim in this unique time will be our specific task.

If we could move on to the next slide, please, we will look at those specific questions we are trying to answer. So, we will look at the efforts that have been taken by governments to try and ensure that everyone, in this challenging time of the pandemic, can enjoy the new normal to the best extent that is possible.

We want to explore whether this unique time leaves space for multistakeholder decision making as we have known it before. Has the enhanced governmental control impacted the way we develop policies? Has this happened now or is this something that should be expected? And how effective will we be in developing these policies focused on DNS abuse?

But as you will see, on the next few slides, we might want to explore that notion—to include specific end-user interests—also those focused around specific fundamental rights, as Alex will explain during our meeting—during our webinar today. And as you can see, we will try to forecast whether this pandemic impacts the way we develop policies in the future.

If I could have the next slide, it has the agenda. You will see this, also, on our wiki space. I will start us off with a very brief introduction. I just have a few slides to give you context. Then, I will be happy to give the floor to Yrjo, who will provide us with a reflection on how best to frame—how best to summarize the efforts that have been taken around the world that might have impacted end-user interests. We will try to identify what those end-user interests are.

Then, I'm glad we are joined by Alexandros, who will provide us with specific examples of how governments have tackled this challenge. And then, we will look to Marita to give us a summary, or a forecast, of what lies ahead.

We have reserved roughly half an hour for questions and summaries. So, your questions … Claudia was kind enough to explain how we usually work with questions to those newcomers that I am certain we have in the group. Please try to follow that specific way of posting your questions in the chat. We will try to accommodate, also, from live questions from the floor. Raise your hand and we will be happy to unmute your mic.

And because this ICANN meeting is virtual, we're also trying something new, which is a Twitter feed that uses the hashtag "ask At-Large." So, should there be any issues or questions that we will not be able to address during this session, feel free to use Twitter as a platform for us to discuss the issues presented here today.

If we could move to the next slide, I would just like to give you a bit of a context because when I proposed this session, I heard some of our members say, "Well, this is not really something that ICANN is about." So, just for us to build capacity and better understand what might be the challenges we're dealing with, I wanted to show you a few headlines—a few points of reference.

The pandemic, as already said, has enhanced the use of ICTs. Some have claimed that states who have successfully targeted that challenge—who've combatted the pandemic relatively effectively—resorted to innovative ICT measures.

You can see here a headline from the Brussels Times that focuses on the way that South Korea tackled the pandemic. And coincidentally, this specific meeting is targeting predominately the Asia Pacific region. So, what better location for us to look at those regional methods of solving the challenge—of addressing the challenge.

If we could move on to the next slide, this way of tackling the challenge has caused some concern. And this is why we look at fundamental end-user rights—individual rights that might be impacted by the way ICTs are used during the pandemic.

As a case of an example, you can see here the joint statement from ISOC and Norway. And since we have good representation of our ISOC community here, I'm using this as a point of reference. The way that the apps have been developed might impact fundamental rights. Is there a link with the work we do here? Is there a connection between the way that information about those potentially infected is being collected with the policies that ICANN develops?

If I could have the next slide, which is the last of those in my introduction. ICANN has been tracing legislative efforts around the world. We've looked at GDPR very closely. We are concerned with personal information that might be enabled to individuals or companies who should not be entitled to that information because of this innovative European legislation. So, is there any movement—is there any legislative trend—we should be aware of when it comes to end-user interests?

If I was trying to be provocative—and those of you who know me know very well I'm never provocative—I might ask whether privacy concerns, and websites or providers that use apps that might infringe upon individual rights, should be considered a form of DNS abuse. If a certain website provides content, provides applications, provides tools that might infringe upon individual rights, should we consider them DNS abuse?

We do that when it comes to online fraud. We do that when it comes, for example, to COVID medications. If you advertise illegitimate COVID medications or treatments online, you will likely be considered as

DNS-abusive. If you offer an app that infringes upon individual rights, is it also a case-in-point?

So, those would be provocative questions I would put on the table before I turn the floor to Yrjo to give us a recap of what has been happening around the world, with states trying to counter the pandemic. And then, I would like to hear from Alexandros, giving us examples of what ICT measures have been used when trying to counter the pandemic. And then, we will move on to a brief presentation by Marita, giving us a prognosis of whether those legislative trends might impact the way we do policies here within ICANN. Has increased governmental control impacted the multistakeholder model?

With that introduction, I'm going to give the floor to Yrjo for a recap of legislative trends or events happening around the world that might impact end-user issues. Thank you, Yrjo. The floor is yours.

YRJO LANSIPURO: Thank you, Joanna. Thank you for inviting me. Good afternoon, good evening, good morning from Finland. My name is Yrjo Lansipuro. It's 5:00 AM local time but the sun is already up. This is mid-summer in Finland. It's a big thing here. And I am happy to say that we got rid of most corona infections just in time for the celebrations.

Now, different countries have different corona experiences but they all share something important. Everywhere, the internet has played a huge role. It helped us to survive. It helped us to hang on, on the bits of

pieces of normal life. Now, this meeting—this ICANN meeting—this is a big theme of the meeting, the coronavirus epidemic, pandemic and the internet. But we'll try to look at it from the end users' point of view.

What is an end user? It's not a separate, distinct group of people, somehow separate from other stakeholders. End user is a role that people play when they go online. And during this pandemic, people have been even more internet end users than in normal times.

And I think that most people have realized that they are internet end-users because confined in their homes without access to their usual places or normal life, work, social gathering, and so on and so forth, the internet has been their vehicle to carry on normal life and their window on the world. You could work remotely. Your kids could have education. You could chat with your friends. So, at least in places with decent internet access, you could carry on almost a normal life. In my homemade Latin, connecto ergo sum. I connect, thus I am.

But even more remarkable, at least my experience has been that societies kept functioning. More precisely, in spite of the unprecedented clamp down of liberties in the physical world, democratic societies continue to function democratically. Even with freedom of assembly abrogated, traffic frozen, and curfews imposed, the society did not degenerate into a collection of atomistic individuals, isolated and alone in their homes, at the receiving end of communications from above.

So, somehow democratic societies remained active. Pluralistic political bodies, interest groups, civil society entities went on, using

the internet. And of course, there were a lot of telecommunication, teleconferencing innovations ready on the shelf, just to be used when they came to this good use.

Now, this has been my experience. But it would be interesting to know other examples—how societies managed from the end-user point of view. And as Joanna pointed out, there was this dangerous moment of whether governments would actually take advantage of the epidemic to create surveillance systems that could be used, if need be, at some other occasion.

Now, in our interactions with the GAC, we have argued that citizens and internet users are the same people. And during this pandemic, people … You could almost say that they were citizens because they were end users. They could play the role of active citizens because they had the internet. They were its users. In an emergency like this, resilience of the society seems to depend on the internet. To what extent, you can argue about. But I think that the lesson has not been lost on governments or any other stakeholders.

But this forced and sudden transformation from offline to online has also shown big gaps and dangerous divides, not only between developed and developing or underserved regions, not only between but also within countries. And I think that the experience has added just one more reason for leveling the field or trying to give equal opportunities for using the internet to all because the strengthening of the resilience of society is the interest of all stakeholders.

But now, for the bad news. Unfortunately, there have been always bad actors who want to exploit the distress of other people. And even a global pandemic looks like an opportunity to them. According to Europol, the European international police organization, criminals swiftly took advantage of the pandemic on the internet. They used the crisis to carry out social engineering attacks, phishing, and business email compromise.

Europol has assembled a long list of cyberattacks against organizations and individuals. Criminals took advantage of the heightened need and health concerns—need for information and supplies. There were even attacks at the health infrastructure, like a Czech hospital. The pandemic was a golden opportunity for all sorts of snake oil merchants. People were anxious to hear the good news about a miracle cure or vaccine. And according to Europol, well-known fraud schemes were rehashed and adapted to corona-related fears and hopes.

And as far as children are concerned, if they are in normal times addicted to their smartphones and video games, during the lockdown, their lives shifted further from the real world into an online, virtual one. And according to Europol, sex offenders found in this development an opportunity to access a broader group of potential victims. A report was published by Europol just a couple of days ago that raises alarm on child sexual exploitation images online during the pandemic.

Now, many of these heinous activities are squarely within the definition of DNS abuse—any definition at ICANN and its stakeholders. Action has been taken. And we'll hear about those actions during this meeting. There's a plenary session in a few hours about DNS Abuse and Malicious Registrations During COVID-19.

There was a webinar on this theme a couple of weeks ago. And the impression I got was that the number of malicious registrations was less than expected. And it was said that the media has done this a bigger problem than it was and so on and so forth. There is a discrepancy here because on the other hand, we have all this evidence of criminal activity noted by the Europol and probably other law enforcement agencies. So, the question is where did that come from? And I hope we hear some answers during this ICANN meeting.

Meanwhile, WHO, the World Health Organization, and UNESCO have raised alarm about what they call "infodemic" or "disinfodemic." And of course, we should respect the Bylaws and refrain from speaking about the content. But I think that two observations have to be made.

First of all, in the undergrowth—shrubbery on the internet—that kind of harmful weeds are hopelessly intertwined. It's like lions in a jungle creeping around each other. And misinformation and disinformation prepare ground for DNS scams of all sorts. And for the end users, it's all the same. And my question is if there is content that is just there for aiding and abetting DNS abuse, shouldn't that content also be treated as DNS abuse?

Second, even the framework to address abuse, led by Registries and Registrars, concedes that there are cases where registries and registrars should take action, even on what they call "website content abuse." It says that underlying such abuse is the physical and often irreversible threat to human life. These are the words from the framework.

And now, the UNESCO Disinformation Report points out that, and I quote, "In a growing number of cases, the consequences of this infodemic have been fatal. Many citizens are being duped, leaving them unable to understand and implement scientifically-grounded preventive measures. People are dying as a result of complacency or resorting to false cures."

So, to my mind, the borderline between DNS abuse and website content abuse is open for interpretation. It's a line drawn on the water and it may shift with time. And after the big storm like COVID-19, it would be good to revisit those waters again and redraw it again if necessary.

Finally, while we remember the 100s of thousands who have perished and are still reluctant to proclaim victory over this pandemic, I think that we can trust that as far as the internet is concerned, this experience has made the survivors stronger. As they said, what doesn't kill you makes you stronger. I believe that when dust has settled, the internet community, including everybody in their end-user role is stronger, more equal, and in a better shape to meet further challenges. Thank you.

CLAUDIA RUIZ: Joanna, are you able to speak?

JOANNA KULESZA: I should be unmuted now. Thank you very much Yrjo. This is exactly what we were looking for. I see the discussion in the chat. Thank you very much for this. As you might have noted, Yrjo, there are questions about data—about DNS abuse data—whether we have numbers for all these claims. Please kindly note, this is the first of DNS abuse and end-user issues sessions. We will host a sequence of these. One of them is focused exactly on acceptable thresholds and that will have specific numbers.

I don't think there are numbers that are carved in stone at this point, as Yrjo was saying. We are rather trying to shed some light on this phenomenon—that COVID-related … Allegedly, because I see some people saying here there is no specific DNS abuse that's related to COVID. So, we will try to explore this. Is there a specific trend we're facing in DNS abuse when it comes to COVID, as Yrjo was referring to?

If I could have the slide with Alex's introduction, Claudia, that would be wonderful. So, Alex will give us details on the measures that are taken and ICT tools that are being used. Because you might have concerns, we are using tracing apps as an example.

So, it seems like there is consensus about magical cures for COVID. Again, we will talk numbers as we progress with this meeting. So, those magical cures for coronavirus, if you advertise them, that's

consumer fraud. Consumer protection issues are raised as ground for enforcing DNS abuse prevention measures. Are there other aspects of this, rather than just consumer fraud—rather than just the concerns that Yrjo mentioned? We will look at an example of tracing apps that Alex will provide us with.

If I could ask you, Alex, to give us a very brief intro on the Fundamental Rights Agency. What is it that you guys do? What's the angle that you have on coronavirus, protecting individuals? And I know from personal experience you guys have done a tremendous series of bulletins that is focused on the latest developments in coronavirus preventive measures.

And this is why I'm really, really glad that you accepted our invitation at this late hour for you. Thank you so much for joining us. I'm happy to give you the floor. Our next presenter is Alexandros Kargopoulos, working from the Fundamental Rights Agency. Alex, the floor is yours. Thank you very much.

ALEXANDROS KARGOPOULOS: All right. Thank you. Good morning to everyone or good afternoon. I'm very glad to be here amongst this company to present to you. First of all, a couple [thoughts] of who we are and what we do. I work for the Fundamental Rights Agency. The Fundamental Rights Agency is an independent body that was established back in 2017 with regulation 168/2007. It's a specialized agency of the [EU—a public] institution.

Our staff includes legal experts, political and social scientists, statisticians, and communication specialists. Personally, I'm a legal expert. And our main purpose as an institution is to instill a fundamental rights culture across the EU and helping bring the charter to life for everyone in the EU.

Our team shares evidence-based insights, [backed with] advice with policy decision makers and with stakeholders from the local to the national level. In particular, we issue analytical reports, policy briefs, focus papers, legal opinions on pending legislative initiatives by the commission and so on and so forth, based on desk research, on qualitative socio-legal studies, and large-scale quantitative surveys.

And we aim at collecting and analyzing data from the EU member states. And we provide independent, evidence-based advice on rights. For example, I would like to briefly mention a [inaudible] that could be of interest to you all, is the quite successful so far [inaudible] European data protection laws back in 2018. And also [ready to publish], for example, [inaudible] big data—the big data discrimination in data policy decision making, focus papers dealing with discrimination.

Also, a paper on data quality and artificial intelligence, which discusses the relevance of data quality in AI big data systems from a fundamental rights perspective. And also, in our website, you will find all kinds of products, materials that are freely accessible and available to all.

In this context—in the context of [inaudible], we are currently issuing a monthly bulletin with respect to fundamental rights, implications of

the coronavirus pandemic in the European Union. This bulletin looks at the [the vast] fundamental rights issues posed by measures implemented to counter the pandemic amongst EU member states—for example, its effect on the judicial system, work-related issues, measures affecting marginalized and distinct groups of persons, so on and so forth.

In this context, there's a second bulletin, which covers a period between 21st of March to the 30th of April, with dedicated-focus chapter on the technological solutions developed by EU member states, which involve processing of users' data to help contain the pandemic. The focal point of the discussion, as our bulletin was focused, was the use of contact-tracing apps.

Also, besides those, our evidence indicates and analyzed the use of self-reporting websites and mobile apps. Also, the use of location data from telecommunication providers for tracking people and [inaudible] the use of analyzed mobility data of population used for statistical [or other] similar general purposes. And also, other measures involving the processing of users' data, such for example drone surveillance during social distancing measures, thermal cameras, the workplace, and so on and so forth.

Now, before going into detail on contact-tracing apps and further other [technological] exploits, first I would like to start of with a small intervention from the measures taken—from the measures adopted by EU member states on access and use of communication data from service providers.

As mentioned, our evidence shows that across the EU member states, two measures are employed. First, the use of aggregate communication data to assess and evaluate the mobility of populations and the use of traffic and location data belonging to identified individuals, in particular to track down individual people in forced isolation and quarantine restrictions.

As regards to the access to individual communication data, of course, these are the most alarming fundamental … This have brought forward these measures—the most alarming fundamental rights concerns. Our evidence shows that for the referencing period of the second bulletin, a considerable number of member states, namely Bulgaria, Czechia, Hungary, Latvia, Poland, and Slovakia all passed legislation allowing their health and police authorities to access and process traffic and location metadata from communication providers, track down individuals in the context of COVID-19, especially individuals that were under forced quarantine isolation. [Lithuania] was also [purveying] similar legislation during the reference period.

In Hungary, new laws gave considerable powers to health, police, and immigration authorities, and the minster of innovation and technology, to access various personal data of users, including also their telecommunication data. Only the Czech Republic, consent of the user was required, while for the others, such access is mandatory, irrespective of the user's consent. Czechia also said data cannot be as of these [communal] proceedings. In Bulgaria, judicial approval is required but only in an ex post basis.

In Poland—this is a notable example—people in forced quarantine must download and use a mobile application for such purposes. Installation and use of this application is mandatory. And this application actually registers the user's home address and accordingly warns the local police, based on traffic and location data and GPS data from the device, when the user is breaching the mandatory isolation.

Our evidence suggests that such measure attracted a lot of criticism from civil society, political positions, and experts. For example, in Germany, the health minister tried to pass a similar legislation—a legal amendment—allowing the authorities to access communication data for tracking individuals. And then, the government withdrew the draft legislative amendment after public criticism. The Croatian government also withdrew a similar draft amendment after similar criticism from NGOs, academia, and the [inaudible].

Also, quite importantly, in Bulgaria and Slovakia, where such legislation has passed, relative constitutional complaints were filed, which were pending during the referencing period of our report.

Why is this discussion important? It's important because Article 15 of the Privacy Directive, "exception allows authorities to access and process the traffic and location metadata only in cases of threats against public or national security or for preventing, prosecuting, investigating, or [inaudible] crime." It does not include, as such, an explicit basis to access such data on public health grounds.

On the contrary, Article 23 of the GDPR, "personal data rights may be restricted for reasons of public health." Therefore, it's debatable to which extent such data—that is metadata from communication providers, belonging to identified individuals—can be lawfully acquired and processed on a mandatory basis for COVID-19 purposes.

Now, with regards to aggregate data, the situation is a bit different because according to the GDPR, "anonymized data are not considered personal datasets, provided that individuals cannot be identified." Our evidence shows that authorities, at least in Austria, Bulgaria, Croatia, France, Germany, Denmark, and Estonia, Finland and Slovakia as well, are using such aggregate data from communication providers for statistical and other purposes relating to COVID-19.

In Austria, Denmark, Estonia, and Germany, the national DPAs confirmed the legitimacy of such practice and were heavily involved in determining the conditions for such processing of such data deriving from communication providers.

Other notable examples include, for example, France, where 11 universities concluded an agreement with Facebook, allowing them to access aggregate data from Facebook's users for research purposes relating to COVID-19. Such data also include—from Facebook—includes location, traffic data, and social maps of users' interactions.

However, concerns still remain. For example, in Germany and Denmark, there were fears from civil society raised that anonymization of such data can be reversed and that such data can be accessed by third parties.

Now, let's turn to the discussion to the issue of contact-tracing apps. First of all, what is currently widely known as contract-tracing apps are apps installed on mobile phones and other mobile devices that use Bluetooth sensors or can also use location data from mobile devices to create a record of persons that came in proximity with its other. This mainly allows for warnings to be sent to those people, once a user tests positive. And also, it enables better contact tracing.

Therefore, in reality, the term "contact-tracing" is a bit misleading, as in essence, what these apps do is they actually perform proximity tracing, not contract tracing as such, in epidemiological terms. So, actually, the term "contact-tracing" does not describe the method used but rather the purpose of such apps.

In March 2020, the World Health Organization urged countries to track or test any individual showing symptoms. And also, the Commission, with joint European roadmap towards lifting COVID-19 containment measures highlighted the use of contract-tracing mobile apps as among the measures that will support deconfinement. This was also reiterated by the Center for Disease Prevention and Control. So, the relevance comes more strongly not during the lockdown period but mostly during the deconfinement period—the period that we are passing now—mainly in the EU member states.

Now, the main concerns, according to our findings, that relate to the use of such is actually that such apps allow the monitoring of individuals' private life. They enable access to a person's contacts and

whereabouts. Based on such data, one can actually produce a complete social graph of a person.

Continuous access to data and systemic monitoring of individuals by contact-tracing and other similar apps, however, constitutes a serious interference with fundamental rights, namely the right to personal data protection and the right to private life. Identifying a person's associations with other individuals or whereabouts could actually reveal her or his political or even religious beliefs, for example.

Also, such data—at least the danger that lies with the use of contact-tracing apps—is that such data deriving from this application can be repurposed and used for other purposes—for example, for surveillance purposes and so on and so forth. And also used by themselves, or more dangerously, when such data are combined and used with other data, such for example data deriving from communication providers.

Also, another main concern relating to such apps is that their efficiency is quite dubious. It is uncertain to what extent proximity tracing through contact-tracing apps is relevant for epidemiological purposes.

And here we have, for example … We have two notable examples. Two people that are in close proximity to each other but behind a wall in an office, which actually they never come into contact with each other but based on contact-tracing apps, these people were in proximity. So, you have a warning if one or these two is tested positive.

Or also, we can have another example by two people, taking the opposite example, are within minutes in the same closed space. For example, they take the same elevator but never come in contact with each other so we don't have a proximity warning but it will be quite probable that one person has infected the other person through this type of contact, which cannot be traced by proximity tracing.

Also, according to the studies, a very large number of persons must use such apps in order for these apps to be effective. According to the study published by [inaudible] University, 60% of all mobile phone users and 80% of smartphone mobile users much use such apps in order for those apps to be effective.

Of course, others caution that contact-tracing apps may provide a false sense of security, as mobile phones and their sensors are tracing coronavirus exposures, which cause a false a senses of security to end users who may feel that they are protected by these contract-tracing apps and that they will be warned if somebody tests positive. But in essence, we are not sure to which extent this will be [accessible] for their location.

Now, with regards to the EU responses in the use contract-tracing apps, the EU has been quite in active as a whole in providing a regulatory framework [inaudible]. So far, however, most of the ad hoc initiatives taken by the commission—the European Data Protection Board—are soft law instruments.

For example, European Commission published three important documents in April, [inaudible] books for the use of mobile

applications and the guidance of maps, supporting the fight against coronavirus epidemic in relation to data protection. The European Data Protection board also adopted guidelines for the use of location data and contact-tracing tools. The Council of Europe also published a joint statement, setting [out the] standards.

Of course, all these soft law instruments actually build on the existing law, including in particular the GDPR, Convention 108+ and the Privacy Directive, as well as the Charter of Fundamental Rights. All these highlight the following technical requirements that such apps should follow. Mainly, for example, the voluntary use of such apps. That there should be a [prior] assessment before such apps are released. That privacy by design and data anonymization are principles that should be effected in the technicalities of those apps. The need for specified purposes, clearly [a basis]. The use of anonymized data only. Security requirements that need to be placed to protect from cyberattacks.

Non-use of location data, GPS. So, according to the EU [institutions], such contract-tracing apps should not be based on GPS or other location data but only on Bluetooth proximity data. The need to follow interoperability. The existence of sunset clauses—for example, deactivation and deletion after the epidemic, and so on and so forth.

These are all, so far, in the guidelines that the EU institutions have published. However, the situation in the EU member states, indeed, is quite diverse and varies significantly. During the referencing of our bulletin of our research, from the 27 EU member states, in all but

seven, contact-tracing apps were either under development or already available.

We've seen a variety of models in developing such contact-tracing apps. In some members states, like for example Germany, Ireland, and Denmark, whereby public authorities were collaborating with the private sector and [inaudible] an institution for the development of such contact-tracing apps. In other member states, such for example Cyprus, such contact-tracing apps were developed by private actors, and are freely distributed, and were not subject to authorization or [regime]. So, [inaudible] promote their use.

Now, with regards to the technical specificities of such apps, our findings indicate that apps in the majority of EU member states, they rely on Bluetooth data, indeed—Bluetooth proximity data. However, apps in Bulgaria, Cyprus, and Lithuania are based on network and on GPS location data, not on Bluetooth data. In Slovakia, the available app uses Bluetooth and location data at the same time.

The biggest probability [inaudible] has raised with regard to the use of such apps is whether such apps should follow a centralized or backend architecture or whether they should follow decentralized approach. In the first, data, such as encryption keys in particular, are generated and stored in the central server who attributes those to particular users. In the other model, the decentralized model, all data, especially encryption keys and the [individual] identifiers that are generated by the user's device are generated and stored exclusively on user's device.

Especially from the civil society, civil society has so far seemed to be promoting the use of decentralized data, as most commenters argued that the decentralized model is more end-user friendly, particularly with respect to data protection and privacy concerns.

The European Commission, the European Data Protection Board, did not specifically advocate either approach. However, the European Parliament specifically proposes the use of decentralized models by members states and is against the use of centralized models.

However, our findings from the situation in the EU member states indicate the states are equally divided in which model to follow. For example, in Estonia, Finland, and Poland, which follow a decentralized model, the user can consent to share his Bluetooth proximity data with health authorities. In Portugal also, which follows a decentralized model, warning of other users is done only after the authorization of an intermediate medical expert. In Czechia, on the other hand, which follows a centralized model, authorities have access to personal data but for a limited time only.

It appears that centralized systems did attract most of [people's] concerns, as they're prone to [inaudible] cyberattacks. As commentators argue, it's much easier for particular users to identified through centralized apps. And this can be done, for example, either through designated attribution of encryption keys to users or even through combination of other personal data—for example, combining the user's IP address that will be available to the server with whom the user comes into contact to download and use the app. Or even the

combination of other personal data breaches—for example, telephone numbers.

Now, also, our evidence suggests that in many EU member states, contact-tracing apps, such for example in Austria, Bulgaria, Denmark, the Basque Region, in Latvia, Lithuania, Poland, and Slovakia as well also include further health functionalities, such as symptom reporting, medical screening, and communication with health authorities.

For example, in Denmark, the app informed users if their COVID-19 test is positive. This is effected mainly by the unique user code that is available to all citizens alike, which identifies the users with the government and the central services provided by the government, such as, for example, health services. The app in Lithuania, also, enables coronavirus symptom tracking and also the receiving of health advice and information. In Austria, a recent legal amendment provided that the available contact-tracing app also is bundled with voluntary screening functionalities to enable end users to transmit personal and health data to the nearest health authority.

Relatively, the European commission stressed that users should be able, through the app, to provide their consent separately for each of app's functionalities. And when you have an app that is bundling different functionalities, consent should be provided distinctly for all those functionalities separately.

Now, another issue of concern is the source code availability and transparency. Evidence gathered by our agency shows that the source code of tracing apps is or will be hopefully made public in most EU

member states. However, most EU member states have not included a distinct legal obligation in this respect, forcing developers to make such source codes transparent.

Also, our evidence shows that in some of the states, such contact-tracing apps must pass through mandatory state authorization before they are released. For example, in Italy, the COVID [administration] has set up a task force of experts that review the proposed contact-tracing apps, and especially review those contact-tracing apps with respect to data protection conformity and the technical requirements. The same has happened in Netherlands, where at the end, no contact-tracing app that was proposed was able to pass the relative scrutiny by the authorities.

And it's quite … It's a very positive step that a lot of member states, such as, for example, France, and Finland, and Italy, Latvia, and the Netherlands, also the data protection authorities were involved in this process by examining and assessing the data protection conformity and the technical characteristics of such contact-tracing apps.

Now, I would like to close this presentation by making some closing remarks and saying that, indeed, we see that technology is a tool that can help governments and can help society to overpass and curb the epidemic. However, we should be really cautious of disproportionate use of technology that may actually lead to form of digital captivity of people, whereby technologies that have been untested or unclear as to their advantages—as to their relevance for fighting the epidemic—are used and are used in a mandated manner by citizens.

The role of technology and private access in the civil society is quite reinforced in developing such apps but also in scrutinizing such apps or other technologies that are available at large. And also, we've seen, at the same time, the benefit but also the disadvantages of that GDPR. First of all, we see the benefit of, in the sense that we have a flexible [inaudible] for technologies to be developed. But on the other hand, we see its limits, whereby the open-ended architecture of the GDPR actually requires for more specific legislation to pass in order to establish guarantees for [inaudible] the end users.

And thus, I would like to close here at this point. I would like to thank you all.

CLAUDIA RUIZ: One moment, Joanna. We're not able to hear you. One moment.

JOANNA KULESZA: Now I'm unmuted. Thank you very much, Alex. That was an interesting presentation, especially when we look at the chat that seems to have gone up in comments. The ground we're exploring here is using this example, that Alex has provided us with in much detail, as a possible threat to end-user rights.

So, the link we're trying to explore is, if you will, to a certain simplification, a comparison between COVID cures, which are clearly infringing upon end-user rights—I don't think there is a discussion on that, as Yrjo emphasized, unless we're discussing that as well. And that

would be going back, I believe—and apps that Alex described in much detail as predominately abusive.

So, the Fundamental Rights Agency has significant concerns. And I understand [inaudible] in his professional capacity. So, nothing more than serious concerns would probably be [right] here. But as he indicated, civil society also, including the data protection authorities in Europe, is concerned with that specific way of targeting the pandemic. If those apps are illegal, they would be threat to end-user interests. If they are hosted on a website en masse, or if they are hosted on different websites, would that be abusive? Would that be something were we come in?

The answer could simply be no. We say, "Well, there's no end-user interest here. We don't care. We have no tools to address it." Is the DNS abuse framework a tool we could use? Is there ground for end users and to try and advocate their interests? We've looked at GDPR. We've looked at WHOIS. We've looked at IPs. Maybe there is a way for us to also be aware of this happening. This would be just an example. There are a few other fundamental issues or rights we might want to address. We've selected this one because the FRA has been wonderful in providing comprehensive study.

So, the threat we're facing is one of end users' data. It is being used beyond allowed limits, thus being abusive. We will take questions in the Q&A round. We are a little bit beyond our planned agenda. Thank you very much, again, Alex. We're hoping you will stick around and answer questions. If you do have questions, as Michelle is indicating in

the chat, please post. I've kindly asked staff to keep track of the questions that are being posed. We will try to pick them up in the time that is left for us.

And we have Marita Moll. Marita, the most challenging question is your hands. Is there a job for us? Is there something we can do as the multistakeholder model evolves? Or is this something that that governments are doing? There's little we can do. There's nothing we can do. What is more, if the government are forevermore strong and designing specific laws, will this impact how we do our job here?

I'm going to give you the floor. As I already said, we're a little bit beyond our planned schedule. Marita has a few slides. I'm certain our wonderful tech support and staff will put them up. Marita, the floor is yours. Thank you very much.

CLAUDIA RUIZ: One moment, Marita, while we unmute your microphone. Marita, are you able to speak? Marita, can you please check—

MARITA MOLL: I've unmuted myself.

CLAUDIA RUIZ: Thank you.

MARITA MOLL: All right. Thank you. It's not clear whether you're doing it centrally, or whether we're doing it, or we're both doing it. Thank you, everyone, and thank you for the previous two presenters. Really interesting information. My name is Marita Moll. Last time I said that on the previous meeting, my name was stolen by a Zoom bomber. So, if you hear an echo, maybe it's not me.

But no. I actually have a different task here and that is the task to talk about the multistakeholder system and maybe how we might be seeing changes in that system because of the COVID-19 circumstances that have been imposed upon us. So, I won't be talking about DNS abuse but more about how we're going to manage moving, with the multistakeholder system, back into a way of working that works for us but probably going to be different.

Can I have the first slide, please? Okay. I'm going to start out with a quote by a very long-time participant in this world, Wolfgang Kleinwächter, who wrote a wonderful article in CircleID last week. And this is what he said. It was really an article about the new UN Roadmap on Digital Cooperation. But I thought it's relevant here, the way he's phrased it.

"Many governments fear that the opening of the UN doors to non-state actors is a risky infiltration of state sovereignty, which is the core principle of the UN system. When governments accepted Tunis compromise on the multistakeholder to internet governance, their understanding was that work for the internet but not for the world. Now, the internet is the world and there is no world anymore with the

internet. So, two different cultures are colliding but this clash offers more opportunities than risks."

I think his comment really holds true right now, that the internet is the world. The last three months has really shown us that our way of coping with this kind of crisis is just so hugely different than how we might have previously coped with such a crisis. It's not the first time a pandemic has visited the world. But much of the world, we were able to carry on doing what we were doing. And that's because the internet has enabled us to do that. And so, it's just become absolutely crucial. And so, we have to work out how we can manage this in the future. And we'll have the next slide, please.

Sometimes, it's suggested that COVID is going to not work or make it harder for us to work in this multistakeholder way. I think that there's too much going on out there to think that it's multistakeholder way of doing things is going to stop. Might slow down.

The thing I present as evidence here is that the UN Roadmap for Digital Cooperation, which is just being introduced, is going to try to expand the concept of multistakeholder cooperation into other fora, suggesting that it would bring stakeholders from governments, business, science, technology, and civil society together in other places, like digital trade, human rights, and future technologies. We can think of the World Trade Organization or the International Labor Organization.

But the idea is that because the internet is so fundamental, underlying to all the work that we do, that the multistakeholder process really

has to be part of it at all levels. Now, that is despite and recognizing that there are world tensions currently, which have been enhanced by the current pandemic. There's more distress, more misinformation, more surveillance, apps that are going to track us if we accept them.

So, it may make it a little more difficult and make it take a little longer to do this kind of things—introducing the MS progress into other fora. But it's more important than ever because the internet is the world. And so, we must continue to take this process seriously and bring it to other places.

That's an introduction to talking about what's happening at ICANN with the multistakeholder process and how the process might be affected by what's going on right now. Next slide, please.

We're going to have one year now, once we get through the next meeting in Hamburg being virtual, without any face-to-face meetings. And I think it has to be said that the community has adjusted incredibly well. It is, after all, a community that's accustomed to working virtually and does it all year long. So, just carrying on in some various intensive and immersive situations, as in meetings that last for days, we can definitely say that it has gone well. But can it continue like this.

In all of our countries, the pandemic managed to expose the vulnerabilities in our systems. In Canada particularly, it exposed that we were not dealing with our elderly population very well and that those were the people who were held—who were most impacted and died due to the pandemic because our systems to manage the health

and welfare of elderly people was really very bad. And we knew this all along. So, that was a vulnerability that was exposed in a very brutal way.

Vulnerabilities will be exposed by things like this and that will happen, also, in our ICANN environment. We know, from the work we've done over the last two years in the multistakeholder evolution process, that there are a number of weaknesses in the system. And we are currently trying to work our way through those. We have currently a request for comments out to deal with the six remaining topics, about setting priorities and how we deal with consensus, and scoping. So, we're working on those things.

But we know, in the end, I think, that the volunteer constituencies supporting the system are most at risk. That's where our biggest risk is because if we can't support those people, we won't have a multistakeholder system. Can I have the next slide, please.

There are a number of pressure points here, which tell us that things aren't going to change. For one thing, we're realizing just how much it costs to put on face-to-face meetings—approximately four million US dollars, whereas $500,000 US dollars, approximately, for virtual meetings. That's a lot of money that could possibly be used in ways that might benefit us more.

One thing that's not on this slide, and it should be in here in capital letters, was the environmental issues. And these are coming up. For the past two years, we've been hearing about, "Well, is this really a very environmentally-sound thing to do, to be shuffling many, many

people from one location in the world to another?" So that's another pressure point that has to be thought about as we start to move into a new world.

However, we also know that recruiting for the volunteer constituencies relies on the face-to-face meetings for education and engagement. This is a way that we ramp up volunteers. And it's going to take a lot of thought in how we actually manage if we're not meeting all the time in the same way. And we all know that meeting face-to-face really helps make decisions. It helps people find their way through impasses. So, how would we do this in another type of scenario? Can I have the next slide, please.

Those are the things that are going to be difficult. But we also need to look at the opportunities that are going to be created by this. We could find our way into new configurations and new options for ways of meeting and ways of making decisions—new ways for communities to engage with each other. When we do all that, we're probably going to find new alliances and new partners to work with. And if we take the time to do this carefully—trial and error … There's going to be errors. There's going to be things that don't work. But we can end up with a system with is better in unanticipated ways. Please have the next slide.

Stimuli. It should say "stimuli," not "stimulus." Some of the things that could happen is that perhaps we'll move into hybrid-type meetings. Maybe we don't need to. Maybe we're not all dying to sit on planes for

14 hours, spend four or five days in a meeting room with no windows, get back on the plane, and come home.

Maybe there are better ways of doing that. Maybe we could have hybrid meeting schedules. We could have new outreach possibilities to build the multistakeholder system from the ground up in a more sound way than we're doing now.

Bringing this back to the end users, they're local and they're very hard to reach. It's not easy to set up meetings about ICANN, to get people interested in topics they don't know about and things that happened at meetings they didn't go to. So maybe, if you had meetings more locally, you would get more people interested and more information out there. So, this could be innovative and it could support experimentation. Let's go to the next slide.

Yes. So, has COVID-19 redefined the multistakeholder consensus development in the ICANN space? Not yet. But we're beginning to realize that it's probably not going to be a return to exactly the way things were, in all aspects of our lives and in this one, most certainly so.

We're going to have to be ready and willing to experiment. I think were going to have to trust each other and make sure that—trust each other to be committed to the principles of inclusion and representation that were some of the very basis of issues that came out, or are coming out, in the evolving multistakeholder system.

So, this does all fit into how that system evolves. And so, it's not optional that we do this—we figure out better ways to include and make sure that people are represented. And maybe this is going to give us the perfect opportunity to find different ways. I'm not in any way suggesting that we should not be having meetings and meeting each other. But maybe in different ways, maybe not as often as the world meetings. Next slide, please.

So, can we still make decisions bottom-up when public health and security are at stake? As we saw at the onset of the world crisis, the speed was essential and cooperation was essential. And those countries that realized that and moved quickly were better off in the end. But crisis is temporary. And the key thing here is how we're going to exit that crisis and how we're going to figure out where the danger zones are as we come out of it.

For the multistakeholder system, I think we have to work our way through the future. We'll have to trust and be committed to the process. But in the end, it could be very much stronger, as long as we don't all try to defend and expand our territory. As we work together, we could come up with a more interesting, better system in this great experiment of how to have many people involved in such important decision making. So, I'm going to leave it at that. Thank you for the opportunity.

JOANNA KULESZA: Thank you very much. Thank you, Marita. I feel like there's a lot of emotion in this room, which I think is wonderful. And that is largely

due to our wonderful presenters. We have questions in the chat. They are noted. I see hands going up. And this is actually what I was hoping to do. I would like to hear back from those of you who feel there is a comment needed—there are issues that need to be raised during the 12 minutes we have left.

I have Sebastien and I have Owen who have their hands up. I'm looking forward to those comments. If I could just ask you, gentlemen, to keep your comments brief. I would like us to close on time. And then, possibly, after a very brief summary. Sebastien, the floor is yours. The same goes for Owen. Please try to keep your comments brief. If there are any other comments, do feel free to raise your hands. I'm going to hand it over to Claudia to manage the muting any unmuting of our speakers. It's Sebastien and Owen next. Thank you very much.

CLAUDIA RUIZ: Sebastien, you should be able to unmute yourself now.

SEBASTIEN BACHOLLET: Thank you very much. I was hoping to be able to speak in French but I don't find out how I can do that. I was following the discussion in French but I have to move back to Zoom and it seems that I have only to speak English. Okay. Maybe next time.

I am concerned that it seems to be, this presentation, the way of thinking of At-Large and of ALAC, and I hope it's not. And I hope that we will have some time to have this discussion. I'm not sure that we

need to have this discussion. Or we may have this discussion here. But don't forget we will not … I hope we will not saw the branch we are sitting on. And it's exactly what's happened with this last presentation. And I am very, very worried about that.

There are already meetings going on at the local level. Plenty of meetings are going on at the local level. They are done by our At-Large structure. They are done by Global Stakeholder Engagement. They are done by other parts of ICANN and other constituencies or stakeholders.

Therefore, what I think is important is what we learned from this situation of one year without physical meeting. It's how we can do better work in between two face-to-face meetings. Because face-to-face meeting is not just what we are doing here. It's a lot of other things. We are also meeting people, doing business, for people who are doing business, and then seeing some issues not just related with ICANN.

Therefore, we can't just say, "Oh. We have proven that we can work." Yeah. But we've proven that we work quite badly, or not as efficient as if it's face-to-face. So, for some parts it was interesting—more people. Therefore, I would like that we take the good of each part and not saying we need to have one to replace the other.

And I have plenty other things to say but unfortunately, we have no time and Joanna told me that I have just one and half minutes. That's okay. I will stop here. But frankly, if we don't have this discussion

within At-Large, taking into account the point of view of each RALO, for example, and ALSs, we will have missed a lot. Thank you.

CLAUDIA RUIZ: Okay. Thank you, Sebastien. Owen, are you able to speak?

OWEN SMIGELSKI: Yes, I am. Hopefully everybody can hear me.

CLAUDIA RUIZ: Yes.

OWEN SMIGELSKI: Great. Thank you. So, I just wanted to highlight I appreciate the ALAC taking this. Abuse is a very important thing. But I just wanted to also bring some facts and data back into this because I used to work at ICANN. I worked in Compliance. I was there for six, seven years. And now I work for a registrar.

The COVID-19 response, I was shocked at how the whole industry worked. Registrars and registries came together and just did this whole amazing collective. And they worked with law enforcement, and government agencies, and stuff like that. It was ridiculous, the amount of domain names that were reviewed and taken care of. It was great. It was awesome.

And so, I just don't want that to be overlooked, or missed, or something that we don't recognize that because this industry did a

really, really, really amazing job in some extraordinary circumstances. And I think we should recognize that and understand that moving forward, we can do that. And if we need to do something crazy like that in the future, we can do that. But that was good. But I don't want that to be … There's data and facts missing here. So, I just want everyone to realize that a lot of stuff was done good here. Thank you.

CLAUDIA RUIZ: Okay. Thank you. Fabricio, you can unmute.

FABRICIO VAYRA: Ah. Yes. Can you hear me?

CLAUDIA RUIZ: Yes. We can hear you. Thank you.

FABRICIO VAYRA: Great. Yeah. Listen, I want to applaud Owen for bringing up all the great effort that was just done in response to COVID. I just clearly … I went back, actually, before the session and looked at what's led up to COVID, at least in my time at ICANN. And today it's COVID. A while ago, it was earthquakes. Before that it was hurricanes. The bad actors basically take advantage of every big event that comes up.

And so, my question, I guess, for Owen and industry is why is it that we're constantly waiting for the bad thing to happen and for someone in Congress to write you to pull together and do all this great work that

we're applauding right now, as opposed to understanding that the bad actors aren't going to go away and that we should just set up those systems now to be proactive, to make the system healthier, to help consumers, etc.

I just don't think that being reactive is probably the answer. We should learn from what's happened, and especially what's just happened, and build our systems proactive, and continue to work. And that should include ICANN Compliance, as opposed to ICANN constantly pushing the effort back on the community and registrars.

CLAUDIA RUIZ: Thank you. Joanna, we're not able to hear you.

JOANNA KULESZA: Thank you. Thank you very much. Thank you, gentlemen, for those comments. I see Sebastien's hand is up again. I'm going to give you the floor very briefly again, Sebastien. I'm just wondering if we have any comments from our panelists, since they have taken the time to join us at times and peculiar hours. So, I'm wondering if our panelists wish to have any summary. I'm going to give Sebastien the floor briefly again. And then, I'm going to try and wrap up this exciting discussion.

We have questions noted down. We will, for the sake of time, try to answer them on the wiki. I think that's an appropriate space. I will seek counsel from our wonderful staff, where to best place them. As you noted, there is also a Twitter feed that you're more than welcome to use.

So, this is me checking with our presenters, if there is anything Yrjo, Marita, or Alex want to address in the three minutes we have left at this point. No? I see a no from Marita and I don't see our gentlemen stepping up. Sebastien, for brief comment, go right ahead. And then, I'm going to try and wrap up.

SEBASTIEN BACHOLLET: Joanna, I'm able now to use the English interpretation—the tools we do have. That's why I'm speaking in French. And I want to make sure that the system works well. We have to adapt to this new system. I hope you can hear me.

Just to make sure that the next time we want to take the floor in another language—in French or in Spanish—for ALAC, we can do it and make sure that the interpretation into English works well. This is a great tool but we have to use it. Thank you so much.

Thank you very much, Joanna. Just to test if the French interpretation is working for everybody and if everybody can use the tool. Thank you very much. And I look forward for continuing this discussion. Sorry for that.

JOANNA KULESZA: Thank you very much, Sebastien. Thank you for testing. This is the first policy session. It's good to know that it's working. And it is, indeed working. I could, without an interruption, hear our wonderful French interpreter. Thank you very much for all your work.

Thank you, everyone who participated. Thank you for taking the time. Thank you for the lively discussion in the chat. This is me trying to wrap up, since we have only a few minutes left. Our staff will be happy to assist you with using the translation tool. We're looking forward to you joining our other policy sessions here with At-Large.

This is the place for consensus so all your views are most welcome. It might be easier to find consensus in person, as Marita emphasized. And I've seen that mentioned, also, in the chat by Jonathan. But we're glad that you're here. These are challenging times, as Marita said, and we need to be working together.

The point of departure is to understand where end-user interests lie. And this was the purpose of this discussion. Is there an interest within the community to look at that specific aspect of end-user interests and include it in the DNS abuse framework? As I already said, there are different examples we might want to look into. This is something that came up because of the pandemic. So, there are specific individual interests we might want to look at.

But there is a discussion around DNS abuse—how broad the topic is, how closely this links to national, regional legislation. I've appreciated discussions we've had before around cybercrime conventions, national criminal laws. I would like to hear those discussions again within the DNS abuse discussion—the dialog we're having—the framework that is being defined. We're trying to shape and specify.

So, I look forward to you participating in other At-Large sessions. Most of those focused on DNS abuse, including setting an acceptable

threshold—something that came up in our discussions in the chat. When do we know that DNS is abuse is happening? Is it real? Do we have metrics? There is a group chanting metrics in the background of this meeting. So, I encourage you to participate in that discussion. I hope you have found this meeting—these theme—to be thought provoking.

I would like to thank our panelists for taking the time and taking a bit of a different look—a different approach—to the policies we're developing or the scope of policies we're developing, with specific focus on DNS abuse. Thank you to all of those who participated. I know we have some of you participating at peculiar hours. I know we have some of those who are not ICANN meetings regular, including one of our speakers. So, thank you very much for taking on this challenge—trying to talk to us and trying to discuss the COVID pandemic in the context of multistakeholder model further development.

I want to thank our interpreters. Great job, guys. Great job from the tech team. Everything seems to be working smoothly. Once again, thank you to our panelists. And last but not least, thank you to our staff. We would not have been able to do this without you. With that, I'm going to conclude, just two minutes past the top of the hour. And I look forward to seeing you again in virtual Kuala Lumpur. Thank you, everyone. The meeting's adjourned.

CLAUDIA RUIZ: Thank you, everyone.

[END OF TRANSCRIPTION]