BARCELONA – HLGM: Thematic Challenges in the IG Ecosystem – Cybercrime, Data Protection and Privacy
Monday, October 22, 2018 – 12:15 to 13:30 CEST
ICANN63 | Barcelona, Spain

MANAL ISMAIL: So with your permission, please allow me to introduce the chair of the following session. Mr. Francisco Polo, Secretary of State for Digital Advancement at the Spanish Ministry of Economy and Business.

And session two will be on thematic challenges in the Internet governance ecosystem including cybercrime, data protection, and privacy. So thank you, everyone, for understanding, and it is just to make sure we finish in time for lunch. Thank you.

FRANCISCO POLO: Please, we are starting now session 2. There is no coffee break upstairs. We are running out of time. Session 2 is starting now.

Welcome back from the coffee break. We are now moving on the last session of the morning. During the next hour and a quarter we will discuss about an exciting subject, cybercrime, data protection, and privacy.

In particular, we will address the need to find a way through dialogue and cooperation to tackle these challenges recognizing the concerns, government and individuals have with respect to privacy, data protection, and the increase in cybercrime. We will also explore how to maintain human rights and an open Internet in an environment of

increasing national and regional legislation which can have a converse influence.

To expand upon these aspects, I give the floor to the moderator of the table. It is a pleasure to rely the attendance of our chairman of the Senegalese Data Protection Act.

AWA N'DIAYE: Thank you very much, Mr. Minister. I would like, if you allow, to speak French.

I would like to start right away. We will first thank the Spanish government, of course, as well as ICANN for this high-level government meeting. We would like to go back, if I may say, on the topic that was spoken about quite a bit already.

It is a very hot topic, very current topic. That current topic has been mentioned previously. It is the issue of security and integrity of the Internet as it relates to cybercrime.

We all know that ICANN is the technical protector of that or make sure that we have security online. But, of course, even though there is remarkable work done within ICANN, unfortunately, it is not enough in order to prevent different threats from being present on the Internet. So let us first ask Mr. John Crain who is in charge of security within ICANN to talk to us about governance. He is in charge of the issues of governance and security.

And so he is a key component within ICANN to make sure that the Internet is open, secure, and stable.

So let us see what he has to tell us. Mr. John Crain, you have the floor.

JOHN CRAIN: Thank you very much. And thank you, everybody, for giving me this opportunity.

I want to talk a little bit almost philosophically about technology and the principles that the Internet was designed over. The Internet or the ARPANET, as it was once called, is often described as being something revolutionary. And indeed it is. It has changed the way that our society works. It was based on principles such as Postel's law, which was developed by Jon Postel and published in 1989.

And the principle is, basically, be liberal in what you accept and conservative in what you send.

This and similar protocols were used -- or similar principles were used in developing the protocols that the Internet works on. Much of the growth of the Internet may be traced back to these initial principles, including principles such as openness and transparency.

Those early technologies and early protocols were aimed at making the network work.

WHOIS, which you've probably heard of, was one of those protocols. And it was an integral part of how those developing the network and

joining the network communicated with each other to solve operational problems.

Over time WHOIS evolved with the growth of the Internet to serve the need of many different stakeholders such as the registrants of domain names, law enforcement, intellectual property, and trademark owners, businesses, and individuals.

But the main principle of the WHOIS protocol and its use has always remained the same.

The stable operation of the Internet relies on a basic concept. You cannot run a decentralized system, of which the Internet is one. It is a network of networks -- if you cannot find the people who operate its parts to ward off problems and to coordinate responses to issues.

In cases of system failures, abuse or attacks, access to data about who is responsible for which parts of the ecosystem becomes critical to ensure or quickly restore the stable and secure operation of the Internet.

This is a matter that relates to the operational integrity of the Internet.

An example of this could be, for example, as simple as informing someone that that Web site has been compromised and has some form of malicious content. Or it could be talking to an Internet service provider to let them know that there are problems with their service.

But the Internet was not only revolutionary. It is also evolutionary. It changes. It evolves to adapt to the needs of the users and society. In many ways the Internet reflects the users and the society that uses it.

Principles have changed over time.

One of the guiding principles today is, of course, security.

An early example of technology that brought added security to the Internet is something called HTTPS.

This was developed in 1999, less than 20 years ago.

And this technology that now allows us to encrypt web traffic is one of the driving forces behind the digital economy. Without this form of encryption, it is very hard to buy and sell goods online.

We've seen in recent years the technology evolve to embrace other principles. One of those principles is privacy. It is very closely connected to security in many ways.

An obvious example of this, something else you might have heard of, is the general data protection regulation and the temporary specification that has developed under ICANN and the community is now working on a more permanent solution. But that is a factor from the environment that has driven technological change. We are seeing the WHOIS protocol adapt towards the RDAP protocol. It is just a change of technologies to allow more security, more privacy, and to adapt the principles into Internet technology.

This is normal. This is part of the evolution of technology.

RDAP has been in progress for many years. It wasn't driven, per se, by GDPR on its own. It was driven by the principles of including more security and more privacy into the ecosystem. This is a natural progression.

Much of what we will be talking about today is how we, as a global community, will actually work together to adapt both the challenges and opportunities that these technological changes bring.

Often it is an effort to balance the various and sometimes competing principles on which the architecture is built.

Today there is a still openness and robustness, but there are also security and privacy and other principles that we as a community must work and strive to meet on behalf of those that use the Internet.

With that, I'll say thank you. And I'll pass it back to the moderator. Thank you very much.

[Applause]

AWA N'DIAYE: Thank you very much, Mr. Crain.

Here we have the basis of the architecture of the organization. You talked about data access. So this is the word we needed to hear. Security, of course. But how? How can we preserve security? How can we guarantee security? We need to open in order to secure.

So let's give the floor to one of our experts who will give another perspective on this, the perspective of data protection legal protection of data, protection of privacy. This is the ethical part, the unalienable rights. Mr. Enrique Factor who represents the agency for the data protection in Spain, you have the floor.

ENRIQUE FACTOR: Thank you, Madam N'Diaye. I'd like to thank the ICANN and the Spanish government and the community for participating in this forum.

Ladies and gentlemen, distinguished delegates, my name is Enrique Factor. And I work for the Jefe de Servicio de Relaciones Erupeas, the Spanish Data Protection Authority, which is the national data protection authority, which is part of the European data protection board.

My work is to protect the human rights, specifically the one stated on Article 12 of the universal declaration of human rights, which is very similar to the one stated on Article 8 of the charter of fundamental rights of the European Union and also in Article 18 of the constitution of Spain. It is the right we all have to our privacy.

We all agree that everything is data. As a matter of fact, we are data.

And the data that define us as a human being is what we call personal data.

How do we as a society protect the fundamental rights? In the real world, police and other law enforcement agencies take care of it.

But what happens in cyberspace? In the world of computers, law enforcement agencies, and data protection authorities work together in the defense of our rights.

In the European Union, privacy and data protection are not absolute rights and can be limited under certain conditions according to the European Union, which are fundamental rights. The right to privacy and data protection may need to be balanced against other European Union values, human rights or public and private interests such as fundamental rights of freedom of expression, freedom of press or freedom of information.

The right to privacy and data protection may also need to be written up against other public interests, such as national security.

European Union member states adopt measures to reduce threat but to reinforce the police cooperation in matters such as freedom, security, and justice. We do so through established mechanisms like supervision coordination groups for a specific database like Eurodac, the Schenghen Information System, the Visa Information System, and the Customs Information System, along with Europol and INTERPOL with cybercrime is not only with law enforcement control database. I reckon there are other databases like WHOIS which are of paramount importance in cybercrime, but all of them must comply with the law.

Just a final note, we'll fight for the defense of our rights. But this cannot be at the expense of transparency, fairness, and compliance with the law. Thank you.

[Applause]

AWA N'DIAYE: Thank you very much, Mr. Factor. So respect of individual freedoms, respect of human rights, respect of the law that protects individual freedom. So what you will probably tell me is that it is what we have that is most valuable. And it is the most unalienable right that we have.

But there is another perspective, which is also important. It is public safety.

How can we make sure that we are protected against cybercrime without having an impact on the protection of data? How can we face cyber delinquency? How can we improve cooperation between governments through the data protection agencies? In order to help us understand this, we have somebody who is quite qualified with 30 years of experience, head of the European Center for Cybercrime. He is in charge of a working group within the European Union that defines different strategies in that area.

Mr. Wilson, you have the floor.

STEVEN WILSON: Thank you very much, Spanish ministry. Huge pleasure to be here. My thanks to ICANN for inviting law enforcement to speak at this conference.

Can I first start with apologies? My colleague Tim Morris from INTERPOL was supposed to join us but was detained by a serious matter. I will speak for Europol and INTERPOL. I'm here to provide a high-level strategic view from law enforcement on the impact of the WHOIS on our investigations and impact we see on public safety.

Ultimately, this is public safety and public interest. And how can we make the Internet safer for all of us?

Hugely important thing I think that everybody in this room is committed to.

Firstly, in relation to EC3, my organization, we deal with the top level cybercrimes across Europe, working in excess of 200+ investigations a year. We also deal with the high-end non-cash payment fraud, major attacks on the banking systems. We deal with the top-end online child sexual exploitation inquiries not just in Europe but on a global basis and working very closely with our colleagues at INTERPOL. We have digital forensics units and darknet investigations units. But across Europol we also deal with terrorism and trafficking of human beings.

The reality is all of these investigations are affected by WHOIS. If we look at what we're talking about here -- and I thank Enrique for his comments about privacy. Data protection and privacy is at the core of what we're trying to do at law enforcement. It's a fundamental right. Get it correct and the Internet is a safer place for us all. However, we need to balance that with the rights of victims, revictimization for those child abuse victims, the serious threat to life we see on a daily basis, the

exploitation of people online. And that balance is a really difficult one to strike.

What I think is very important to indicate is that law enforcement, our interest, is targeted in relation to top-level criminals and criminal groups. It is not a bulk collection of data.

If you look at GDPR, I think it's a fantastic principle. We would be much safer if we can protect our data to the standards required by the act. However, it's created an unintended consequence for law enforcement and WHOIS and is now starting to impact significantly on law enforcement judicially and ultimately public safety. The practical effect as I've discussed is not only in relation to cybercrime but counterterrorism, serious organized crime, child abuse, high-level I.P. crime, and money laundering. The WHOIS is the starting point for most of our investigations. The idea of linking those registered domains are hugely important, identifying lengths and global investigations because the Internet has got no boundaries. It does not respect national laws, and we need to be able to work on a global basis. And, again, the WHOIS has been vital for the speed of investigations against some of the most dynamic adversities we have ever seen in law enforcement.

I will try to put this into context of some examples of operations that we run. Child abuse investigation, (saying name), an organized pedophile group, selling access to child abuse material on the Internet. We gathered all domain names connected to this group and websites through DNS. But the diverse (indiscernible) is actually fundamental to

trying to do this. Cross-matching of those datasets found mistakes made by these people. And their operational security can be very good. But, fortunately, they make mistakes and that's how we are able to catch them through the use of the likes of WHOIS.

Secondly, 21st, 26th of April this year, AMARC, the ISIS terrorist network, working with international partners, we were able to take down this entire network that was responsible for distributing extreme material, recruiting new volunteers for the organization, and, again, access to the WHOIS database was fundamental to the success of that operation and, again, the extent of how we use this Operation Avalanche from back a year ago.

Cybercrime is a service network, supplying cybercrime services on a global basis. More than 800,000 compromised domains by this group registered. We resulted in five arrests of the top-level individuals in this group. Again, this inquiry would not have been possible without access to WHOIS.

We currently have multiple investigations ongoing that have been slowed down or have been challenged by WHOIS. They're not completely killed, but we are trying to get to the bottom of this.

So, ladies and gentlemen, the future I see the idea of a unified access model as fundamental to what we're trying to do, a single user interface with accredited users. INTERPOL and EuroPOL stand together to say we will try to provide whatever service we can. The whole point is to be able to catch the bad guys.

And, again, just to reinforce, speed is of the essence for these investigations. The criminals act without rules, but we need to develop rules and laws that allow us to catch up and to keep pace with them and deliver an effective deterrent. We need to ensure that the fundamental foundations of the Internet which we all know and love are maintained. And I think it's hugely important to bring this together with access to this database with the understanding that public interest should be the prime consideration. Thank you very much.

[Applause]

AWA N'DIAYE: Thank you very much, Mr. Wilson.

I think that all governments who are here gathered, all of the governments' members of the GAC, agree that it is important to protect the private life of citizens but all are also quite preoccupied or worried by the important numbers of crimes on the ecosystem.

So how can we end this? What are the solutions that we can find? And who -- who are the stakeholders that can work on that? How can we make sure that at the level of our states we can reduce the debate by citizens that are present everywhere that make the Internet the devil because of these crimes? And, yet, we want to protect private data.

We feel that it is an intrusion into our freedoms. What are the solutions that we can find? We talked a lot ever since we started this morning about the major, which is to unite the different components of ICANN

and work around the future of the Internet. How can we build that future?

We have with us someone who is a diplomat by training who is an actor in civil society and also an entrepreneur. So he also understands technical. He co-founded The Policy Network Jurisdiction ever since 2012, so his experience is quite diverse. And this experience is what we need within ICANN so that we can work as a multistakeholder system to get to a inclusive solution.

Mr. Bertrand de La Chapelle, you now have the floor. And I think that maybe you can give us a global solution to this issue. And then we will listen to the different countries to also have their perspective to find out about their expectations and perhaps their questions.

BERTRAND DE LA CHAPELLE: It is good to see a lot of familiar faces. Just very quickly, I want to share a few bullet points. The first thing is that the three interventions before me are the perfect highlight of the challenge that we're all confronted with, which is to reconcile three objectives. One is to fight abusers. The second one is to do this while protecting and even fostering human rights and respecting due process. And the third one is at the same time making sure that the development of the digital economy goes unabated and is not being hampered.

Reconciling those three objectives is a major challenge. And I purposefully use the expression "reconciling" and not "balancing"

because "balancing" immediately gives the impression that you are sacrificing one for the other.

The second idea is that actually the WHOIS debate is a perfect illustration of this tension between the three dimensions. And it shows how difficult it is, and it's an ongoing discussion within ICANN that I'm sure within the context of the GDPR is going to find an appropriate solution.

But the third point I want to highlight is when we are talking about the DNS technical level, there is a danger of seeing it as the ultimate tool to solve a lot of things that are happening on the Internet. And we need to be cautious here and to distinguish the role that DNS operators can have in two completely different dimensions.

When we're talking about safety and stability, security and stability abuses, such as phishing, malware, bots, et cetera, it is absolutely appropriate to leverage the cooperation of the DNS operators to fight those things because it is about the infrastructure, except in a few cases.

However, on the other hand, when we are dealing with the content -- the abusive site content that is underneath, generally speaking the DNS layer is not the appropriate tool because whenever you act by removing a domain name, it has a global impact and often the harm or the illegality is only local. And so there are situations that are exceptional that need to be addressed where a domain name has appropriately been taken down because of the content underneath where a certain

threshold of abuse is being reached. I wanted to highlight those two dimensions.

And, finally, what is extremely important is -- and I used to be in the French Foreign Affairs Ministry. The exercise of sovereignty in the digital age is confronted with a certain number of new challenges because what -- the decisions that one can take at the national level can have an impact on the territory of another country. And it is extremely important that whenever legislations are being developed, the impact that those legislation can have extraterritorially at least is fully taken into account. And this requires communication, coordination, and cooperation between the different governments. But what is even more important is that, the decisions that are being taken -- and it's almost a full circle to the first point that I had. The decisions that are taken in one particular silo or even one particular international organization or even in one particular subtheme, either on economic side or the technological side or the security side, has an impact on the other challenges on the other dimensions. And finding this reconciliation I was mentioning as the first point is the underlying threat.

So to finish, this notion of enabling digital cooperation needs to be made in a few different dimensions and domains.

And the Internet Jurisdiction Policy Network that I co-founded in 2012 has three programs in that regard. One of them is directly related to the domain name space, but the two others are related to cross-border access to eEvidence and criminal investigations, which is a major

transnational challenge, as you all know. And people in the DNS community may not be all aware that the discussions about this topic are likely to impact them as well through, for instance, the eEvidence proposal from the European Commission or the Cloud Act in the U.S., a little bit like the GDPR impacted the discussion on privacy.

The other dimension that you're all familiar with is under which condition can there can be a cross-border request to take down a particular piece of content on an international platform such as Youtube, Facebook, et cetera.

And the last one is in which conditions is it appropriate to take down a domain name because of the activity on the site under this domain?

So this is what we're doing, and I'm very happy to see that the theme of digital cooperation is growing because fundamentally what is at stake is what is the digital society that we want to build together? Who cooperates to develop the norms? Who implements them? And how are they adjudicated? Thank you.

[Applause]

AWA N'DIAYE: Thank you very much, Mr. De La Chapelle. So the great challenge that we are all faced with will not be resolved without the states. So what we expect from the states that will take the floor is to bring their contribution, taking into account their critical role.

We will speak with Uganda, with Frank Tumwebaze, Minister of Information Communication Technology and National Guidance. You have the floor.

UGANDA: Distinguished delegates, we would like to thank the government of Spain and ICANN to have allowed us a few minutes to present our points from the government of Uganda, the ministry of ICT.

We welcome this opportunity according to governments under the umbrella of the high-level government meeting to have this dialogue on critical issues. While Uganda has been a member of the GAC and ICANN for the last six years, we have had cause to run for solutions to ICANN. And we commend the advocacy and public interest, but we still acknowledge that there is a lot that needs to be done.

Today, we need to consider this pertinent subject of data protection and privacy, which is of a key importance as we develop and adopt eServices in the public and the private sector. Uganda recognizes that this is a critical issue in this era of mobility of citizens, the global nation of services and different national data protection regimes.

This is further compounded by the varying degree of cybersecurity capabilities of the different countries who are members of the ICANN, as well as the frameworks that impact flow or access to information by respective government organs.

Uganda, therefore, recommends that the process of development and provisions of the policies and industry requirements that relate to the Internet ecosystem for which we all contribute should ensure the provision of public services and national security are not inhibited.

These processes and provisions should, therefore, take cognizance of the various existing and emerging public interest requirements of all countries.

And as I conclude, I wish to reiterate the country's -- Uganda's commitment to work with the different stakeholders to ensure the continued growth and inclusiveness of the Internet ecosystem for sustainable development for all. Thank you.

[Applause]

AWA N'DIAYE: Thank you very much, Uganda, for being so precise and clear and especially for being brief because I would like to remind each speaker that you only have three minutes max. So that was perfect.

Now I would like to give the floor to Pua Hunter from Cook Islands, director of ICT. Again, from Cook Islands.

PUA HUNTER: Thank you, Chair. I would like to offer the speaking slot to my fellow Pacific participant from the small country of Tuvalu, the Minister for Communications and Transport, Honorable Monise Laafai. Thank you.

MONISE LAAFAI: Greetings, distinguished chair, honorable ministers, ladies and gentlemen. My name is Monise Laafai, Minister for Communications and Transport for Tuvalu. This is my first ICANN meeting, and I'm absolutely honored to be here on behalf of my country.

Thank you, distinguished chair, moderator, and system experts for sharing with us your expertise and experiences in the Internet governance ecosystem.

First I would like to express our sincere appreciations to the gracious host, the government people of Spain, for the beautiful settings and the hospitality accorded to us since our arrival in a beautiful country.

The challenges in privacy, data protection and cybercrime is real in my small country, Tuvalu, real because we have many challenges, and as a small, tiny nation that is isolated by oceans from many regional and international business centers, we are extremely vulnerable to the effects of climate change. It is constantly for us to travel outside our country and we recognize that sea transportation is critical for our economic development. The alternative, telecommunications, is also costly. Our telecommunications sector is modest, a monopoly that supports our population of only 11,000 people. Our legislations have been amended to accommodate E-developments and support E-commerce and address cybersecurity. The capacity of our local IT experts is limited as are the responsibilities in a small administration are multi-task. For instance, our GAC representative is also CEO for the

ministry of transport and communications and takes care of a range of national priorities, both policy and technical. And he is also the adviser to me as minister.

Despite these challenges, however, we are embarking on the implementation of an undersea cable object -- cable to connect our island communities with generous funding from World Bank. I see this as an optimistic development because I believe it will promote the development and implementations of wide mechanisms to address the challenges I have already alluded to. Three minutes will not allow sufficient time to provide a holistic summary of our many challenges but I hope that my country's participation in ICANN meetings will at least narrow the digital divide or gap in Internet governance development between my country and developing countries and also foster a shared understanding of our challenges and best practice among our colleagues in GAC and ICANN.

Many of you here today know the dot domain name for Tuvalu, however, I'm not clear about how it impacts my country in terms of the hot topic of GDPR. Are there any actions required from us to undertake to ensure compliance with the GDPR. With the vast distances and tremendously high costs experienced by a small island state in a Pacific subregion to come to this ICANN meeting, I will welcome ICANN and -- and the partners in the Internet ecosystem to consider facilitating or joining subregional events and to promote the work of ICANN in the region and use the platform to gather our collective input to support

ICANN work, especially in the areas of policy development. Distinguished chair, thank you for the opportunity. Gracias.

[Applause]

AWA N'DIAYE: Thank you very much. The floor is now to the Dominican Republic, Mr. Nelson Guillen, member of the board of INDOTEL.

NELSON GUILLEN: Dominican Republic speaking. I would like to begin by thanking, on behalf of my government, the Spanish government for hosting this meeting in Barcelona. The Dominican Republic has taken the commitment to establish the adequate cybersecurity mechanisms to protect state entities, the citizens, and production sectors. And these measures will guarantee the reliable development of the activities of all the entire population in the framework of respect for human rights. However, we have seen that in order to deal with fundamentalist groups that usually use Internet for propaganda and recruitment, several governments have passed laws that seem to combat cybercrime and cyberterrorism but end up being used to suppress differences. So it is a concern for us that cybercrime and some other behaviors are used as excuses by legislators to criminalize those that criticize the legitimacy of a government or to attack or oppress the critical political thinking. We believe that chase and persecuting and incarcerating Internet users for speaking freely and legitimately is something that shouldn't be allowed. And at the same time goes

against a comprehensive solution that could help us deal with cyberterrorism in the long term. We are concerned about those laws that use the spirit of cybersecurity to prevent access to WHOIS data in order to benefit some particular interests. This translates into a clear conflict of interest that should be solved at the global level and ICANN can contribute to the solution. The Dominican Republic and its interests in contributing to the improvement of security of Internet and in support of individual rights of privacy and the Internet rejects this kind of intervention in the Internet governance system. Because the general interests should always prevail over individual interests. Thank you.

AWA N'DIAYE: Thank you very much. I would like to now give the floor to the European Commission, Mr. Pearse O'Donohue, director for future networks DG Connect. You have the floor.

PEARCE O'DONOHUE: Thank you very much, Mrs. Chair. Privacy is inevitable and perfectly understandable. And the European legislation, the GDPR that has already been referred to as a key example is a -- a move in that direction. Now, Enrique Factor has already put that legislation into context and the protection of privacy in general in relation to other public policy considerations. So I won't go into that in the interest of time because we have also hard of the very real security threats and criminality that

law enforcement agencies are dealing with. And clearly they need to have access to the necessary information in order to do their jobs.

So there is a balancing act between maintaining privacy and ensuring law enforcement and protection against cyber threats. But it is not -- and I'd like to underline what Bertrand de la Chapelle said -- it is not a question of choosing one or the other. In fact, it's a paradox. In order to be able to nurture and protect the open Internet, which is the mission that we're all committed to, as a vehicle for everyone to benefit economically and socially, in order to protect people's data and also for them to have sufficient trust in the Internet so that they will engage with it and with their data in order to fully benefit from its potential. In order to achieve all of that, we must also ensure that the Internet is safe, that it is secure, and that it is not a home for or allowed to enable criminality. And that paradox, that balancing act, is what we must deal with on an ongoing basis.

But given that it has been referred to repeatedly in the work of not just GAC but the ICANN communities over the last weeks including at this meeting, let me deal specifically with the issue in relation to its impact on WHOIS as we have heard a lot of other interesting interventions on the wider issues. And this, I can say, is the position of all of the EU member states and the European Commission. The European Union fully acknowledges ICANN's central role and responsibility for ensuring the security, stability, and resilience of the Internet domain system. And a part of -- as part of that role, ICANN should ensure the functioning of the WHOIS service, including the collection, retention, and where

necessary rendering of accurate data about individual domain names and their registrants. And that can be done in full protection of EU data protection rules and data protection rules from other regions.

We support the ongoing dialogue between ICANN and the European Data Protection Authorities who I would ask you to recall as we have a representative here as well are independent regulators and hopefully not subject to governmental influence, in order to ensure that there is respect of those rules. But we must also underline that there is nowhere in the GDPR that somehow stops the processing of data for legitimate purposes such as that of law enforcement, cybersecurity research, or in fact the detection and follow-up of breaches of intellectual property and other rights. It is simply identifying a legitimate purpose and finding that balance between those legitimate needs and the protection of individuals' data. And that is something which we think will be of great benefit to the entire ICANN and Internet governance community if we get it right. It is a hard task, but nevertheless one that will serve us well for the future in the sense of protecting one of the fundamental issues, the fundamental rights which I know all governments are committed to while also ensuring that the Internet can function to its full potential in the future. Thank you.

AWA N'DIAYE: Thank you very much. I would like to give the floor to the Indian government, Dr. Gulshan Rai, who is national cybersecurity coordinator. >>GULSHAN RAI: Thank you, madam. I take this opportunity to thank the government of Spain and ICANN for hosting

the conference and giving an opportunity to make our points there. The digital economy is growing very fast. We at India expect to reach a one trillion digital economy by 2022.

Along with the growth of the digital economy, certain issues of -- also with a different nature, are emerging. The cybercrime, cybersecurity, privacy, and free flow of information have assumed a greater importance. In the eyes on the verge of developing its privacy framework, which this was announced by the honorable minister in his video message in the morning. We already have a vibrant cybersecurity policy and cybersecurity strategy. However, the interface between the cybersecurity, privacy, and free flow of information in this technology driven era is a great challenge. Not only a challenge for India but it's a great challenge for the entire globe. We cannot have different frameworks worldwide, which are not compatible. Certain frameworks announced recently have caused certain issues and some of which has been mentioned in the interventions and by some of the experts in this panel.

The -- today 90% of the cyber crimes are of the (indiscernible) nature and 9% are of target nature. However, this figure will change as (indiscernible) happens more. Together with the comment, the industry, therefore, will have to come and play a role to combat with the issue of cybercrime and cybersecurity.

Today if you look at the world map there are specific boundaries. There are specific sovereignties there. However, when we look at the -- the appropriateness and universities they work. There is no boundaries

and they work seamlessly there. As the operators work seamlessly, this will cause a seamless connected interoperable networks of frameworks to address our issues of cybersecurity, privacy, and free flow of information. The secure networks and -- and the Internet is a paramount importance and India commits to work with the world community toward an interoperable framework which may address the emerging issues in this technology-driven era. The technologies like artificial intelligence, big data, and machine learning are playing an important role. ICANN and the -- particularly the GAC has a key role to bring the communities together involving a interoperable framework to resolve issues which are emerging very, very fast. Thank you very much for giving said time for the intervention.

[Applause]

AWA N'DIAYE: Thank you very much. I would like to give the floor to the USA with Mr. David Redl, Assistant Secretary for Communications and Information and Administrator of NTIA.

You have three minutes maximum. Thank you very much.

DAVID REDL: Thank you for this important opportunity to speak on these subjects. The united States is a strong advocate for Internet governance and policy development. Simply put, bottom-up consensus-based policies create policies that are trusted throughout the Internet ecosystem,

broad range of issues including privacy and cybersecurity and why we're a strong supporter of ICANN.

Internet governance challenges collectively before us are not easy to solve. There will be tradeoffs and hard decisions. But at NTIA our driving force is a commitment to meeting these challenges in a way that ensures prosperity and clears the way for innovation. The world has seen enormous benefits from this approach, so we must continue to give a green light to innovators to create a more secure, more open, and more prosperous Internet. This applies to the challenge of finding a way to preserve the ability of accessing WHOIS data in light of the implementation of the GDPR. As you know, the WHOIS service is an incredibly valuable tool for the legitimate and lawful purposes of law enforcement, cybersecurity, and intellectual property rights protection. These uses of WHOIS information are crucial for protecting the public interest and ensuring the stability, security, and trust in the Internet DNS.

From the U.S. perspective it is imperative that we find a path forward. And while European officials, including the Data Protection Board, have confirmed the importance of WHOIS access, ICANN took the unprecedented step of passing a temporary specification. And members of the ICANN community continue to work aggressively on this issue through the EPDP. The continued lack of clarity and shared understanding amongst ICANN stakeholders of where the bright lines of GDPR compliance and non-compliance are continues to frustrate the process.

This introduces risk for those companies involved in the provisioning DNS service. With risk profiles highly variable among parties, finding a solution that can mitigate all individual company risk is daunting.

This is why the United States strongly supports ICANN org direct engagement with our European colleagues, including the European Data Protection Board, to see if there is a way to simplify our shared challenge by having ICANN org assume the risk and responsibility for WHOIS access under the GDPR unified access model. This would simplify the problem. Time is marching quickly toward the expiration of the temporary specification.

I urge the GAC to play an active and constructive leadership role in the community discussion of a unified access model. The United States stands ready to work with colleagues in the GAC and the broader ICANN community on this issue. Thank you.

AWA N'DIAYE: Thank you very much. I would like to give the floor to Malaysia, Dr. Mohd Ali Mohammad, Secretary General for the Ministry of Communication and Media.

MOHD ALI MOHAMMAD: I will be very brief.

Given the current development and changes in technology, law enforcement agencies, in Malaysia especially, are facing numerous new challenges when combating crimes in the era. Criminals are get being

more sophisticated while conventional method of investigation may no longer be as effective as before.

To meet these challenges, law enforcement agencies may use and utilize every information available that will assist in the investigation process, including WHOIS information. Law enforcement agencies through legally provided channels also enlist the assistance of domain names manager for provision of information relating to investigations.

For that reason, the role of domain name system community and WHOIS are crucial and should be retained in view of investigative and law enforcement needs. Thank you for the floor.

AWA N'DIAYE: Thank you very much for being brief. I'd like to use the few minutes that we have left to give the floor to John Crain. We talked about domain names and WHOIS quite a bit, and maybe he can give us a little bit of supplemental information on that. Thank you.

JOHN CRAIN: Sorry.

If I may, I've heard a lot of talk about the WHOIS and how important the WHOIS database is. And I wanted to clarify for those who didn't go to the technical session yesterday that, when we talk about WHOIS or indeed when we talk about RDAP, which will be the replacement of WHOIS, these are actually decentralized systems. So there is not one

database, but there are many databases in many locations around the world. That's an important element to bring into mind.

I think it's excellent that we can have these discussions here at ICANN, that we can bring the various parties together and discuss how we find solutions that balance all of those principles, including security, privacy, and robustness of the network.

With that, I'll pass it back to the chair lady. Thank you.

AWA N'DIAYE: Thank you very much, Mr. Crain.

I would like to give the floor to Mexico with Mr. Victor Lagunes Soto Ruiz, who is head of the unit of Innovation and Technological Strategy of the Office of the Presidency of the Republic.

VICTOR LAGUNES SOTO RUIZ: Mexico speaking. Thank you very much to the Spanish government and to ICANN for their continuous cooperation in Internet governance issues.

The role of Mexico regarding digitization has been great, but has been having a strategy of connectivity.

And while we continue connecting more and more Mexicans and breaching the digital divide, we are concerned regarding digital threats and privacy.

We have a national strategy regarding cybersecurity in collaboration with the whole ecosystem in a multistakeholder environment. Last year we were able to publish data strategy in cooperation not only with the industry and the technical sector, the academia and the social sectors, but also with observers and international experts in cooperation with United Nations, UNESCO, the OAS, and in data strategy, it -- the strategy will help us protect citizens, to protect the rights, our economy, the innovative economy of public entities, public security. Because we are raising awareness. We are having programs to that effect. We are strengthening cybersecurity culture, in coordination with the environment, cooperation with the environment, research and development, setting some technical standards, and protecting some critical structures, legal frameworks -- strengthening of legal frameworks. All these to set guidelines to strengthen a sustainable development on the Internet.

I'm very proud to say -- to share with you that the WSIS, the World Society of Information Society, has named this platform as a champion last year. Thank you very much.

[Applause]

AWA N'DIAYE: Thank you very much. I would like to give the floor to Brazil. Ambassador Benedicto Fonseca Filho, who is Director of the Department for Science and Technology.

BENEDICTO FONSECA FILHO: I'd like to very briefly refer to the importance that Brazil attaches to the discussion on the nexus between cybercrime, data protection, privacy. This is a matter of priority concern for us.

Brazil has adopted just last August a new legislation on data protection that is largely inspired, I would say, by GDPR. This legislation should enter into force in February 2020. We are also discussing and deliberating a national cybersecurity strategy. And, as you all know, of course, at the global level, we have been very strong advocates for the right to privacy in the digital age. We have been sponsoring resolutions together with Germany for promoting these resolutions in the context of the United Nations. And also we are looking to ways to put in place instruments to develop to fight cybercrime.

This is to illustrate and I would refer to a notion that was mentioned Bertrand de la Chapelle, the coordination, cooperation among governments within the international community to address those issues and the in-depth context -- and I also revert to Bertrand, that has initially brought attention to the fact that the debate around WHOIS illustrates the true dimensions we want to achieve -- fight, abuse, protect human rights and not undermine development and views of new digital technologies.

In that context, I'd like also to second the -- and highlight importance of the Internet and jurisdiction network which provides platform for discussion on those issues because we do not have a place internationally to address the jurisdiction elements of all those

discussions in one place. And we think this project provides a very important place for that.

And we would be looking forward, of course, to be fully engaged in the discussions on the WHOIS debate in the ICANN context as we concur with the fact that we might -- we must find the right balance in addressing concerns related to privacy on the one hand and security on the other. Having heard the representative of INTERPOL and having heard our Brazilian colleagues that also deal with this, we feel that it is in our very clear interest to -- and I revert again to the idea of trying to reconcile those different dimensions in a way that is appropriate. Thank you.

[Applause]

AWA N'DIAYE: Thank you very much. I would like to give the floor to Samoa, Honorable Afamasaga Lepuiaí Rico Tupaí who is the Minister of Communications and Information Technology.

AFAMASAGA LEPUIAÍ RICO TUPAÍ: Madam Moderator, I regret I will give this session a pass, but wish to record my intention to have my intervention in session 4 later on. Thank you.

AWA N'DIAYE: Yes, of course.

I would like to give the floor to Switzerland, Niklas Nilsson, who is the First Secretary to the Embassy of Switzerland in Spain.

NIKLAS NILSSON: Thank you. I'd like to inform that we talk on behalf of Sweden, not Switzerland.

Anyway, thank you for this opportunity to briefly put forward the Swedish perspective on human rights online and Internet freedom.

We take a human rights based approach to cybersecurity and to ICT in general.

To state what has now been firmly established and confirmed as a fundamental principle human rights apply online as well as offline. Human rights, democracy, and the rule of law must be respected and secured by states and guide the global debate on standards for cyberspace. However, respect for human rights on the Internet is in decline worldwide. In the last years, more governments have censored more public information on public interest. State authorities have jailed more users for their online writing, and cyber surveillance power has increased. There's been more repressive legislation, violence, and the spread of state-controlled propaganda and disinformation. Such measures limit and restrict the participation of citizens in society undermining the foundation of democracy.

This trend can and must be seen in the context on the global trend of a shrinking democratic space. The increasing amount of repressive

legislation and regulation not only limits freedom of expression but also individuals' opportunities to participate in the life of society and to influence decision making. Ladies and gentlemen, thanks to the Internet and social media, human rights are more widely known worldwide than ever before.

The positive role that ICT plays in our lives, our democracy, and our economy must also be highlighted. And this positive narrative of the Internet must be maintained.

The Internet has great potential to promote economic development as well as to create an enabling environment for democratic, inclusive, and diverse societies. The capacity to bring people and politicians closer to one another must not be weakened. But by limiting Internet freedom we are limiting our own development. That is why we argue that a rights-based element in all discussions concerning the opportunities and challenges open by a digitalization is essential if more people are to be able to have access to a free, open, and safe Internet.

And, with this, I finish.

A multistakeholder model with actors from government to industry to civil society including human rights defenders, is an absolute key when developing the framework, content and common standards of the Internet.

So let me repeat Sweden's ambition of an Internet that is open, free, and secure with equal access and inclusiveness for all. Thank you.

[Applause]

AWA N'DIAYE: Thank you very much. I would like to give the floor to the Netherlands, if I'm not mistaken. Mr. Geert Moelker, member of the Management Board for Digital Economy, Ministry of Economic Affairs and Climate Policy.

GEERT MOELKER: I will try to be brief. I'd like to stick to two points regarding WHOIS. A lot has been said about balancing or reconciling the different fundamental rights and privacy but also the right to be protected against crime.

And we agreed it is not a tradeoff. It is a balancing act which we should try to resolve.

And what I'd like to stress is if there's one organization where this can be done, it can be ICANN with its many stakeholders. So that is a very big task ahead of us but we are in a unique position to do so.

And then the second point, that's about the urgency. We are facing an urgent need to come up with modalities to the access data of the WHOIS. Since May 2018, many registries have modified their WHOIS access. They have done this on their own terms without real coordination, and if we do not come up with a harmonized model, the fragmentation will only get worse. Law enforcement will continue to overcome huge hurdles in their investigations while users will not have

certainty about how their personal data are being kept safe. And here again, we see the pivotal role of ICANN and its multistakeholder nature. ICANN is the only organization that on a global scale can provide uniform approach to provide this.

The WHOIS reform cannot be left unsolved and the stakes are too high. We need a timely solution. It clearly transcends the traditional policy process we know from domain names coming from one constituency. It requires action from more stakeholders, from the ICANN Board, the organization itself, and other stakeholders in and outside ICANN. And we strongly support the multistakeholder model, but it is also my opinion that this WHOIS debate is also a new test case for this model after the IANA transition, and let's make sure we pass this test soon.

Thank you.

[Applause]

AWA N'DIAYE: Thank you very much.

I would like to give the floor to our last speaker, Italy, for three minutes as well. Mrs. Rita Forsi who is the Director General of the Superior Institute for Communications and Information Technology.

RITA FORSI: Distinguished delegates, ladies and gentlemen, first of all, I would like to thank the government of Spain for hosting this High-Level

Governmental Meeting. We all know that the WHOIS, the public available address book in which the personal data of the owners of domain names is published, is no longer accessible.

The WHOIS data are used for several purposes, including important public-policy aims such as those related to law enforcement activity, cybersecurity initiatives, intellectual property rights protection mechanisms and consumer safety actions, the so-called domain name environment.

Italy supports the work at each level done until now to develop and implement permanent solutions, but at the same time would like to stress the need to accelerate the investigation of the global model, the unified access model, that could be considered acceptable by the involved parties.

Finally, global solution for a balance between the various interests and the stakeholders' rights is close to be an unreachable goal. The key driver for success is and will remain enhanced and the structured cooperation among all the involved parties of the Domain Name System community. At the same time, all the DNS community must acknowledge that acting fast is crucial when dealing with the Internet governance issues. To achieve that, Italy believes that the ongoing dialogue between ICANN and the EU data protection regulation authorities is essential. The real challenge we all are facing is to protect, at the same time, all the aspects of the issue here highlighted regarding the stakeholder of Internet.

Thank you.

[Applause]

AWA N'DIAYE: Thank you very much.

Well, here we are at the end of this debate with the different states. What we can see is that we don't have two opposing topics but they need to be taken together. It is something that is necessary. We needed to hear those principle -- those fundamental principles of human rights; also the necessity for all stakeholders in cybersecurity to talk together, to cooperate.

And before I close this session, this panel, I would like to go back to Mr. De La Chapelle and ask him to tell us again how important it is to find a global solution, a multistakeholder solution.

Mr. De La Chapelle, you have one minute.

BERTRAND DE LA CHAPELLE: Really less. I don't want to disappoint, but it's less about about a global solution than identifying problems on an issue-by-issue basis.

I was very closely listening to what was -- what was said. On the whole WHOIS debate, there's a close connection with what was discussed in the first panel, which is how does the interaction between governments and the rest of the community takes place within ICANN and how much

the governments participating in the GAC are also conveying what is discussed in their own processes. That's important.

And the second idea that I want to highlight is that in as much as ICANN is an extremely important space, it has a limited mandate, and there's a danger that because this community is there, everything that is related to the Internet has a tendency to fall within this community. So it's important to identify where the topics are being handled on an issue-by-issue basis in something that is related to policy innovation, because some topics do not belong in ICANN and it's extremely important to create as many opportunities outside for the issues that are emerging for this communication, cooperation, and coordination among the different actors.

So there's not one single global solution, but there's probably a global approach of policy innovation allowing initiatives to pick on a topic and bring the different actors together. That's what we're doing at our small scale, but there are others that are doing similar things.

AWA N'DIAYE: Thank you very much, Mr. De la Chapelle.

To conclude, I would like to give the floor again to Mr. President. I would like to remind you how important all of this is. We need to reinforce cooperation between the different stakeholders. The multistakeholder cooperation will be essential in order to get to a solution, even if that solution is complex, as you all mentioned.

Another important fact that I would like to remind you of that we talked about is we need to harmonize our laws to get to that solution. So what does that mean? The laws, the national laws, should not work against each other and should not be an opportunity to deviate against freedom of expression on the Internet. So really harmonize our laws so that the Internet can be trusted. The Internet can benefit to all to their full potential.

Thank you very much. I would like to give the floor to Mr. President.

FRANCISCO POLO: Thank you very much, Mrs. N'Diaye. This was an excellent session. Thank you very much for moderating held for the session. (Indiscernible) because we had also for this session.

This is the last one in the morning. We will be back at 3:00 p.m. for two more sessions.

Thank you very much.

[Applause]

MANAL ISMAIL: So thank you, Mr. Chairman. And thank you for the moderator, subject-matter experts, and discussants, and special thanks to the delegations for the participation.

So as Mr. Francisco mentioned, this is the lunch break. For head of delegations with the orange round sticker, please, lunch is served at the

banquet hall. Please take the escalators just in front of the room upstairs and follow the signs and you will be guided by ICANN staff. And for everyone else, please enjoy your lunch, and kindly make sure to be back in the room at 3:00.

Thank you.

[END OF TRANSCRIPTION]