ICANN74 | Policy Forum – NextGen Presentations (1 of 2)
Tuesday, June 14, 2022 – 13:15 to 14:30 AMS

DEBORAH ESCALERA: Hello and welcome to the NextGen at ICANN presentation. My name is Deborah Escalera, and I am the remote participation manager for this session.

Please note that this session is being recorded and is governed by the ICANN expected standards of behavior. During this session, questions or comments submitted in the chat will only be read aloud if put in the proper form as I've noted in the chat. I will read questions and comments aloud during the time set by the chair or moderator of this session.

Interpretation for this session will include English, Spanish, French, and Russian. Click the interpretation icon in the Zoom and select the language you will listen to during this session.

If you wish to speak, please raise your hand in the Zoom room and once the session facilitator calls upon your name, kindly unmute your microphone and take the floor. Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and language you will speak if speaking a language other than English. When

speaking be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

With that, I would like to welcome you to this session and thank our NextGen at ICANN participants for their hard work in preparing their presentations. I would also like to thank my mentors, Sophie Hey, Dessalegn Yehuala, and Roberto Gaetano who have been working with the students over the past several weeks and guiding them through the ICANN meeting process. I would also like to thank my colleague Betsy Andrews who will be running the slides today. With that, I will the hand the floor over to our first presenter, Joel Christoph. Joel, the floor is yours.

JOEL CHRISTOPH: Thank you very much. Good day, everyone, and thank you to everyone present both online and in person. I will be presenting Charting the Growth of the Internet in 2022 which is a project that documents the demographic and economic knowledge we have from different sources and what they tell us. Next slide, please.

Before beginning, I'd like everyone to consider for a moment, what proportion of the population in low-income country do you think uses the Internet? Low-income being defined as living on approximately €2.7 or less per day.

The second question is, in low-income countries how many mobile cellular subscriptions do you think there are per 100 people? Do you think it's closer to 25, 50, 75, or perhaps something different?

And finally, how many secure Internet servers would you think there are per 1,000 people in North America? This is perhaps a little bit more difficult to estimate in terms of the definition, but these are some questions which I hope you'll be able to answer at the end of this presentation. Next slide, please.

In the past decades we've seen changes in terms of what a lot of people are researching and publishing about. And one thing is that we've seen a very stark growth in dimensions of the Internet since the '90s and also more recently in social media and Facebook as opposed to, for a baseline, I've shown the frequency of the word "censorship" in the corpus of literature published in English.

So the point of this slide is to show that we have a growth in the interest in many of these topics which really is quite persistent. And it indicates that the scholarship on such issues is going to continue to be quite important and to become part of the body of literature that we have to deal with. Next slide, please.

Moving to the main part of the matter, here's a graph that shows the proportion of individuals by region that are using the Internet. Unfortunately, the legend on the right has come out a little bit

distorted. But the main point is that we do see a steady increase in many different regions in the number of individuals that are using the Internet. And there's particular accelerations in different points in time.

So for example, in the past few years notably in South Asia there has been relatively faster increase. And there's also been convergence toward 90% in some of the most high-income regions where the top two in blue and red represent North America followed by Europe and Central Asia.

Importantly, I've included in brown the low-income group which corresponds to the countries by the lowest income category as defined by the World Bank. And here it's, again, the people that would live on average on €2.7 or less every day. And even in this group we are seeing almost one in five people accessing the Internet. So that's a sign that as the diffusion of different technologies to access the Internet is increasing so is the access in some of the lowest income regions of the world. Next slide, please.

To compare this to the absolute numbers, we see that while there had been relatively early start in the usage in the United States shown in green, over the past decade we have seen a notable increase in the number of Internet users in China and in India. And given their relatively larger populations, this is something that is going to continue to be reflected in a lot of the usage. And also

thereafter, the number of ideas originating from different regions of the world.

Now the lower portion of this figure is quite crowded, but it represents the other 10 countries that form the top 13 countries with the largest number of Internet users. So examples are Brazil, India, Russian Federation. Next slide, please.

Now to compare the number of users to the number of mobile cellular subscriptions we had a bit of a better idea of what might be a proxy through which different people are going to be accessing the Internet. So this is data that's provided through the World Bank based on the International Telecommunication Union. And we see that in many regions such as North America, Europe, and Central Asia we have far more mobile cellular subscriptions than people. And here again, the nongeographic but economically defined grouping of low-income is also seeing at least one mobile cellular subscription among two people. Which points to the direction that the access through mobile networks is going to continue to broaden around the world. Next slide, please.

If we compare this to the fixed broadband which might be considered a different means of accessing and communicating, we see that there's a less marked increase. Especially in the past few decades, we're not seeing neither on the Y axis does it go to 120 nor do we see a fast convergence in different regions,

especially in South Asia, Sub-Saharan Africa, and the economic category defined as low-income.

The interesting aspect might be that even among the highest income regions, so perhaps North America under consideration, there's a pretty clear case of stalling below the 50% threshold. Next slide, please.

Now if we move to the number of secure Internet servers per million people, so this is defined as the number of distinct publicly trusted TSL/SSL certificates using encryption technology, there is a huge difference compared to the previous slides across the regions because in North America which in this case is primarily the United States and Canada there is a very large number per person followed by Europe. Whereas, in most other regions such distinct certificates are not yet very frequent. Next slide, please.

And if we consider a step back and think about the usage of the Internet as a share of population correlated with the GDP per capita, there is a suggestion of a positive relationship in that in higher income per capita countries more users are going to be using the Internet. But as we see in the top and right part of the graph, there is a saturation point around 6,000 current international dollars per capital. So corresponding to roughly the income levels of Norway, Bahrain, the United States, or Switzerland where beyond such an income level there's no longer

any increase because the saturation of access to the Internet has been achieved. Next slide, please.

In a final slide I wanted to also take a step back and consider when we are trying to chart this expansion across space and time it also represents the difference in the intensive use and not only the extensive use of access to the Internet.

So this is based on survey data in the United States where when people were asked about the daily hours that they engaged with digital media, since 2008 there have been new devices and technologies that have been developed but notably the introduction of mobile devices has not led to a pure substitution but rather an addition in the time that people are spending engaging with such media.

And this suggests that as different technologies are going to be developed and different ways to access, it won't be a purely substitutive phenomenon but instead more time in our lives broadly speaking we'll be connected digitally.

And with that, I'd like to bring my part of this session to an end. I thank you very much, and I pass the floor back to Deborah. Thank you.

DEBORAH ESCALERA: Thank you, Joel. Are there any questions for Joel? Let's check the online participants. Okay, thank you very much for your

presentation. Very well presented. Okay, we're going to go on to our next presenter, Mirabella Knoben. Mirabella, the floor is yours.

MIRABELLA KNOBEN: Thank you very much. Hello to everyone. Thank you for attending the session. Today I would like to present my seminar paper's topic that I wrote last summer. It's similar to bachelor thesis. I was in a seminar about the Digital Services Act that I will also explain in a few. And my topic was the regulation of content through algorithms and especially what principles are necessary to respect human rights in the digital sphere. Next slide, please. Yeah, thank you.

So about the Digital Services Act. As we all know, Facebook, Instagram, Google, WhatsApp, etc., are just some of the big online platforms that we are confronted with on a daily basis. And as I'm sure we've all experienced, they play a huge role in influencing our opinions and providing us with information. And in order to update the now outdated regulations of the e-commerce Directive from 2000, the European Commission published a draft on the so-called Digital Services Act in December 2020.

It basically sets out stricter rules for so-called VLOPS which is the abbreviation for very large online platforms. And quite recently at the end of April there was a political agreement on the DSA by the European Commission, the Council, and the Parliament. And as it

is a regulation and not a directive, after the adoption the DSA will be directly applicable throughout the whole European Union and will apply at the latest from 1 January 2024. Next slide, please.

So what exactly are algorithms or recommendation systems in the sense of the Digital Services Act? They are defined in Article 2, Letter O of the DSA. And the definition is that they are fully or partially automated systems that suggest specific content to the user on the user interface. So in a technical sense, digital platforms can be seen as recommendations systems because users of such platforms are shown customized content on a daily basis prioritized in comparison to other content. Next slide, please.

So now about the heart of my seminar paper, my presentation, which interferences are possible with human rights? And I focused both on the freedom of information and the freedom of speech that are both stated in the Charter for Fundamental Rights.

Firstly about the freedom of information, because social media platforms are made to satisfy the user as, again, I'm sure we all know they are made to make us as an individual come back to see content that you either agree with or you already know. That obviously can lead to one-sided reporting and to the so-called filter bubble effect. Because if you only see content that you just like because you already agree with it, it can be pretty one-sided.

And based on that, the freedom of speech can also be endangered because individuals form their opinions based on the information that they are provided with. And if the information they are provided with is created algorithmically, which means that there is no human control behind it, the formation of the opinions can be influenced as well. So the freedom of speech is in danger as well by algorithm. Next slide, please.

So the question now is, which principles are necessary to prevent these kinds of interferences? I focused on two possible principles in my seminar paper. Firstly, on systems based on the so-called participatory design which is pretty self-explicable word I would say because it basically means that the systems that are based on the participatory design include more human participation and thus represent more people's values. And the goal of all of this is to create morally defensible algorithms that incorporate society's overall values.

And as I'm sure we've all heard, especially in the last days at least once, about the ICANN multistakeholder model which I know is an ICANN internal model. But still, I thought that the basic idea of it could be implemented as well by social media platforms. And the main goal of the model is to make the voices of all stakeholders, so all interest groups heard in the same way. And therefore it emphasizes decentralized control and inclusive and participatory processes.

Given the size of very large online platforms such as Instagram or Facebook, this model is pretty difficult to implement. But as I said, I think the basic idea of making every interest group's interests heard can be a good way to ensure more transparency and a more participatory online atmosphere. And talking of transparency, next slide, please.

Because in the Digital Services Act in Article 29 there are two demands stated, and firstly it is the demand of more transparency which basically means that the very large online platforms are obligated to disclose their most important parameters so that the users know which parameters they are dealing with considering recommendations systems.

Secondly, the so-called opt-out possibility which means, explained in an easy way, that when you open your Instagram application or Facebook application you're presented firstly a possibility with recommendation systems and secondly a possibility without. The concrete implementation of this is still unclear, but I think it can be very similar to what we are dealing with on a daily basis at the moment when we open a website and are consenting to cookies being used.

The intention is to prevent especially the interferences with freedom of speech and other fundamental rights and can also lead to more trust of the users toward the online platform which can be useful for the platform itself.

And to conclude, before the main features of the actual implementation are clear, I think firstly it's necessary to draw attention to the fundamental rights concerns to ensure greater sensitivity for the topic in general. And because the Internet is borderless and even though the Digital Services Act is a European regulation, I'm convinced that an international solution is necessary. Because as we all know, the Internet doesn't stop at the borders of the EU. And that I think is the only way to ensure a secure and attractive online world in the long term. Thank you.

DEBORAH ESCALERA: Thank you, Mirabella. Are there questions for Mirabella? Let's see. Online participants? Okay, thank you so much for your presentation. We will now go on to our next presenter, Jan Batzner. Jan, the floor is yours.

JAN BATZNER: Hello, altogether. Thank you so much for this opportunity. The security of the Internet is a goal that we all share. So let's speak about cyber incidents today. Next slide, please.

A cyber incident is a adverse security event resulting in the loss of confidentiality and integrity as defined by ICANN. An example could be a denial of service attack where the attacker is making a machine inaccessible to its intended users. Or maybe more relevant, a spoofing attack. So pretending to be someone else. To

give you an example, Instagram.xyz to phish a user's information that is inserted here. One slide back, please. All right, thank you.

What I want to do today is I want to evaluate prevalent designs of public cyber incident data sources. I want to look with you today in data sources and databases that actually publicly share these cyber incidents, how they share it, and how can we evaluate it. What you see here is a network graph that I created. You see here cyber incidents grouped by nations, how they were affected. Every point is a nation and the color scheme is showing the intensity of the conflict. Next slide, please.

There are differences in these data sources. The ICANN Cybersecurity Incident Log, for example, is recording all cybersecurity incidents that are happening in the ICANN space and on the ICANN products. Just to define, a security vulnerability is a weakness in a product that allows the hacker to compromise. So whatever happens in an ICANN products is recorded here.

All the datasets below are coming from the public policy space. So these ones share publicly all kinds of political cyber incidents that are relevant. And what I want to do today is I want to look at those datasets and how they have been evaluated and ask what we can learn from them and can we make any conclusions. Next slide, please.

This is how the ICANN Cybersecurity Incident Log looks like. There's the date, the issue or the incident, the status, and the

information that is as one text block on the very right. To give you an idea, right now all the status of every listed incident is closed. Next slide, please.

Now we'll have a look at the public policy approaches. What we want to see if we look at these datasets is all lines completely overlapping and completely showing the same because the intention is that they should measure exactly the same.

We see something different. In green we see a collection by Heidelberg University. In yellow we see the Council of Foreign Relations tracker by the Council of Foreign Relations. In blue we see the Dyadic Conflict Incident Dataset by Valeriano and Maness. All show a different amount of datasets at different points of time which shows us that there's a very different methodology behind the collection of all of those. The most inclusive one is the green line, the one of Heidelberg University. Next slide, please.

So let's continue with one of Heidelberg University and just ask a political science question. If we can group them according to countries, we can look at the in-degree, how many cyber incidents are getting toward that country. We can look at the out-degree, how many cyber incidents are originated in that country. And following that, we can look at the reciprocity. So if a country is getting a cybersecurity incident toward them, do they point also one back?

This graph shows the top ten most conflicting countries. And even among those, the reciprocity is low. A perfect reciprocity would be 1. No reciprocity is 0. And even the most conflicting ones are maximum around 0.5. Next slide, please.

Another try to see how much can we quantify this information. Here I'm looking at the regimes measured by the Freedom House Score and different characteristics of cyber incident conflict. On the left side we can see the relationship between out-degree and the Freedom House Score. And on the right side the relationship between reciprocity and the Freedom House Score. We cannot make any clear conclusions from that. We don't see any of these relationships. Next slide, please.

One of the reasons is that there's a small number of relevant conflicting states which highly bias such political science approaches. There is a lot written on that and there are a lot of approaches that try to quantify, but the point I want to make is these approaches can be very dangerous or misleading because what is here marked in red are the countries that are actually relevant that we actually want to look at. Next slide, please.

So let me conclude. There are three main things that I can take out. First, the goal of all these approaches is transparency. And transparency is majorly achieved with things like these incident logs, the cooperation of different stakeholders, and the sensitivity for methodological questions. As we saw in the graph

earlier that the methodology highly impacts the answers that we can give to exactly the same research question. Thank you very much.

DEBORAH ESCALERA: Thank you, Jan. Are there any questions for Jan? Check the online participants. Okay, thank you very much for your presentation. We are going to move on to our next presenter, Nadezhda Arteeva. Nadezhda, the floor is yours.

NADEZHDA ARTEEVA: Hello, everyone. It's a pleasure to be here with you today. Let me begin my presentation about the DNS abuse in the EU. Why it happens and how it can be tackled.

The main problem with the definition of the DNS abuse is that the new types of abuse are commonly created and their frequency waxes and wanes over time. Which was noted by ICANN SSAC committee in 2021. But there is a definition that's adopted by ICANN and contracted parties, and it's quite straightforward. According to ICANN, DNS abuse is malware, botnets, pharming, phishing, and spam where it's a vehicle for [proceeding harms].

Why do we need to define DNS abuse? It is because most registrars and registries want a narrow definition of technical harms that they can understand and have the capability to

address and which also limits the impacts of an imprecise and often disproportionate approach.

So in 2022, the European Commission kickstarted the year with a set of publications of relevance for ccTLDs such as the DNS abuse study and the communication on an EU strategy on standardization. And I will refer to the DNS abuse study a few times in my presentation as, in my opinion, it's one of the most [inaudible] documents for the EU DNS abuse strategy [combatting].

According to the European Commission the DNS abuse intends to assess the scope, impacts, and magnitude of DNS abuse as well as to provide input for possible policy measures on the basis of [inaudible] gaps. And it defines DNS abuse as any activity that makes the use of domain names or the DNS protocol to carry out harmful or illegal activity. Next slide, please.

So let's talk a bit about the evolution of the DNS abuse issue not only in the EU but just in the ICANN community in general. Some contractual provisions governing DNS abuse originally came from policy work done by the ICANN community in 2009 and 2010 through the Registration Abuse Prevention Working Group. They managed to give the DNS abuse definition that I previously cited and outlined the main points of ICANN strategy that was developed further.

More than six years ago, in SAC077 the SSAC wrote about ICANN's proposed marketplace health index which was one of the first attempts to tackle the issue of DNS abuse. You can see the quotes on the slides. They offered to implement some auditing activity including mandating future disclosure of aspects of registry and registrar operations and behavior in a form that emphasizes consumer protection over industry norms.

According to some parties, not much has been done in the following years, or not enough has been done. And this problem has especially become critical during COVID because by most measures the volume of new domain registrations that includes the words "coronavirus" or "COVID" have closely tracked the spread of the deadly virus in 2020.

So around that time, there was the [COVID] Cyber Threat Coalition formed which was a group of several [inaudible] security experts, and they published data that shows there was a rapid increase in the domains in the last week of February. And around the same time, the Center for Disease Control began publicly warning that a severe global pandemic was probably inevitable.

So initially, ICANN encouraged registrars in February to be more proactive. However, no specific mechanisms were advised. However, the DNS abuse related to COVID drew the government's attention. For example, some [inaudible] sent a public letter to

domain name company leaders. And in general, it received some attention from the governments because of the harmful consequences for the fight with the pandemic it implied.

And so later in May 2020, ICANN enhanced measures to [inaudible] the problem, and a detailed algorithm was developed and shared with the public [inaudible] that outlined the strategy that registries and registrars have to adopt to define the malicious domain names. Okay, next slide, please.

However, let's now talk about why DNS abuse happens and what are the prerequisite, the environments that let it happen. There was a study in 2021 that was later cited and confirmed in the EU DNS abuse report that I previously mentioned. This study confirms that one of the main reasons why DNS abuse happens is the lack of contact data due to GDPR regulation.

As we know, the European Union's General Data Protection Regulation adopted in May 2018 restricted the publication of personally identifiable data in WHOIS. So in response, the ICANN established a new policy allowing registrars and registry operators to redact or withhold personally identifiable data from publication in WHOIS. As some studies claim, it resulted in consequences such as 85% of gTLD domain registrants can no longer be identified and other figures that you can see on this slide.

Another problem that's related to DNS abuse is the long lifetime of a DNS abuse report. Some recent studies suggest that the average lifetime is 32 days. Of course, it's quite debatable, and many registrars claim to deal with the DNS abuse reports within 10 days or even fewer days. But depending on the case, this period of time might vary. And for some registrars it might be particularly long.

And another problem that prevents us from fighting and combatting DNS abuse is the lack of knowledge about DNS abuse and the lack of knowledge regarding the required actions if it is encountered. Next slide, please.

So how can DNS abuse be tackled in the EU? The report also outlines a few steps, a few measures that can be undertaken according to the authors in the EU to tackle this issue.

First of all, we have a recommendation to select providers with more validation standards for domain registrations. The report suggests that we need to hold domain registrars to higher standards, and they need to take a customer validation approach that verifies who the customer is to ensure DNS abuse is not happening.

Another point is initiate prevention and remediation solutions. Free hosting and subdomains, as the report suggests, are services that were originally intended for legitimate services. However, now they are commonly exploited in phishing attacks.

Companies should activate proactive detection of suspicious domain names containing targeted brand keywords according to the report.

Another step proposed by the authors is increase adoption of controls. Domain name system security extensions can often [authenticate] communication between DNS servers. However, low adoption and lack of deployment can lead to hackers taking control of an Internet browsing session and redirecting users to deceptive websites. So the authors suggest that DMARC protocol should be continually adopted as the first line of defense against business email compromise.

And the last point is better standards for top-level domains. A TLD is the final component of a domain name, as we know. And unfortunately, the generic TLDs are the most abused domains by volume. However, some new gTLDs and ccTLDs, they have a particularly high concentration of fraud because nowadays it's quite easy to get a TLD for less than a dollar and phishers love this easy accessibility. So the report suggests that there should be some measures taken regarding this problem.

Thank you. I'll be happy to answer any questions if you have those.

DEBORAH ESCALERA: Thank you, Nadezhda. Are there any questions? It looks like we have a question in the audience. Do you want to come to the microphone? Thank you.

[DAVID:] Hi, I'm David [inaudible], ICANN something. Hi. Thank you for your presentation. Thank you all. I'm curious as to whether or not what you're asking for is for ICANN to do more than it's already doing. Given how hard and contentious this issue is of data privacy and the various directives that may be coming out of EU policy, including for example the NIS2 I think is what it was called [and your NIS2 directive.

And maybe you could speak a little bit about what actually it is that you want ICANN to do at this moment, if you had your way. Like if you could sit down with Göran and say this is what I think you need to do in order to cut down on DNS abuse, what would you ask him to do and how likely it is that you think that will happen?

NADEZHDA ARTEEVA: Okay, so thank you for your question. I think the point about ICANN in the critique, I think it was mostly addressing this particular situation with COVID. So I think it's just that when crisis happens, and they quite often happen, I think maybe in these situations there should be more rapid reaction. Because of

course, with the DNS abuse during the pandemic just the consequences of this DNS abuse were quite horrifying because they could potentially cost human lives. And of course, this can, for example, lead to people getting access to false information and to other negative outcomes. So to me this critique point that was offered against ICANN by some authors in my opinion it was just addressing mainly the way that ICANN deals with a crisis.

DEBORAH ESCALERA: Okay, thank you. It looks like we have an online question from David [inaudible]. Oh, that was you. Okay, thank you. Okay, thank you, David. Okay, let's see. Do you want to come to the microphone, please? Thank you.

UNIDENTIFIED MALE: Thank you. [inaudible] some information of most abused gTLD extensions. You mentioned that mostly those are new ones. And what about the free ones as we know that there are some older ones, ccTLDs that offer free domain names. Did you answer the question?

DEBORAH ESCALERA: Can you repeat that? We couldn't hear you very well.

UNIDENTIFIED MALE: Yes. Have you got the data of those gTLDs that are mostly involved in the DNS abuse processes?

NADEZHDA ARTEEVA: So of course, in the reports…thank you for your question. In the reports it was presented in a brief form, so there were no examples. If needed, I think we can look them up. Yeah, I can.

UNIDENTIFIED MALE: Yes, just in your…it was really interesting listening, and you did specifically mention that this problem is especially with new gTLDs. So I would suspect .xyz is one of them. Well, why not call out the names? And maybe you could base your report on some data. And if you could share a little bit more of that data, please. And that's it. If not, that's fine.

NADEZHDA ARTEEVA: So if needed, basically the report I cited was the EU report on DNS abuse. So if needed, I can just probably share the link with you or send the PDF documents and you can read more about it. Because it's in the section about policy recommendations, so in the end of the report there is this section.

DEBORAH ESCALERA: Okay, thank you so much. Please be advised that all these presentations will be posted in the ICANN archive website after

today. Okay, our final presenter is Liubomir Nikiforov. Liubomir, the floor is yours.

LIUBOMIR NIKIFOROV: Well, I'm not used to those presentations. Thank you. Next slide, please. Next slide. My name is Liubo. Liubomir Nikiforov. I'm a Ph.D. student at the University of Barcelona, and my research is focused on informed consent, transparency, and Internet governance.

Today this presentation aims to outline the lack of precise guidelines on consent in the registry/registrar agreements. And the current situation leads to transparency and credibility risks for ICANN and different ICANN stakeholders. And I also at the end mention some of the possible solutions. Next slide, please.

The current registration process of generic top-level domain names is a contractual procedure involving three parties. Those three parties are a registrar, that's an entity that processes domain name registrations. A registrant, the person or an entity that wants to register a domain name. And a registry operator, which is the entity that maintains the registry of domain names registered in a particular top-level domain.

This agreement has one article. It has more articles, but it has one interesting article for me. It's Article 2, Paragraph 18 which establishes its data protection requirements. The same article

contains also a definition of personal data, notification requirement for data purposes, as well as data recipients' identification and consent. Next slide, please. Next slide.

Okay, thank you. This is the article I'm talking about. As you can see, it's the only article in the base agreement dedicated to personal data. And it intends to [englobe] all relevant information, all relevant dispositions on personal data. It's very difficult to read and to understand which poses questions on its intended purpose and final utility. Next slide.

What are the challenges? They are multiple. However, I will focus on the challenges which the consent requirement poses. According to Article 2 Paragraph 18 registrars have to obtain the consent of each registrant in the top-level domain for the collection and use of personal data. The Article 2 Paragraph 18, however, doesn't specifically what are the requirements for the validity of this consent nor the form that it has to have.

In order to exemplify these problematics, I'm going to use the GDPR, the European data protection regulation model in order to show what's wrong with it. According to the European regulation for consent to be valid it should be an informed, specific, free, unambiguous act of will of the data subject.

From the Article 2 Paragraph 18 of the registry/registrar agreement, we do not understand how and when this consent should be obtained. If it should contain strict and full description

of all the purposes for the data processing, what means could be used? Perhaps violence and intimidation are a valid means? And if the information given to the registrant should be intelligible to him. We have no idea whether the registrant can refuse to give consent and what will be the alternatives if he refuses to. Next slide, please.

But why is it important at the end? Well, because we live in a data driven society where information and data are tradable. And this is why it's important to ensure further stakeholders' trust in ICANN's credibility and also to ensure reliability and trust for an open and transparent Internet.

While in the EU we can count with specific safeguards on data processing, ICANN operates on a world level, on a global level. And current agreements may result in excessive abuses for registrants in different parts of the world. A process where the registrant understands the purposes and the expected outcomes of the data processing. And agreement benefits the registrar reducing possible misunderstanding, possible litigation issues and cases, and provides a competitive advantage to registrars and also reputational benefits for our organization as a whole. Next slide.

As I have promised, I am going to discuss possible solutions. One of them is the most obvious one, to revise the current article and to make it lighter and clearer to read. Maybe divide it in sub

articles. Especially on consent those data protection clauses should identify cases where consent is needed, provision of how and when consent should be given, as well as specific requirements for validity. An example thereof could serve the GDPR, the European data protection regulation, where consent should be an act of will which is specific, fee, informed, and unambiguous.

This model, of course, is not flawless. But if we can save our digital footprint as a prolongation of our personality, then informed consent is one of the democratic guarantees for our digital dignity. Thank you, and I expect your questions.

DEBORAH ESCALERA: Thank you, Liubomir. Are there questions? No questions? Let's check online. Okay, so as a reminder, all of the presentations will be posted on the ICANN website. And if you have any further questions that you may come up with at a later time, you can always email me at engagement@icann.org.

I want to thank you very much for being here with us today and remind you that our second set of presentations will be taking place tomorrow and invite you to join us. Thank you so much.

[END OF TRANSCRIPTION]