BARCELONA – NextGen Presentations
Tuesday, October 23, 2018 – 12:15 to 14:15 CEST
ICANN63 | Barcelona, Spain

UNIDENTIFIED MALE: ICANN 63 NextGen Presentations Session on the 23rd of October 2018 from 12:15 to 2:15 in Room 127-128.

DEBORAH ESCALERA: Hi. If there are audience members here for the presentations, there was a little error on the schedule. NextGen is having lunch for the first half hour. The lunches here are only for the NextGen. Then the presentations will be starting shortly after they are done with their lunch. So, it's closed session for the first half hour and then we'll start the presentations. You're welcome to stay in the room if you'd like, but we're just going to be delayed for a short while, while they have their lunch.

Hello, everybody, and thank you for joining us for the second day of the ICANN 63 NextGen presentations. My name is Deborah Escalera. I am program manager for public responsibility support. I manage the NextGen program. I'd like to thank my returning NextGen ambassador, Sarah Ingle from ICANN 61; Desara Dushi, ICANN 58; and Razoana Moslam from ICANN 60. They are returning ambassadors that are here to support the new NextGen as mentors.

So, we're going to start our presentations right away. First up is Maria Korniiets from the Ukraine. Maria?

MARIA KORNIEETS: Thank you. Hello, everyone. Thank you for being here. My name is Maria Kornieets and I will do my presentation about Youth IGF Movement in Ukraine. I'm the ambassador for Youth IGF Movement in this country. This is the logo of Youth IGF Movement.

Let me tell first a little bit about myself. Well, basically, I did masters in international economic relations and then I kind of got into software architecture. I've been studying it for two years now. I've also been lucky to participate at YouthDIG this year.

So, then, first, as you might guess, what Youth IGFs initiatives are about, they are about organizing Youth IGFs. Basically, our first event that was called Youth IGF Initiative Ukraine was held a year ago. It took place in Kiev, Ukraine. Kiev is the capital of Ukraine. We were lucky to have around 80 participants. We had seven speakers in six sessions and the event was around four hours. Here you see some nice pictures.

Basically, what did we discuss that time? We spoke with young people about the history of the Internet and the possibilities for the young in the Internet ecosystem. [inaudible] we had NextGen, presented NextGen Program and Fellowship Program.

We also did a little bit of both. It's kind of interesting. You might notice that only 30 people answered. Well, you cannot get people after the event to do something. They are already tired.

Basically, I think it's kind of interesting that more than half people acknowledged they were addicted to the Internet. That one you see.

Less than 10% said, no, they were not. So, majority of people said, "I didn't know I am addicted."

Also, this year there's also been a youth IGF event in Ukraine. It took place in September, too. It was joint with National IGF this year. Those were called Days of Ukrainian Internet. I've been a part of the organizing team and we were happy to get around 100 participants this time. The same, the topics were mainly about cybersecurity, a little bit of block chain and net neutrality, too.

I mentioned that what we basically do is organize an IGF, but also it's important to build a community of people who know about Internet governance issues, who care about Internet governance issues. So, how do you do that?

Well, the basic is of course we have a Facebook page that we try to keep running and alive. The most successful, I would say, posts are of course some videos and pictures. For example, on the left, you see Olivier Crepin-LeBlond. I asked him if he doesn't mind to be shown in the presentation.

Anyway, we were lucky to get also 500 views, more than 500 views. I think it's quite nice for our Facebook page. On the left, you see me presenting something with glasses to appear more intelligent. Anyway, of course, it's not all we do.

Also, you might know that October is cybersecurity awareness month. What do we do for that? First, just a day before I left to come here, we've

organized an event about the careers in cybersecurity. Well, why career in cybersecurity?

First, I've been to a few events and always people say that it's a lack of qualified cybersecurity experts in Ukraine. It's hard to build the capacity. It's hard to educate people in this fast-changing environment. Also, it's kind of interesting for students, of course, too. So, we decided to hold an event like that.

So, it was also kind of nice. We've got a lot of people and even it was even so popular that we had to close registration three days before the event. Here you see my team helping me to organize event. Well, and also, who was the presenter? We are also happy to get quite nice speakers. It doesn't play right. It's a video. Oh, it works.

So, when we calculated how many people we've got, we were like, "Yeah!" So, we did that. It was more than 100. Actually, the whole room was full, 120 people, maximum. We were doing this to celebrate.

Anyway, apart from that, maybe you know that in cybersecurity you can hold nice events by scaring people, like scaring people how much data they put online and so on. We incorporated that a little bit, too.

Well, we asked people to submit their [inaudible] registration form and you know how you tick the box that I agree to the terms and stuff. We took the form copy there and we incorporated there … Well, there was the link to the terms. They're not working. They [have] no legal powers or anything. So, we tried that.

You have to make a [comment, picture] after the event, ask one question to the speaker, eat one piece of pizza, and in case you don't do that after the event, you have to send – on each birthday of the organizers, you have to send them a pizza with a text, "I serve you, my Lord." Well, nobody read that. We asked people if anyone read that. So, we asked them to be more careful with their data.

Also, there was supposed to be [live] here because it's just happening right now I think in the Ukraine maybe in 20 minutes. We've organized a debate around cybersecurity issues with the debate club. So, maybe pictures will be coming. Follow the Facebook page.

Also, we have some future plans like holding more webinars and, as you see, we did something on cybersecurity about of course Internet governance is wider. It's also law issues and many human rights issues. So, it would be nice to hold more events on that, too. That's it. Thank you for your attention. Any questions?

DEBORA ESCALERA: Thanks, Maria. Are there any questions from the audience? NextGen? Oh, there is one question from the audience.

OSKANA PRYKHODKO: Hello. Thank you very much for a very interesting presentation. I am Oksana Prykhodko. I am also from Ukraine. Could you please say some words about Youth IGF Movement? Is it a future organization? Do you have a website, financial resources, or what it is it? Thank you.

MARIA KORNIIETS: I guess we can talk about that after the presentation. Thank you.

DEBORAH ESCALERA: Any other audience questions? NextGen? Okay, thank you so much for your presentation. Our next presenter is Natalia. I can't say your last name. How do you say your last name? Dulkowska.

NATALIA DULKOWSKA: Firstly, let me thank all of you for being here today. [inaudible] and PhD candidate in the field of European Union Internet Property Law. My PhD is an attempt to make systematic analysis of scope of [inaudible] and one on trademarks extended protection in European Union jurisdiction.

So, we've already mentioned of the functions of trademarks and the purpose of the law protecting trademarks. As a researcher, I know that all of the most important trademark cases from the last years arose on the basis of Internet law matters, technological companies, and e-commerce business disputes.

So, when does an Internet domain name qualify as a trademark? Without any doubt, the Internet has changed the way that the world does business. Whether someone can protect their visual appearance of a website together with a domain name from copying by others. Actually, it's one of the most IP questions. The Internet has [inaudible].

Just like [Jan] yesterday said, the need to distinguish one person's products or services from [others] is at the heart of trademark

protection. So, typically, this is a complete [inaudible] symbol, combination of the tools used in conjunction with one entity's goods or services.

So, the trademark protection serves the public interest by making the public aware of what person or company has produced a particular product. So, therefore, a domain name can qualify as a trademark when it's used in connection with a website that offers services or goods to the public.

But, as a webpage has too much information and [inaudible] trademark [inaudible] principles of trademark laws [stressing] the distinctive appearance of one product or service as compared to another [inaudible] trademark themselves.

However, only some types of commercial domain names qualify for a trademark. In other words, using a generic name for the service or goods. For example, like transportation information. The owner of the name will have less trademark rights against the user of similar domain names than he or she would if her or his domain name was more distinctive.

So, here's a quick look at the differences between domain names and trademarks. Very often, a business will use its business name, brand name, or another kind of business identify as its domain name. However, unlike trademarks, domain names are global, unique by nature and the most important can be shared between two websites.

So, a registering domain name doesn't automatically give any rights over the matching trademark and we can only gain this right by registering a domain name as a trademark.

So, what happens if there is a conflict between an Internet domain name and existing trademark? Even if a company owns a registered trademark, someone else must still have the right to the domain name.

As I said, there are generally three kinds of domain name disputes. Firstly, it's like two trademark holders, one domain name. When this happens, it's a race to the domain name first. For example, Delta. Delta airlines and, for example, Delta Dental have Delta as registered trademarks in different industries and different markets. In this case, Delta Dental cannot bring an ACPA or UDPR or [inaudible] against Delta because it is within its right by using a mark within each market, and clearly there's [inaudible] consumer confusion, as well.

The second kind of domain name dispute is when no one owns the trademark but everybody wants the brand. So, in the event that no trademark is involved at all, then it's just first come, first serve. And not all domain names are trademark protected. So, sometimes all about who can afford those beautiful generic domains.

The most interesting part is when sometimes a person known as a cyber squatter registers a famous one on trademark with repute as a domain name hoping to later profit by reselling the domain name back to the trademark owner.

So, the first kind of domain name dispute is cybersquatting. It's like when you own a trademark and someone without rights to the mark is exploiting your trademark in bad faith. And if we believe that someone has taken a domain name in bad faith, what we could do is the trademark holder could file, for example, in US a federal lawsuit under the Anti-Cybersquatting Consumer Protection Act. Or what is cheaper and faster, the trademark holder could initiate an ICANN-approved arbitration proceeding under the Uniform Name Dispute Resolution Policy.

So, this one is not a [inaudible] example. In fact, such a scope of [violations] is rather common in [inaudible] country. For example, the figures extracted from the Danish studies showed that for the period of one year there were 566 dot-DK domains that were registered by suspected infringers of trademarks immediately after the domain names had been given up by the previous registrants and became available for registration.

So, to quickly conclude, finally and in summary, it is definitely a question how to fight this criminality. So, what could we do?

Firstly, we need legislative framework enabling bulk domain name seizures, longer grace periods from domain expiry to re-registration. Also, comprehensive Know-Your-Customer requirements from registries is also one of the solutions. Then, the implementation of international investigation and prosecution with common strategy and common goals.

So, these are just [committed] proposals which will help us to move forward, but there's a lot of work to do for further improvement to make the domain names and trademarks proceedings system more fair, more clear, more balanced. That's actually what I wanted to point out. And here is my contact information. Thank you.

DEBORAH ESCALERA: Thank you, Natalia. Are there questions from the audience? Go ahead.

[DAVID MARGOLIS]: Hi, [David Margolis]. Why would you do the seizures in bulk as opposed to one by one? Isn't it a bad act of filing a bad trademark and not the bad actor?

NATALIA DULKOWSKA: Yeah. I think it's about bad faith and bad act, but [inaudible] international comprehensive [proceedings] which could help us to prevent it.

[DAVID MARGOLIS]: Yeah. But, I still don't understand why in bulk, like the bulk.

NATALIA DULKOWSKA: Because [about five]. Because when someone is automatically trying to register the trademark which is free for a moment, but it's still infringing someone's rights. I think it's kind of [a bulk] domain name seizure. That's my perspective. Thank you.

DEBORAH ESCALERA: Any other audience questions? NextGen? Okay, thank you, Natalia. Our next presenter is Sabrina Wilkinson. Sabrina?

SABRINA WILKINSON: Is this working? Yes. Okay, great. I have a very bad sense of time, so if someone could give me a nod when we're at two minutes maybe, that would be great. Sarah will? Okay, I'll my eye on you.

So, hello, everyone. My name is Sabrina Wilkinson. I'm a Canadian. Maybe before I start, I'll ask. I know there's at least one Canadian here. Are there any others? Oh, yes, that's true. Okay, we have a few.

I'm studying in the UK at Goldsmith's which is a part of the University of London and I'm here today to talk to you a little bit about my doctoral research which focuses on obviously the politics of Internet policy in Canada.

So, perhaps before I dive into the various elements of my project, I'll just briefly outline what I mean by politics. So, here, I mean that I am researching the various interactions, dynamics, strategies, and influences that exist in this space between different groups involved in policy development about the Internet in Canada. So, this includes journalists, academics, activists, lobbyists, public interest groups, politicians, policy makers.

I'm very much focused on how policy is made and then what are the implications of these dynamics on subsequent policy outcomes. But, first and foremost, it's the development process which is my key focus.

So, I guess in this presentation I'm just going to go through my research questions, methodology, theoretical considerations as well as – sorry, I'm a little nervous – some of my initial findings.

So, to get at this question about the politics of Internet policy in Canada, I'm informed by various other inquiries that kind of fall under this broader question. So, these include what are the key players involved with which ideas and aims? Which discourses and rhetoric are employed? What institutional processes and rules are involved and what do these rules and processes mean for the inclusion of different voices? And finally, this gets to the implications of these interactions on subsequent policy outcomes. But, what do these findings from these initial questions mean for what policies are developed when we're talking about the Internet in Canada?

And specifically, what does it mean for the capacity for … I use the term information intermediaries but I guess I mean technical entities that operate to provide Internet access or to manage information on the Internet. It's very broad here. I'm talking about things ranging from Internet service providers all the way to social media platforms like Facebook. But, what do the interactions in this space mean for the capacity for these technical entities to provide access to or control the movement of information?

So, I have a couple of theoretical considerations that inform my project and inform these questions. These are a focus on the ways that gatekeeping processes occur both in policy making environments. So, I mean here that there are individuals in policy making environments that have particular means of access or influence in different ways than other groups. I also mean that these sorts of gate-keeping practices also occur on the Internet or in the provision of Internet service itself.

I also have a concern for the capacity of powerful actors to dominate policy scenarios about Internet policy and, in turn, a concern for the ways in which that domination may impact policy outcomes. And I have an interest in finding ways to better incorporate – and I think I should also add more meaningful and incorporate the public in Internet policy-making in Canada, specifically. What's my time? Five minutes, great. Thanks, guys.

So, to again answer these questions in a more practical sense, I'm using a number of largely qualitative methods. I'm interviewing people involved in two case studies in Canada's communications policy environments. I'm happy to elaborate on these case studies during the question period but I'm not going to lay them out here.

So, I've conducted interviews with about 30 people involved in these two cases so far and I expect to maybe interview about 75 in total. I'm analyzing primary documents and data, so I'm looking at the funds and resources that have been used in lobbying efforts. I am looking at the various policy interventions and documents and speeches related to my particular case studies.

I don't necessarily have an ethnographic or participant observation element to my project, but I would note that when I was back in Canada for pretty much the last month and I actively attended and observed what went on in meetings relating to the policies that I was studying. And here, I took a count or I guess watched how people interacted and what sort of … I don't know, I guess what sort of interactions occurred in these particular spaces, and this in some ways informs how I think about my case studies as well.

So, I've just started my second year and I will be doing data collection for this project throughout this year. So, these are very, very initial findings. But, I guess it's corporate actors, and again, if people would like to talk about this in specifics, I can go into it in the question period. But corporate actors have substantial resources and influence in the Canadian Internet policy environment. I think more interesting is that these resources and influences are often leveraged in really creative and unique ways to augment or support certain policy positions.

I've also found that public agencies and departments in Canada are kind of in what I would consider a period of over-consultation right now, which obviously at face value, consultation is great. But I think it poses various problems. For one, there should be perhaps a more streamlined approach to these issues. Moreover, in periods of over-consultation we see, particularly public interest groups, who are under-funded and have fewer staff members really struggling to participate in all of the various activities that are going on.

I wrote this before I came to this meeting and learned a little bit more about how ICANN works, but I guess in terms of how my initial findings may eventually be applied to thinking about things like ICANN and other organizations, I just think it's very important that individuals in this space and researchers in this space pay attention to the covert and often novel ways that powerful interests can influence policy processes.

I also think that consultations and inquiries related to Internet policy should be inclusive. And this gets back to my point I made earlier about the sort of over consultation that is currently occurring in Canada. I think it's really critical that participation is meaningful and takes into account the many individuals that are operating strictly on behalf of the public interest, don't have very much money, don't have very much time, and it is critical that their participation is meaningful. That's my info. Thank you.

DEBORAH ESCALERA: Thank you, Sabrina. Are there any questions from the audience?

STEPHEN BARRY: Stephen Barry from dot-CA. I was wondering if you could opine a bit on over-consultation from marginalized groups such as indigenous groups or low-income groups in Canada and how that specifically [inaudible] their involvement in policy.

SABRINA WILKINSON: That's a really good question. So, I think there are … The broader problems with respect to over-consultation that applied to all public interest groups are a lack of resources, a lack of funding, a lack of time. Are people working other jobs and doing this on the side? I think all of those also apply to marginalized groups.

I'm trying to think of issues that are especially relevant to marginalized groups. I think that's a critical question. I guess it might be … Canada is obviously a huge country, and with respect to, let's say, groups that are living in rural and remote communities who are already often marginalized dealing with various other issues, have really crappy broadband services that are expensive, as I'm sure you know well, I think they're also facing other issues because they're not in Ottawa where policy making and these kind of practices of influences and strategy take place.

So, I think maybe that's one marginalized group and each of them face different issues, but individuals living in rural remote communities in Canada are often forgotten because they are not physically in the space where these things happen, so it's especially critical that finding and programs that really support their meaningful participation allow them to overcome that barrier.

STEPHEN BARRY: Thank you.

DEBORAH ESCALERA: Any other questions?

[DAVID MARGLIN]: What are some of those covert and novel ways that political processes or whatever processes are influenced?

SABRINA WILKINSON: Yeah. That's a good question. I thought someone might ask that. One that I'm still looking into but that I've had many different people flag is a little bit complex, so I'll try to … It has to do with a particular process that Canada's media regulator, which is the Canadian Telecommunications - oh, what is it? Canadian Radio – what is it? It's very long. Canadian Radio Television and Telecommunications Commission.

Anyway, essentially runs a process by which incumbents and public interest groups and various stakeholders can come together to consult on particular issues and public interest groups are given an opportunity to recur some of the costs that they spent to participate in this proceeding by putting forth an application to the regulator which then gets either approved or denied or reduced on certain grounds. Their application involves laying out the source of funds that they've used. And if the CRTC approves it, then those funds will get pulled from the incumbents and brought to the public interest groups, which at face value, seems like a good way to do it and a good approach, but something that I still need to evaluate but something that has been pointed out to me as perhaps there is an issue in the ways in which incumbents who are allowed to respond to that application that is being made kind of pull apart and criticize the public interest group's

application to the extent that it forced the public interest group to use much more unpaid labor because the work that has gone into making [this] application isn't paid, use many resources to get these funds. Does that make sense? That was a little bit inarticulate.

I guess the point is that there are things that are complex and difficult for me to explain and not really known.

DEBORAH ESCALERA: Okay. Any other questions? I thought I saw one over here. No? Okay. Thank you, Sabrina. Great presentation. Our next presenter is Stefan Filipovic. I'm really bad with last names. Sorry. I'll just go with Stefan.

STEFAN FILIPOVIC: Can you hear me? Sorry. [inaudible], I guess. So, my name is Stefan Filipovic. Some of you already know. I [inaudible] at the University of Oslo and also I practice IP law in my free time. Today I will be talking about WHOIS Platforms Operator Compliance with GDPR.

So, what is WHOIS? Basically, WHOIS is a lookup service that provides answers to the question who is in charge of specific domain names or an IP address. That means that it basically contains, it maintains the database of both personal and non-personal data.

In charge of WHOIS platforms are registry operators and registrars. And why they should care? Well, because of the very first thing on the slide, which is they maintain the database of personal data.

ICANN's response to GDPR was introduction of temporary specification for gTLD registration data which is a temporary solution which can last up to one year and basically modifies existing requirements under registrar accreditation agreement and registry agreements.

The most important thing about temp spec is it introduces some new obligations on WHOIS platform operators. Those requirements can be found in appendix 8 of the temporary specification and basically access to personal data must be restricted [inaudible] for someone who wants to see personal data on registrant. He shouldn't be able, unless there is explicit consent provided by the registrant.

There is another possibility when a third party can access personal data and that is when a third party has legitimate interest that overrides, that prevails, over fundamental rights of registrants. That can be a bit tricky. That's why I think that this approach is a bit risky and there's some downsides to it.

First of all, identify temp spec. No clear definition on what should amount on legitimate interests and currently there are no clear guidelines for WHOIS platform operators.

Furthermore, this requires from WHOIS platform operators to basically balance between fundamental rights. It expects from them to decide whether the right to seek information, the right to receive information, should prevail over registrant's right to privacy.

Sometimes, you have [inaudible] European Court of Justice or European Court of Human Rights is that cannot get on the same page

about it. So, I think that's really burdensome on WHOIS operators. For those reasons, my opinion is that WHOIS operators will be inclined to err on the side of caution in order to avoid the huge fines that can be imposed by DPAs. Ultimately, that will lead to a chilling effect.

So, how does temporary spec work in practice? Well, usually when … Okay. So, I did a quick search and usually when registrant has a citizenship of the EU country, they indeed redact all personal data. But when WHOIS operators are not sure, they make mistakes. And in this case, this is the case of [inaudible] who currently lives in the EU country. I don't know if you can see, but here are all his personal data exposed. So, what's the reason for that?

Well, I think that, first of all, WHOIS, it might be I think they maybe misunderstand GDPR's territorial scope because they concentrate on a person's citizenship, while instead they should probably concentrate on where that person is. I think [inaudible] Article 3 of the GDPR is really clear because here you can see that the focal point is where that person is located and not whether he is a citizen of an EU country or not.

So, in this situation, I am Serbian national, but as long as I am in Spain, I am protected by the GDPR's provisions. Similar provisions can be found in temp spec.

Also, there is another possible … Maybe they understand what the GDPR's territorial scope [inaudible]. So, there is another reason for that and probably that's more likely I think that maybe when they decide where the person resides in the EU or not, they rely on mailing

addresses and country codes with telephone numbers attached. [inaudible] subjects provided and the registry domain name.

I think that sometimes registrar's are not maybe that responsible so it may be too much to expect from them that they will always, when they change their postal address, that they will actually go and update that information. So, who gets in trouble? Well, ICANN because ICANN is data controller, and of course registry operators and registrars, they're in trouble because of the huge fines that go up to 10 million Euros or maybe 4% of the total [inaudible] annual turnover which can be quite high for huge tech companies. So, this is just some of the example of WHOIS operators who violated GDPR and who are in line with it.

So, in my opinion, the only way to ensure compliance with the GDPR is to apply thin data requirement to all data subjects regardless of where they're from.

Luckily, ICANN is working on developing new mechanisms, new policies, on how to bring all of them in line with GDPR. So, there is [inaudible] protocol which is basically [inaudible] to be a replacement for the WHOIS protocol and in order to standardize access [inaudible]. Also, there is unified access model. This should include some sort of accreditation bodies that [inaudible] credentials for third parties that want to access personal data. And at the end, there is GDPR temp spec and currently my understanding is that they are considering whether temporary specification for gTLD registration data should become ICANN's consensus policy, and if so, what should be the content of that policy? Yes. Thank you very much. So, if there are any questions …

DEBORAH ESCALERA: Thank, you Stefan. Any audience questions? Okay, NextGen. Did you have a question? Nobody? Okay, thank you so much. Our next presenter is Teresa Quintel. Is it Theresa or Teresa?

TERESA QUINTEL: I actually don't know myself [inaudible]. You can say it however you want to. So, first a remark. I thought that my presentation was yesterday so that's why I wrote it on this presentation.

I'm a PhD student at the University of Luxembourg in Uppsala University in Sweden. But I usually work on data protection. So, right now, I'm presenting on something completely different because I recently wrote an article with a colleague of mine who is working on self-regulation and liability of intermediaries.

So, the title of my presentation is Self-Regulation of Fundamental Rights and I will speak about initiatives by the European Union. Does someone have this click thing, without clicking it?

So, I will speak about initiatives by the EU for the regulation of hate speech, illegal content, and disinformation online. I will quickly speak about self-regulation in the EU, hate speech, then some of the initiates. It's not all of them. There's a lot more. Open questions, criticisms, and I will suggest some solutions.

So, self-regulation in the EU is a dominant form of regulation in the online environment because it provides flexibility and complements

formal legislation, and then the EU, there's this idea of we do not want to prevent competitiveness to its other players by over-regulating. That's why self-regulation. Which basically means that private parties undertake enforcement measures to tackle legal content online by blocking, removing, monitoring, and filtering content.

That means that these measures may interfere with the fundamental rights of online users. For example, the right to freedom of expression where legal content is being blocked or removed or the right to privacy and data protection where online platforms monitor and filter the content. It may potentially also interfere with rights of online platforms to conduct business.

So, what is hate speech? And this is the wrong presentation. This was not supposed to be here.

In the EU, there's no universal consensus on the definition of hate speech, but there is a framework decision on racism and xenophobia from 2008 which defines hate speech as "all conduct publicly inciting to violence or hatred directed against a group which is defined by reference to race, color, religion, dissent, or national or ethnic origin".

The problem is that the national laws of the EU member states are often very broad and ambiguous and the illegality differs between the member states.

So, the EU Commission in May 2016 published together with four major IT companies – so, it was Facebook, YouTube, Twitter, and Microsoft and nowadays there's also Instagram and Microsoft-plus – a code of

conduct on countering illegal hate speech online in which the companies committed to having in place key and effective processes to review notifications and to remove or block access to such content, to have community guidelines in place in which they clarify that they prohibit illegal content on their platforms, and to review valid notification requests against these guidelines, or where necessary, against the national laws that transpose the framework decision from 2008.

Moreover, they should review the majority of notifications in less than 24 hours and where they consider the content to be illegal, removed, or blocked content. They should also engage in education and awareness raising and provide information on the procedures of submitting notices.

So, this code of conduct is a non-binding instrument and it's very unclear and very ambiguous. So, the commission in March 2018 published a recommendation on measures to tackle illegal content online which is much more detailed than the code of conduct in terms of notices and counter notices.

The recommendation encourages online platforms to improve transparency with regard to these notices and counter notices. So, the content providers should be informed whenever his or her content is being blocked or taken down and should then have the possibility to contest this, remove it by submitting a counter-notice.

Online platforms should also publish transparency reports on the content taking down or blocked and the time for removal or the time

for taking action. They are encouraged by the recommendation to use proactive measures, meaning automated means to detect illegal content. So, for example, upload filters, which should be accompanied by appropriate safeguards, so that legal content would not be removed, meaning human oversight and revue. There should also be measures that notices in bad faith that were submitted should be prevented.

Like the code of conduct, the recommendation is a non-binding instrument and it's difficult to enforce [all these] encouragements by the European Commission.

In April, so one month afterwards – so, this is not supposed to be here, either – the Commission issued a communication on disinformation. It's a different matter than covered under the code of conduct on hate speech and the recommendation from March 2018. But it's similar in the way that it's self-regulatory measure and it's very difficult to enforce.

In this communication from April 2018, commission proposed some key elements which were then implemented in a code of practice on online [inaudible] which was published in September this year.

The problem of disinformation is that it's not illegal content. Disinformation is not defined by law as illegal content, and therefore the risk of disproportionate interference with fundamental rights such as the right to freedom of expression is even higher than under content that is actually legal by law.

So, the code of practice. In the code of practice, the signatories commit to in more scrutiny of ad placement, more transparency about political advertisement, specifically also with a view to the European elections next year, closing off fake accounts and marking of bots, empowering consumers and improving media literacy, and the research community in order to inform more about disinformation and the public about how to detect such disinformation.

So, the points of criticism that I already mentioned would be that there's an overly broad definition of hate speech and a different threshold in the different member states in the EU. There's a risk of [inaudible] of enforcement activities from the state to private companies, such as Facebook and Twitter and that could lead to an elevation [inaudible] community guidelines about the law.

Then there's no legal definition of disinformation and fake news, so they are not illegal as such. There's a risk of an excessive interference with the right of freedom of expression, also the right to privacy and data protection where proactive measures such as automated means and future mechanisms are used by the online platforms.

So, the question would be whether this non-binding nature of the measures is sufficient and makes the online platforms actually accountable towards their users.

So, the open measures would also be that there's no [inaudible] mechanism. It's only counter notices that are being suggested. Court legal proceedings are deemed to be less efficient than alternative

dispute settlement, although these measures are much more transparent than court proceedings.

The recording by hosting service providers is according to how many take-downs had been pursued by the online platforms and not whether the content has been taken down according to the community guidelines or according to the law. And there's no binding commitments with regard to auditing.

So, there's possible solutions that I and my colleague proposed in our article, one of which would be to consider online platforms a [source] of public spaces which have a public responsibility, meaning that they would have to comply with closely defined public interest criteria and would not only act reactively by taking non-content but would use proactive measures.

That would mean that companies would be obliged to identify and classify the risks related to illegal activities on the platforms and would then implement preventive measures according to the risks.

The platforms would also have to demonstrate that their risk responses are adequate, that they're proportionate and effective with regards to the risks that they have identified and that they respect fundamental rights. So, that would be in accordance with the duty of care and the holistic risk management approach.

The problem in that approach would, however, be that it would remain open how competent authorities would judge on the proportionality of the measures because they would not only need to have more insight

into the data management strategies of the companies, but also need to understand and have the technical expertise to actually carry out [orders] of these strategies.

So, the article will be published sometime in 2019, probably, and this is my contact. Thank you very much.

DEBORAH ESCALERA: Thank you, Teresa. Any questions? Audience questions? NextGen? One at the end. It's not working. Try the next one.

[DAVID MARGLIN]: Oh, now it's working. Good. Hi. We're all here, as we sit here subject to expected standards of behavior to be at the meeting. Would you favor some kind of expected standards of behavior generally and how would they be promulgated and who would be subject to them?

TERESA QUINTAL: I'm not sure whether I understood your question. The respectful behavior towards within this community or?

[DAVID MARGLIN]: Well, we are all here. By coming to the meeting, we've ticked the box that says we're all subject to these expected standards of behavior and we're going to conform to them. It sounded to me like you'd be in favor of there being an expected standard of behavior that is general to anyone having discourse on Facebook, Twitter over the Internet. And if

you do support that, then where would it come from and who would it apply to?

TERESA QUINTAL: Well, what I've been speaking about is I think it's a very different approach in Europe or in the European Union than in America, because in America there's free speech First Amendment rights are much higher regarded than in the EU.

What I've been speaking about was more actually illegal content. It's not about behavior or respectful behavior towards others in the sense that you should be nice to others, but it's people that post illegal content and hate speech that actually [inaudible] the integrity of others and that is illegal and therefore has to be taken down. The problem being that in this presentation, platforms can actually judge on which content could be taken down in accordance to their guidelines and not in accordance to the laws because, in the EU, there's 28 different laws and it's very difficult for the platforms to judge on these laws or to know all these laws. So, they might take down content in accordance to their guidelines which might not actually be illegal and thereby take down legal content which should not be considered hate speech or illegal under the national laws. And that might then lead to a restriction of freedom of expression.

But, yes, it's always nice to have these guidelines and codes and respect towards others, but what I've been speaking about was actually illegal content.

UNIDENTIFIED FEMALE: So, it's clear that … You made it pretty clear that speech online and content is usually regulated either by self-regulation or by [inaudible] law. Do you think that in the future, with the issues with the challenges that we face today, should we expect more hard regulation of content?

TERESA QUINTAL: Well, there are some member states that have now implemented [inaudible] self-regulated illegal content, one of them being Germany and [inaudible] in which companies have to show that they have certain structures in place that they are able to take down illegal content, and otherwise there will be high fines.

So, it's not regulated in a sense that they have to take down content, but they need to demonstrate that they have these structures to be able to. In France and in the UK, there's also laws or attempts to regulate more, and with regard to this communication on disinformation, the Commission also said if companies don't comply with this code of practice, which is non-binding and companies can withdraw at anytime, they will propose regulation.

UNIDENTIFIED FEMALE: Thank you.

UNIDENTIFIED MALE: Maybe come back to the first few slides. I was wondering who actually has the responsibility of blocking, removing, and so on? Do you think

that the scope of the responsibility of the company who do the blocking or something, now it's broader? So, for example, it used to be maybe just the content provider, but now who actually [inaudible] provided … It's like a [inaudible], so the only provide the broadband, the Internet service, but they don't really manage the content. Do you think it's also now the responsibility also lies on them or not?

Also, maybe about how it works, who actually is blocking, removing, and so on. Is it the concern from the government? Of course it depends on the members then and so on, but I think different countries can be different how it works. Thank you.

TERESA QUINTAL: Okay. It's much more complex than I showed in my presentation. If you want, we can speak about that later. I tried to summarize it very quickly. So, in the EU, there is a directive, a law, that is called E-Commerce Directive which prohibits the filtering of content online. So, platforms are, in that sense … So, they don't really have a responsibility, but … So, how to explain?

You have these community guidelines. As I said, they are supposed to have these community guidelines in place, and whenever a user … So, on Facebook, for example – take that because it's the easiest. You can submit a notice that this content disturbs you. Then you have to say why and why you would like to have it taken down. Then, it will be checked, your notice, by the platform and it will be checked according to their guidelines, and if necessary, in accordance to the national law.

Then, it will either be blocked, taken down or it will remain because they don't agree with you and that it's illegal.

At the same time, law enforcement in the different member states can also submit notices and their so-called trusted flaggers which are experts in the field of hate speech and illegal content. They can also submit notices.

When it's illegal content, then it will be communicated also to the [competent] authorities in the member states. I don't know if I answered your question. Yeah, to a certain extent. I think maybe what he was referring to was also geo-blocking would be a way that you can prevent something but we can talk later.

DEBORAH ESCALERA: Okay, thank you.

UNIDENTIFIED MALE: Sorry. We can continue in e-mail. That's fine. Thank you

DEBORAH ESCALERA: Alright. Thank you so much. Any other question? Okay. Great presentation. Thank you so much. Our final presenter is Ualan Campbell-Smith.

UALAN CAMPBELL-SMITH: Hello. Hello, everyone. My name is Ualan Campbell-Smith and I'm going to be presenting on the topic of cyber sovereignty. It's quite a broad

topic so I'm going to kind of give a broad overview and then a few specific examples and definitions.

So, before I start, just quickly about me. I'm from the UK. My background is in politics and international relations, so hopefully we've gone over all the legal jargon. There won't be any in this, but I did appreciate it. I'm now doing social science of the Internet at the Oxford Internet Institute.

So, just to give you a quick overview of the structure, I'll give an overview of sovereignty and the Internet and how they relate, contrast sovereignty in China and the UK and then finish by saying, "So what? Why should any of you care? Why am I telling you this?'

So, what is cyber sovereignty? Cyber is a word that kind of means everything and nothing. It involves the virtual, so information, data, also the physical, so networks, the physical infrastructure and this poses problems for the concept of sovereignty because sovereignty is, in the shortest possible definition I think ever, government-controlled within borders. So, you have some countries which have information sovereignty, some which kind of stress network sovereignty. So, the way these three different areas [overlap] is quite important.

Why this is relevant here at ICANN is we've all heard about the multi-stakeholder model, but this is the multi-lateral model. So, the Internet is bordered and regulated nationally.

So, my undergraduate dissertation, I focused on cyber sovereignty in China because it is, I suppose, the poster boy cyber sovereignty. So, in

2015 at the Wuzhen World Internet Conference, President Xi Jingping said that cyber sovereignty would be the guiding principle of Chinese Internet policies.

I group this into the four pillars. Here is quite a long definition. I don't know if you can read it. But effectively that China can develop its own Internet public policies and that no other states can interfere with its internal affairs. So, I grouped it into territoriality, autonomy, control, and sovereign equality.

So, most commonly, people think cyber sovereignty, it's the great firewall. But, there's a lot more to it than that. For example, last year was China's cybersecurity law came into effect which kind of includes data territorialization kind of similar to the GDPR but also then goes a lot further. So, look up that law of you're interested in that.

So, China's position has changed over the years. In 2016, in the report on World Internet Development it says that multi-lateral and multi-party participation will be important. So, this is a shift that's kind of accepting that Internet governance is going to need more than just the government and even just being here today, I've seen that China is the vice chair on the GAC, or was until this meeting, but is still involved in Internet governance.

So, sovereignty in cyberspace doesn't just mean Internet regulation in the terms of China. So, I looked at the UK as well, being from the UK. So, the UK's national cybersecurity strategy said that cyberspace is only one sphere in which we must defend our interest in sovereignty. This is

an important distinction because the UK is protected in global cyberspace whereas China is protected within China cyberspace.

So, just because the government doesn't control the Internet doesn't mean that governments don't kind of have a duty and the obligation to protect critical national infrastructure and citizens within that cyberspace, if that makes sense.

A couple of the NextGen have asked me, "Brexit, GDPR. What's going to happen?" I was going to avoid talking about it because all the Brits are probably sick of it, but effectively after Brexit, GDPR is going to be written into UK law under the Data Protection Act and there's an interesting difference which is that the Data Protection Act is going to also cover, make kind of concessions for national security, so we can see the national security. Whereas GDPR focuses on kind of business, I think in the future, more and more of these data regulators are going to focus on national security because it's national security concerns that are pushing the cyber sovereignty movement.

So, finally, why does anyone care? So what? Why are you looking at this? As we've heard in many of the presentations, the fragmentation of the Internet is a very big topic of discussion and cyber sovereignty is one of the ways in which the fragmentation of the Internet is coming about. We saw the map yesterday of the balkanized Internet with China with its own Internet, and so it's really important to track the principle of cyber sovereignty and how it's enacted in different countries. So, like I was saying with China how it's had a shift in policy. How is it going to change in the future?

For example, the World Internet Conference is in two weeks' time in China. So, what are they going to say? How is it going to impact World Internet? Who knows? I'll see in a couple of weeks.

Secondly, it's important to balance sovereignty, security, while still maintaining a global Internet. So, we've just had a presentation on WHOIS and GDPR by Stefan. Thank you. It means I don't have to go into that, but basically, how countries can ensure national security without breaching data regimes or regulation which is going to go about and how national security is written into that regulation I think is going to be really important going forward.

Finally, a bit controversial, as the word controversial said, the former CEO of ICANN, Fadi Chehade, moves to be a co-chair of the Wuzhen World Internet Conference Advisory Committee. I know that's a bit controversial. You can Google it. There was a lot of hoo-ha around that, but I think it's important because governmental fragmentation in the form of cyber sovereignty also leads to technical fragmentation. So, how ICANN is going to react in the future to increasing national jurisdictions of policy and frameworks could impact how the Internet functions on a technical level around the world.

So, thank you very much. I know it's a brief overview of a very big and important topic. If anyone wants to read more, I know a lot of us NextGens have pointed out Milton Mueller, but it's a really good book if you want to read it. That's a shorter paper to give you an overview of it all. If anyone has any questions that I can't answer now, e-mail me or

shoot me a connect on LinkedIn because why not? But, if anyone has any questions, I'll be more than happy to answer.

DEBORAH ESCALERA: Thank you, Ualan. We have your first question right here.

RUSS MUNDY: Thank you. Great presentation. A couple of things. Fadi is now with dot-donuts. So, he's [inaudible] so he's now with dot-donuts. He keeps moving.

One of the things Dr. Andrew [Clements] talked about is the digital sovereignty issue in the Canadian context is the e-mails flowing through the main servers in the US which are subject to NSA, so which I'm sure you're aware of. It's, again, digital sovereignty issues. I'm sure it's facing the same situation. Look at Afilias. They moved their head office out of Ireland back to the US for a number of reasons.

I guess how do you address that issue? I know you dealt with China and the UK. Is there a similar kind of situation where there's scrutiny of and potential violation of people's privacies?

UALAN CAMPBELL-SMITH: Okay. So, a few things there to address. Thank you for the question. I think the point about US and a lot of Internet traffic going to the US is obviously a massive concern of a lot of countries. The ICANN reform in 2016, for example, is kind of symbolic of those pressures, but also how – I only learned this at this meeting, which is why it's great, but that

ICANN is also subject to Californian laws as far as I'm aware. So, there's all these issues with how do we have a global Internet that isn't subject to any territorial jurisdictions and I don't think that's a problem that's going to be solve anytime soon.

In terms of global data flows and privacy, a quote in Bruce [inaudible] book on data and global Internet flows is that often people use that as an example to kind of … They use it as an example to kind of advance the cyber sovereignty movement in a way. It's kind of a good excuse for why we need greater domestic control and I think that's kind of a dangerous prospect. I think, obviously, Internet privacy is really important but that's why we have GDPR and these sorts of regulations. So, I think it's not as much of a concern but I definitely think that that will be an important part of national security policy and how we get around that.

UNIDENTIFIED MALE: Thank you for the interesting topic that you presented. Because you mentioned four pillars. I was wondering if censorship is also part of the cyber sovereignty and how do you see the data localization because some countries still use the data localization policy where maybe we see it maybe from the legal perspective where we found that the server, if it's located in the country, it means it will be matched with … So, the [manuals] or the hardware is there, so we feel it's safe. We feel it's still within our territorial, but apparently maybe not necessary. So, how do you see this as relevant data localization policy? Thank you. [inaudible] question.

UALAN CAMPBELL-SMITH: So, if I understand correctly, I think it's important to not confuse data localization with censorship. I think just because data localization and it's stored in servers within a country doesn't mean that that entitles the government to go through that data or monitor it or censor it. So, I think in the case of China, that is part of the reason it is censorship, that it's domestic, but it's also for external interference, so to protect against other countries interfering critical, national infrastructure means it's a bit safer, but I don't think that data localization always equals censorship. And what's the second question? Sorry.

UNIDENTIFIED MALE: Sorry, the question maybe is mixed, but totally separate. First one, do you consider that censorship is part of cyber sovereignty? That's the first one. Sorry, maybe it was fast [inaudible]. Then, the other one. Do you think that the localization policy is still relevant for this space? Because we often people from the legal team [inaudible] rather than maybe from technical perspective or maybe it's also maybe, I don't know, national interest not always about censorship and so on. But maybe if we [inaudible] the data, if the server is not there, we sometimes maybe a little bit don't trust the interest of the foreign company who actually has all our data and so on. Maybe this is the question.

UALAN CAMPBELL-SMITH: Okay. I think I focused on the UK because the difficulty we're talking about cyber sovereignty is that it doesn't really mean anything. In all the academic literature, it refers kind of specifically to a case [inaudible] China where the government owns or kind of controls a portion of the Internet. So, I think in that sense, to say censorship is always a part of cyber sovereignty is true in most cases because the way that China justifies it is not, "Oh, we want to censor the Internet." That's not how they say it. They say it by saying, "We don't want other countries interfering with our affairs. We don't want our security being undermined." But that's no different to … They're saying that which is kind of then also allowing for online censorship, whereas if you compare it to the UK, it's saying that we're still going to protect national security in cyberspace, but it's not our cyberspace to be censoring, if you see the difference.

So, I understand the question because it is confusing cyber sovereignty, sovereignty in cyberspace. They kind of all mean different things and how they interact is a case-by-case basis, if that makes sense.

The second question about data localization, I think that's a big debate and a matter of opinion [inaudible] case-by-case basis, but the fact that GDPR has just come into effect and mandates safe storage and storage within the EU kind of shows that clearly it's on the top of priority of most governments at the moment.

DEBORAH ESCALERA: Thank you. You had a question?

UNIDENTIFIED FEMALE: No. Actually, I think the last two questions, your answers, I also wanted to point out first that … I wanted to ask you what you mean by sovereignty but you already answered that. Then I think this balancing act between a global Internet and sovereign interests sounds impossible, because you either go … And China is the most radical example but you also have other examples of [attempts] to create a state of sovereign Internet, be it content-wise like Russia does [and Turkey].

So, I think I will just repeat the question. How can global Internet with the fact that information is rooted in different places, how can you have sovereignty and global Internet and not do what China does, basically?

UALAN CAMPBELL-SMITH: Okay. Thank you for that. Like I said, this definition of sovereignty doesn't put justice to 400 years of political theory on the concept of sovereignty, so it's really complicated, it's contested. It involves a lot of different factors and it's evolved for 500 years and so now how it evolves further with the Internet … It always uses an example of how globalization is decreasing sovereignty because the Internet is everywhere. So, I agree it's a really tricky issue, probably not one that can be handled by a master student in [inaudible] presentation, but hey, I'll give it a go.

I think how we're going to manage sovereignty and a global Internet, I think goes back to the way the UK kind of phrases it is that cyber

sovereignty shouldn't happen. Nobody should own the Internet. It's a free, open, borderless Internet to use the ICANN lingo, or something to that effect. But I think it's really important to define the ways in which sovereignty is undermined through cyberspace.

So, there was a book published by NATO and some lawyers called "The Tallinn Manual on International Law Applicable in Cyberspace." Heavy. The section on sovereignty kind of talks about how loss of life through cyberspace is undermining sovereignty. So, if you use your computer to kill someone in another country, you're undermining their sovereignty. But I think that it definitely has the potential to go a lot further than that. You can destroy critical national infrastructure. You can take hospitals off the grid. All these things are possible. So, I think there is a lack of general Internet consensus on where is our sovereignty in cyberspace and I think it's important to discuss it and define it because that's how we can say whether Russia interfering in an election, is that undermining our sovereignty or are they just propagating disinformation on the global Internet? It's difficult.

DEBORAH ESCALERA: Thank you. Are there any further questions? Thank you for an excellent presentation. That concludes our presentations for today and for ICANN 63. I'd like to thank our audience members for joining us today. Thank you so much for your support. That concludes our presentations. You all did an excellent job. Really good job. I just want to remind you that all the presentations are embedded in the schedule, so you can go back and take a look at all of them.

Tomorrow we have our photoshoot. So, we're going to meet at 11:00 at the registration desk. I know there's a couple—

[END OF TRANSCRIPTION]