MONTREAL – NextGen Presentations
Wednesday, November 6, 2019 – 15:15 to 18:30 EDT
ICANN66 | Montréal, Canada

UNIDENTIFIED MALE: Those countries are representative of the youth that responded to the survey.

MODERATOR: That is a very interesting presentation. Congratulations and thanks for that. [Leza Rainbow] from Kenya CT Action Network and I was a NextGen and then a NextGen Ambassador, now a [inaudible].

It's very interesting that you find that Millennials have less usage of IUT devices than the older generation. Did you find any insights of why the statistics reflect that?

UNIDENTIFIED MALE: No, I didn't, and that's an interesting finding that I don't really have an answer to. I think part of it is due to the fact that Millennials might be more educated on some of the risks and for that reason, they use them less. Another thing could be like financial barriers to accessing these devices because a lot of them are. IUT is certainly kind of a nacent state and a lot of these devices, for example, Apple watches or Alexas, they tend to be fairly expensive so it could be that as another potential reason as to why there's less usage amongst Millennials.

MODERATOR: Okay, one final question, Arjun.

[ARJUN SANYA]: I'm Arjun [inaudible], NextGen Ambassador. I was just like to ask, so those recommendations were drawn out of the results you got from the sample because from what I got and from what you explained, you had a fairly amount of answers but only from one country so up to which point do you consider the answers representative of the greater population, which are the youth, and if you make such a difference between regions you surveyed?

UNIDENTIFIED MALE: Okay. So do you mind repeating the question? Is it that do … Do you mind repeating the question?

[ARJUN SANYA]: Sure. So my only question is you made several recommendations, and are those recommendations based on the sample results you obtained? And if so, do you consider that the results from the sample are representative of the greater population or did you extrapolate it up in some point in your research, the recommendations you wanted to do?

UNIDENTIFIED MALE: Okay, two kind of questions. The first one was I don't think the recommendations we made were ones that were … Okay, I don't think the respondents we surveyed were representative of the sample. I do think and the recommendations were partially drawn from or inspired

by the responses we got from our survey. Part, some of the recommendations were candidate specific and some of them were more general standards.

MODERATOR: Okay, thank you Arjun. We are moving on now to our next presenter, Diler Cavdar. Diler.

DILER CAVDAR: Hi, everyone. My name is Diler Cavdar and I am going to be presenting on the top five elements that should be included in privacy policies.

So first, a little about my background. I'm from New York City and for my undergraduate degree, I studied English education at New York University. I am currently a third year student at Berkeley Law School.

So last semester, I participated in my school's technology law clinic and in my work there, I co-wrote a model privacy policy. So while doing that, I worked very closely with a lot of policies and a lot of different industries and I gained my own perspective on what I thought some essential elements of a privacy policy are. So a few quick disclaimers, different policies or industries may already have some of these elements or they may need these more than others. Second, policies need to be at the minimum compliant with local and national privacy laws, as well as a GDPR if it operates in Europe.

And I do want to note that this presentation is based on my one semester of work closely with these policies and I am coming at this

from a more humanities background as opposed to a technical background.

So my five elements are: appropriate and specific data retention guidelines, limited data collection, specificity of the third party that data is shared with, explicit user rights of their data as well as readability, and a common theme sort of weaving these all together is transparency. So I want you to keep that in mind.

So first, appropriate and specific data retention. The issue is that businesses might retain user data longer than they need to and they might be ambiguous about the timeline that they actually keep their data. So they won't say. They won't be specific about it.

So for example, we have T-Mobile and Craigslist here who say that they retain your information for as long as they have a business need or purpose. So what does that mean? And then we have Venmo who takes it a step further and says that they keep sharing your information even after you're no longer their customer. And then Snapchat doesn't even promise that deletion happens within any timeframe and they may keep your information in backup for a limited period. And again, we don't know what that means.

So a solution is that businesses need to specify the actual number of days that they retain your data as well as whether there are any variances. And then, of course, you may deactivate or delete your accounts so businesses would specify how long they keep your data in those situations and they should keep in mind what happens if the user returns. So maybe with Facebook, you may leave and then come back,

deactivate and come back, and you may do this in other sort of websites as well and it might vary based on the website.

The business would also provide an explanation of how they got to this number and they should commit to not sharing your information with third parties without your consent. So a good example, actually, Facebook does have some good examples. First, they say that they store your data until either it's no longer necessary to provide their services or until your account is deleted. So if you delete your account, your data should be gone. And second, they give two specific examples of when, of numeric examples of when they delete certain aspects of the data that you give to them such as the log of your search or your ID information. Whether or not these two numbers are good or not, I don't know. But at least they are provided.

Next is limited data collection. So our issue here is that businesses may collect more data than they actually need to carry out their business purposes. So this can manifest in ambiguity. So for example, Twitter, they collect your tweets. Okay, that makes sense. They collect content you've read, liked, retweeted, also makes sense. But also other information. So what does that mean, right? It could mean anything unless they specify that further.

And then Instagram, they also collect a lot including our mouth movements, our battery level, our signal strength, and it's interesting to think about how does that equate to me scrolling through my Instagram feed? They also collect the actions we take, again, very ambiguous.

So solution, of course, they shouldn't collect more than they need. But a way to keep them accountable here is that they should specify the purpose of each piece of collected information. So for example, Etsy specifies that they collect your physical address for the purpose of you buying something and having it shipped to you. Otherwise, they don't need to collect this from you.

Second, Airbnb. Airbnb distinguishes between information that is necessary to collect and information that you can choose to give to them. And again, it provides an example that they specify why they would collect your address book contacts, which is to let you invite your contacts to use Airbnb.

Third, specificity of the third parties that data is shared with. So businesses may share your information with third parties without specifying why or without specifying who they are sharing your data with. Even if they do specify this, these lists may be incomplete. So a quick example, [Sophie] says that they share your information with third parties which include but is not limited to that list. So that language invites them to share your information with whoever else they feel.

So the solution is that businesses should specify the categories and specific names of third parties that they share information with. This list should be exhaustive and it should also identify the information shared with each party because sometimes not every party needs all of your information, right? It'll vary based on what use they're giving to this business.

So we have Reddit. Reddit says that they don't share your information unless one of the specific following circumstances applies, and then we have T-Mobile and Spotify which both provide specific examples of if you do a certain action, they will share your information with a third party in order for you to achieve the specific purpose outlined in those examples up there.

Fourth, explicit user rights of your data. So businesses may not be transparent about the rights that you have about your data with their business or they may not give you many rights at all in regards to your data. So a solution here is, first of all, the privacy policy needs a section dedicated to user rights. Users need the ability to devote permission for them using their information. Users should be able to correct, update, delete, deactivate their accounts. They should have access to all information that a business has on them and that includes information that a business gets about you from a third party. Users should also be able to transfer their information and have the right to give consent to their information being shared.

So this is a base example, but T-Mobile lets you access and modify your contact information. This is something that all policies probably already have. But this should be sort of done at a larger level as well. And then Apple provides you with access, including a copy of your information and hopefully this includes information that they got about you from third parties.

Okay, so my final element is readability. So often, privacy policies are too long. They may have no table of contents, no summary. They may

have difficult legal or technological jargon and use no headings. So Apple doesn't have a table of contents and then Etsy here talks about having certain information using TLS which is Transport Layer Security but then they don't define what that means.

I had not heard nor understood what TLS was until I started working on privacy policies in the middle of my graduate studies, so that's interesting background to think about.

So the solution is that these policies need to have a summary or table of contents, jargon should be used if necessary, and sometimes it is necessary, in which case they should have definitions. And these policies also need to have a permissible aesthetic which means being a reasonable length, font sizes, using graphics, tables, diagrams. And this is important in order for everybody, all types of users, to be able to read and understand these policies because sometimes it's people who are, perhaps, only have high school degrees, maybe even less than that. Teenagers often use a lot of different services and so we need this information to be accessible to a wide audience.

So two examples. Etsy, they do indeed have a table of contents and I believe that that also has hyperlinks which is also helpful. And then T-Mobile indicates that they use web beacons and then they also define what that means which is important.

So in summary, I know I use a lot of examples from businesses that are out there, some positive, some maybe not so positive. And it is possible then in some cases, I didn't have the full context which may have been available in the rest of the policy but it's also possible that that didn't

actually exist in all the policies and I want to reiterate the importance of transparency and this is important because information should be accessible to a wider audience, like I mentioned, to all types of users regardless of their technical or educational background.

More specific information should be given. So that leaves less room for ambiguity on the part of the business. Information should also be better protected and the reason that this is all important is that it all goes back to accountability, right? So businesses then have to be accountable with what they do with your information because they're making all these promises to us.

So one final thing I want to end on is I started thinking, "Well, what about ICANN's privacy policy?" and I was in a meeting this week here at ICANN where someone who is not NextGen said casually during a meeting that ICANN doesn't have a policy, a privacy policy, and I was, let's say, surprised. So I looked into it and I did find a policy from 2012. So if anyone is wondering, there is I guess, perhaps, an un-updated policy that is out there for ICANN. Thank you for listening.

MODERATOR: Thank you, Diler. Very well done. Are there any questions from the audience?

MARIANA MARINHO: I wanted you to be specific when you say that ICANN doesn't have a privacy policy because I'm aware that we do have some, especially for our website. We've updated recently with GDPR, all of our terms of

service. I'm also involved with updating our privacy policy and terms of services for a lot of our applications, for instance, the fellowship application, the NextGen application, [inaudible] was involved with that where we've been updating a lot of stuff. We've been working on a lot of GDPR work and we take this very seriously. Thank you.

DILER CAVDAR: Yeah, thank you. So it wasn't myself how made that comment but I was in a different meeting this week at one of the sessions and someone else, someone who was not a NextGen member – I don't recall who it was – they said that ICANN didn't have one and then I was similarly confused because I was like, "What?" So I looked into it and I found the policy. The one that I found online, perhaps it wasn't the most updated one. So I definitely found that the policy exists but I guess this shows that perhaps not everybody is aware that it's out there.

MARIANA MARINHO: And as you guys are aware, ICANN is very, we have many groups and many services, and it's, perhaps, that some of them have been updated and some are in the process of being updated. But this is definitely something we're working towards.

DILER CAVDAR: There are a couple of online comments from Mark to everyone, "Diler is an amazing speaker. What a great idea to end with ICANN." And from Eileen Kwipoya, "Nice presentation."

Okay, do we have more questions?

SEUNG JAE LIM: Hello. Seung Jae Lim from South Korea. Thank you for an amazing presentation. I have a question about the readability part. If I remember correctly, terms and conditions in corporate law – was it? – it's kind of for efficiency, right? Efficiency is quite important in this area so one question I have was if we, in order to make the readability be better, there may have to be some more inclusion of information just like you said. But actually, that might be going against the efficiency area of corporate law so like, and in addition to that, if you add more information, maybe the corporates could try to kind of transcend – am I using the word right? – their responsibility to the user of the service, maybe? So how should we deal with these kind of potential problems?

DILER CADVAR: Yeah, that's a really great point and I didn't have time to say it during my presentation, so I'm really glad that you did. It's such a difficult balance. It's so hard because on one hand, you want to be as inclusive as possible and have as much information as you can for the users to read them. But on the other hand, that goes against keeping it concise and it is hard. And I'm not quite sure what the answer is. The only things I can think of at the top of my head is maybe doing studies on thinking about what is maybe the most efficient length that a privacy policy should be, so what is a length that most users will read it and actually read the whole part of it or can there be a section that is moreso

dedicated for users where the most important information or [valid] information is at the beginning.

And those are the only two things I can think of right now, but I definitely want to recognize that it is a really hard balance.

[DAVID MARGLIN]: David [Marglin], North America, I guess United States. Hi. I love your presentation. I was really curious about a couple things, like one, what about when data is coming from a third party and connecting, and how much transparency? You didn't mention that. You talked about data going out to a third party. And then I guess a related question I'd like you to riff on a little bit is like, how tricky do you think a privacy policy can be around the issue of, so like you're working with Facebook or whatever, we're corresponding, transparency about sharing the data but the what we need to do to work with a partner in that instance because so many companies are working with each other and then data can go over to them and then back and whatever. So just what your thoughts are on that.

DILER CAVDAR: So for your first question, do you mean if a third party voluntarily gives a business data about you without that business asking the third party about your data?

[DAVID MARGLIN]: Well, oftentimes, when you are drafting a privacy policy, you're saying you're concerned about the company is sharing your data with a third party. But oftentimes, you're going to get data about that person from a third party and you didn't mention that at all. Like, hey, you signed up for your service and we're going to go, and if you signed up with Facebook, we're going to get information from Facebook about you, right? Now what we're going to share with Facebook. That you've got transparency but what about when Facebook or there are a lot of other instances where that might happen, telling the user, "Hey, if you sign up for our service, we're going to get information from that third party."

DILER CAVDAR: Yeah, so if I did understand correctly, I think that if information is taken about you from other third parties, then that should also be disclosed. So I think, again, the importance is transparency. So if you're using a service, you should know that this service is getting information about you from elsewhere. And could you repeat your second question, please? I'm sorry.

[DAVID MARGLIN]: Just the question has to do with when I read these privacy policies, it seems like as transparent as they might or might not like to be, they're often glossing over the way information is roundtripping back and forth or who it's being shared with. That whole issue in a privacy policy, do you think, does it require more scrutiny? Or have you seen it? You've obviously read 20, 30, how many privacy policies have you read for that?

DILER CAVDAR: Yeah, at least 20 or 30 I think. I think that, again, assuming I got your question correctly, if a business has to share information with a lot of different third parties, then I think a good move could be to specify what information is being shared with each of those parties. Yeah. Is there anything else that I left out there? Okay, thank you.

MODERATOR: Okay, we'll take one final question. Then we need to move on to the next presenter. Thank you.

STEFAN FILIPOVIC: Stefan Filipovic, NextGen Ambassador. So I have a question relating to collection and possession of personal data. A majority of businesses, when they possess personal data, then they don't rely on update and consent from a user, but they rely on legitimate interest. To be more precise, they rely on GDPR's article 61F which says, "Well, if your business has legitimate interest to possess personal data, and that prevails over the right to privacy of a user, then they can do basically whatever they want."

So I am wondering, have you maybe further investigated if those businesses have conducted legitimate interest assessment?

DILER CAVDAR: Could you elaborate what a legitimate interest assessment is a little bit more? I'm sorry, just to make sure.

STEFAN FILIPOVIC: Well, in order to rely on 61F GDPR, which basically says you can possess personal data if you have a legitimate interest, you need to conduct that test. That's a requirement under GDPR in order to prove your accountability and other stuff. So I am wondering have you maybe engaged in conversation with them to ask them have they contacted because I contacted Spotify and they never got back to me.

DILER CAVDAR: No, I didn't. I haven't really engaged with these tests at all. Or that wasn't a part of my semester that I really thought about, so that's an interesting thing to think about. Yeah, thank you.

MODERATOR: Okay, thank you so much. And just FYI, Mariana has provided the link to the updated ICANN privacy policy. It is in the chat and this transcript is available and will be available on the website. Thank you so much. Very good.

Okay, let's move on. Our next presenter is Josh Gold. Josh?

JOSH GOLD: Thank you. Bonjour, [speaking French].

Thanks a lot. I'm especially grateful to those who are not in the NextGen program who are here watching us, probably behind me but also around the table. It really means a lot to us to know that people from

the community who are very engaged in these things are also willing to listen to us and hear our own ideas. So thank you.

My name is Josh Gold and I am currently a research assistant at a laboratory at the University of Toronto's Monk School of Global Affairs and Public Policy that's called Citizen Lab but I would stress that I do not speak in any way for Citizen Lab. I'm not here in any official capacity and nothing that I should say should be taken to be from Citizen Lab. Let me make that very clear.

So my goal in this presentation is to showcase some of my thoughts and recent work on, well, what I've been doing in the past sort of year and how it relates to ICANN.

Just quickly about me, actually, I had the honor – as Arjun spoke, I had the honor of even helping with that report that was prepared for Youth IGF Canada. I am born and raised in Toronto with dual Estonian/Canadian heritage and citizenship, and I've always been interested in conflict and now I'm ore interested in conflict online and in the so-called cyberspace and bigger picture policy estate behavior sort of things in cyberspace.

I'm also on the Board of the Canadian International Council, which is a think tank here in Canada. So let me test this out. There we go.

So I'm speaking here onto a distinction that I see between so-called cyberspace governance and Internet governance, and for me, these definitions are very tough and hard to pin down, and probably don't really exist. But I see cyberspace as an integrated, complex information

and communication system. And the way that that differs from the Internet in my mind, and this might be wrong. This is partly a soundboarding exercise for me, but the Internet is sort of like the book, a book, and cyberspace would be the image or picture, imagination that the reader would get from reading the book. Cyberspace is much broader.

And where I see cyberspace being distinct is that it's a domain in which states are acting their issues of sovereignty in offshore relations, geopolitics, national security considerations. Of course, this is all open to debate but that is my view and understanding. The lines are, of course, blurry.

So we've had a lot here at ICANN on Internet governance but what about this thing that I'm calling cyberspace governance? So I'm going to discuss big efforts in the United Nations toward governing state behavior in this domain and in this space, and I know I will note that the UN is also very involved in Internet governance. The [inaudible] 2006 meeting came out of that and the IGF is, I believe, done under UN auspices.

But in terms of states and states trying to work out how the rules of the road will form in cyberspace, the UN also has some specific groups that have opened up. And this is sort of based on the understanding that the lack of a clear, widely accepted rules or norms for state behavior in cyberspace contributes to ambiguity and impunity which can be taken advantage of by various states, state-linked actors and other groups to behave maliciously and threaten stability and security. In many cases,

established rules already do apply in cyberspace. For example, the Tallinn Manual which is a sort of consensus of several international legal scholars working out of the NATO Cooperative Cyber Defense Center of Excellence located in Tallinn, Estonia has declared and has come to the conclusion that international law does apply, or laws of armed conflict do apply in cyberspace and in cyber conflict.

And I'll speak later to the UN also agreeing that international law applies. But new technology does ultimately pose new challenges and new norms and shared understandings are needed in this space and that's been generally accepted as well.

The call for cyber norms actually was started by the Russian Federation in 1998. Russia called for a multilateral instrument to contain and mitigate threats from information weapons and information warfare while pushing for the ability to retain control over these information environments. So they, the Russians really came up with this idea of information as a security threat, which is maybe not surprising given certain events recently.

But the West from its inception and continuing today, the so-called West, A.K.A. what I see as more democratic minded states are a bit nervous of this, seeing it as a reflection of the desire for governmental control over the free flow of information. And these different approaches to information security have led to disagreements between different kinds of nations, different kinds of states to agree on norms and these disagreements continue today.

So in 2004, we had, as I mentioned in 1998, the idea was first tabled and then in 2001, Russia suggested a working group and by 2004, there was a working group called the GGE, the Group of Governmental Experts that was tasked within the UN to consider threats in information security and cooperative measures, and to study the issue in general with really the mandate to promote peace and stability in the state use of ICTs or Information Communication Technology.

The GGE has had five meetings since 2004 and consensus was reached in 2010, 2013, and 2015. Notably, in 2015, the states in the GGE, which is a small group. I'll say it started as 15 states and now it's 25 states only. But it's regionally distributed and yada-yada. But in 2013, the GGE states agreed that international law does apply in cyberspace. And in 2015, they agreed upon 11 norms, principles and rules for state behaviors in cyberspace. And this was endorsed, importantly, by the United Nations General Assembly, so by all states.

In 2008, oh, jumped ahead. So in 2007 actually, the GGE failed to issue a consensus report and was sort of stonewalled between certain countries and other countries bickering over certain key issues, to put it very ambiguously like that. And in 2018, there were two proposals put forward to move this process ahead. The United States spearheaded a proposal to start a new group of governmental experts and continue that process as was previously started and the Russian Federation put forth a proposal to begin something called an open-ended working group or OEWG, which would be more expansive and include all states in the world and I can later get into maybe reasons why Russia might have wanted that. But they said, and this is a fair argument, they said,

"Well, we should get all the states on the table. It's more democratic if everyone is deciding and we come to consensus all together." Of course, that has its own implications as well.

So now – next slide – the Open-Ended Working Group, and if you'd like, feel free to scan this thing. I forget what article it links to, but it's helpful I'm sure.

The Open-Ended Working Group, the first substantive session of it occurred from September 9th to 13th in this year, so just recently. And this was, I don't like to use the term historic but it did, it was the first-ever global meeting on peace and stability in cyberspace, so the first time that all states in the world got together to specifically discuss these issues.

And if I had more time, I'd speak a little bit more into some of the nuances and drama that happened behind the scenes maybe, but the most important things or one of the most interesting things for me was the seeming split between states emphasizing state sovereignty in cyberspace, noninterference in political affairs and sovereign equality, and also between those states who emphasized more of an open, free and secure cyberspace. Those are the three, open, free, secure versus more of a focus on sovereignty and controlling the space.

So the group, the Open-Ended Working Group, actually saw consensus on many things including they reiterated that international law applies, for example, in cyberspace though some states, notably China, questioned how it might apply in cyberspace and so that question differed. And there was lots of other things that were productive out of

this meeting, for example, focuses on capacity building in developing states and cooperative measures or confidence building measures, CBMs, as they're known in the international relations jargon.

But interestingly, there were also calls as I sort of briefly touched on, there were calls by several states within the group to assert greater governmental control over Internet government institutions themselves and ICANN was also specifically mentioned as a group that some states, notably Iran and China and Russia mentioned that they might like to have some more control over.

And this gets to an interesting issue in my mind because to me, the way I've understood the multistakeholder approach, it's very important that Internet governance stay neutral from states and from political actors, geopolitics, political sort of leanings and I guess national interests. And that also relates to one of these much flouted norms out of the Hague, out of [inaudible] [Dennis Broders] that's now been accepted by the Global Commission for Stability of Cyberspace and a whole bunch of other institutions called the norm for the public core of the Internet, which really says that the public core of the Internet, so these institutions and protocols and DNS really have to stay neutral, neutral from politics and conflict and state level bickering, the idea that politics and technology should stay separate.

And so I will conclude with saying that in ICANN, we have the Government Advisory Committee and I was hoping to understand a little bit more about how it works but I think I'll need some more time. But really, it is the voice of governments and government organizations

in ICANN. But it doesn't have any binding voice and this is an interesting organization because it has some work to do in this space and might face some future challenges from governments who might want to assert more control or threaten the existing structure and model of how ICANN functions or Internet governance institutions function.

So I just have some concluding thoughts on the screen. I've run out of time, unfortunately. I've run out of time, but this is sort of what I've been thinking about and why I'm here at ICANN. And thank you all for listening. And I look forward to any questions.

MODERATOR: Thank you so much, Josh. Do we have audience questions? Okay, we'll start with Abdeali at the end.

ABDEALI SAHERWALA: I'm Abdeali Saherwala from York University, Toronto. So I did a presentation yesterday regarding social media and infiltration of foreign entities. So how do you think that that would be connected with government wanting to have an open, free Internet yet having foreign entities with malicious intent to infiltrate the populations' thoughts, ideas, and even basic facts like up is up and down is down?

JOSH GOLD: Thanks, Abdeali, for the question. I'd like to, I guess, stress that I didn't, it wasn't my intention and I'm not saying this is how you interpret it but just to be clear, I'm not saying that there's a black and white picture

here. It's not like there's good states and bad states going at it. It's very blurry and there is very good reason to assert more control over information and to worry about even in a perfect liberal democracy, to worry about certain kinds of information such as child pornography or terrorist content. And so these issues are a little bit more complicated.

But yeah, the general question of information warfare as you talked about yesterday, or what I see as information warfare, is an interesting one and it's interesting just that some of the states who have been tied to or to whom information warfare acts have been attributed to were actually the ones thinking about this many, many years ago before other countries. And there, it's tricky because if we were totally cut off or if the U.S., let's say if the Democratic National Committee or Convention was totally cut off from Russian Internet, they might have been safer and if they had blocked certain things or had more control over the space in that way, they might have been more protected based on or against what happened. But I don't have an exact answer for you, I think, very complicated questions.

MODERATOR: Any more? Go ahead.

JAEWON SON: Jaewon from Korea and I'm so glad to be your ambassador. And I was glad that you have mentioning about the United Nations. As the person who is [inaudible] the United Nations, I believe it is really important to have the collaboration between UN and the ICANN and I was wondering

what your thoughts on how should the ICANN more contribute to the work with United Nations in terms of desterilization and STDs and all of those really important, but it seems like there is not many things going on with those and then I was wondering how you link to those ICANN's work with the United Nations, how we work.

JOSH GOLD: Thanks. Thanks for the question. I'm very happy that you're my ambassador as well. It's a pleasure.

Well, for me, what I see as very important is the idea that while Internet governance institutions stay separate of this political stuff and state level stuff, that they also have a channel of communication between one and the other to understand and work on issues that are relevant to both and that there's a way of communicating, and that's what I see in the GAC, the Government Advisory Committee, in terms of governments get to put forward what they're thinking and what their concerns are.

Now they do it, the GAC is, as far as I can understand, they're communiques are non-binding so they make recommendations but they can't actually have any power to influence the ICANN community and what ICANN does. And I look forward to learning more about the GAC through meetings here and so on.

But something about at least having a channel of communication open, some sort of, I would call that a confidence building measure even, that

allows the two sides to talk, understand what the issues are and then work it out in certain different ways.

And I don't know personally how sustainable ICANN's current model might be moving in the long run as states start to increasingly pay attention to more Internet issues and what their priorities are.

MODERATOR: Okay, any other questions? Okay, thank you, Josh. Very well presented.

Okay, we'll move on to our next presenter, Kush Bhargava.

KHUSHAGRA BHARGAVA: Hello, everyone. I'm pursuing Masters in Computer Science at University of Southern California in Los Angeles. Being a citizen of India and as student at the United States, I'm being honored to represent both the countries on such a prestigious and global platform of ICANN.

My presentation is about the market of online social influence. It's the cause of a butterfly effect. Internet being a platform that is being accessed by billions of people across the world, my presentation is about how one malicious bad actor on the Internet can have such a negative impact on the lives and decisions of billions of people across the whole world.

So these five logos represent the places that I've worked and studied. These places have helped me understand the importance of Internet governance from the perspective of multiple stakeholders, including academia, the government of India, as well as the private sector and

technical community. Why is this important? Because since we are transitioning from a multilateral approach to a multistakeholder approach, it was very delightful and important to understand the perspective of different stakeholders when we talk about Internet governance, their expectations, their advantages and their limitations.

So we'll start with the first, this image. Data never sleeps, as we all know this very famous quote, data is the new oil. We see how much data is being generated every minute of the day. Facebook users are liking more than 4 million posts every day, 350,000 tweets are generated every minute, 300 hours of YouTube content is being generated every minute. So we know how much data is there on the Internet and how much that can affect the opinions as well as the decisions of various people.

But what does data revolve around these days? Currency. As currency, the more currency we have, the more influence we have on the Internet and the currency that is there on the Internet is these days more about the social currency that is likes, followers, shares, views, comments. This makes you more socially popular. You build a social reputation and when you have a reputation to maintain, you try to boost that reputation to be more influential on the network.

But what is the effect of building that social reputation to boost that social reputation? Because the better your reputation is on the Internet, on the network, the more visibility you have on the network and the more the visibility you have, the more you echo on the network, the

more your generated content echoes, propagates, flows on the network, the more people see your content on the network.

But how does this effect of content propagation on the network affect us? How does this affect the people across the whole world? So this same image we have about the data on the Internet, but what revolves around this data on the Internet?

Buy Instagram follows, these are some ads that you see. These are some domain names, domains that are existing on the Internet. Buy Amazon reviews. Buy reviews on Yelp. Buy Facebook likes. Buy Twitter followers. Buy 10K YouTube views, you will get 10K free. Buy [wine] followers.

So as we see this data that is generated organically might have some inorganic behavior as well. This is not something that is very naturally happening on the Internet, but how does that inorganic behavior affect us? We are generating. We are having a web of noncredible content, which adversely affects the credibility of e-commerce networks that rely on user ratings and reviews for product recommendation. News feeds of various social networks, Google search engine, Yahoo search engine and consequently, the recommendations of YouTube videos as well.

And that inorganic behavior affects the opinions of the masses. It has a cascading butterfly effect on the real world [evens] including, let's say, U.S. presidential elections, prime ministerial elections of India, product choices that you have on different e-commerce websites, Amazon, eBay, religious and regional conflicts that people have such inciting

content that is being generated on the Internet that might be the cause of some inorganic behavior that people have been tending to follow to boost their social reputation.

So my research over the past few years has more been focused on Twitter and how Twitteratis have been having some mischievous follower account. Their followers are not always generated organically. It's a proposed methodology to identify the behavior of Twitter users that opt inorganic followers, why are the services of the black market websites that we just saw as the advertisements of these websites.

We proposed a framework to identify the users with many [inaudible] follow account and also project an estimate of real follow account which is [relevant] to this inorganic behavior and so that the advertisers, the Internet end users, can understand what is real and what is not.

So what are the constituents of this framework? Temporal signatures, neighborhood of user. When we say temporal signatures, we are more focusing on how a user profile is evolving over time. You can gain 10K followers in a day but the timestamp will be able to tell that you gained all those 10K followers in one day which is slightly fishy. So we are focusing on the temporal [inaudible] of a user profile.

We're also focusing on the neighborhood of a user. We are taking different features of a user profile, in which language is that user tweeting, how much frequently the user is tweeting. Is the Twitter from, let's say, [inaudible]? So the user should have characteristics more similar to that region, to the users of that region.

So we are taking the neighborhood of a user and trying to figure out what all users are the outliers in this network and that outliers might have some inorganic behavior which we need to tackle.

We are also estimating the untampered follow account of the user which is suspicious. Using the temporal and static features of the nearest neighbors of the affected Twitter user and trying to repair the credibility of the user on the network.

So these are some of the features that we took, language of the tweet, presence of a profile pic, number of tweets, number of friends, follower gain, how much followers are being gained every minute or in a day, when was the Twitter account created. So all these are some of the features that we took to understand the behavior of a Twitter user.

So these are the final results that we got using our framework. We were able to detect Twitter users with inorganic followers with a precision of 98% and also calculate, predict the untampered follower account of a Twitter user with slightly decent accuracy of 84%. This is the link to our research and I also put a screenshot of the research paper that we published in ACM conference.

So what next? We are talking about inorganic behavior. My research was more based on one social network, but is one social network enough and even we are only tackling the after effect of malicious abuse of a newly registered domain. We are not taking any precautions. It's only preventive measures that we are taking. We need similar tactics for all other social networks for Google newsfeed. We also need tactics

for e-commerce websites to counter inorganic manipulation of these social currencies that we are talking about.

Many social network companies are already trying to do it. Facebook, Twitter have been trying to take different measures. But are they enough?

What's more important is to initiate a policy discussion on the effect of such black market services on the Internet, and the extent to which it hampers the goals of online trust. I have been looking at ICANN's initiative and there has been an initiative called Registrar Accreditation Agreement, RAA, that you call it, and it focuses on giving a report of the abuse of the different newly registered domains to the registrar so that they can take action against them.

But that is also towards preventive measures after you know that some domain names are being abused. You're trying to prevent that. But there should be some precautions that we need to take to ban the existence of A-list black market services on the Internet, maybe check, put a more stringent check on about how we can figure out that the domain name ownership whether it's being changed in less than ten days or 15 days. So that means if the ownership is being changed very frequently, maybe there is some malicious activity that might be going on, on that domain name.

So yeah, this was the gist of my work that I did over the past few years and I'm up for questions.

MODERATOR: Wow, really fascinating research. Okay, do we have questions from the audience? Okay, we'll start with you.

[DAVID MARGLIN]: Loved your presentation, thank you. Do you think there's a way to shame people who pay for all these followers? So you can do 90 or someone can get 98% accurate figuring out that somebody with 160,000 Facebook followers who are all in the "stans" – Kazakhstan and whatever – are not real. Would there be some way to then disseminate that information or have their Facebook page light up or their Twitter page light up so that other people looking at it could go, "Yeah, 98% likely these followers are bought and paid for by some black market site," and that would be one way of taking care of the problem.

KUSHAGRA BHARGAVA: Yeah, definitely it's very good way of tackling this issue. We can definitely have, let's say, a kind of a chrome plugin or different kinds of browser plugin when you open your Facebook newsfeed or a Facebook page through that browser. That browser can run our framework in the background and give a kind of light that you're talking about which can give a signal whether that user is more into gaining its social currency or social reputation through black market services or the follower account is actually real.

But my reason for presenting here is not about giving any kind of preventive measures because these are the things that, now, the damage has already been done and we are just trying to flag the

damage that this is a damaged profile, this is a clear profile. We should try to at least take more precautions such that these activities are not even starting to, should not even start to happen on the network. So my request or my focus is on initiating such kind of policy discussion where we can have a check before assigning newly registered domains to any company or any individual on the network.

ABDEALI SAHERWALA: This was, I wish this presentation was yesterday considering how similar it is to mine. I have three questions. I'll be very blunt when it comes to the questions. So the first one is, okay, for those who do not know the butterfly effect, what is it?

The second question is could your tactics be used to identify bots and trolls on different social media platforms and then eliminate them?

And also, the third question is can your methodologies be used on other social media platforms like Facebook which I intensively badgered on yesterday.

KUSHAGRA BHARGAVA: I'm really sorry. I only remember the third question.9

MODERATOR: What is the butterfly effect?

KUSHAGRA BHARGAVA: Butterfly effect, yes. So when I talk about the butterfly effect, it's more about taking in a general scenario that, let's say, a flap of a butterfly can have effect, multiple effects, a cascading effect on multiple scenarios or in multiple events. So when, butterfly effect in terms of social network or in terms of the Internet, when we are not putting a proper check before assigning newly registered domains, there is a possibility of malicious abuse. When there is a possibility of malicious abuse, that thing is being catered to multiple users across the whole world.

When that abuse is being catered to multiple users across the whole world, their opinions are bound to change and that has clearly affected so many real world events across the whole world, including Brexit, including Indian priministerial elections, including U.S. presidential elections. One post changes the opinions of the masses so we need to tackle the source of the problem. That's why I just called it the butterfly effect because one thing can have a cascading effect on the Internet.

The second question, can you repeat it again? The bots, yeah. So the question is whether we can tackle the bots through this research.

UNIDENTIFIED FEMALE: I do.

KUSHAGRA BHARGAVA: So these black market services are a kind of bot that we consider and when they say that we are going to sell you 10K followers, they have – I don't know if you worked on it – but I'd like to be as, I'd like to tell it in as layman terms as possible. There are different APIs that different

social networks provide, Twitter, Facebook. Through these APIs, you have the ability to post a tweet programmatically, to like or tweet programmatically, to gain, to follow somebody programmatically. So when you do all these programmatically, you can do it in bulk in a second.

So our research is trying to understand the damage done by these bots, but definitely they could be a lot more things done in this research, and yes, definitely I'm looking forward to exploring how we can detect Board behavior on the fly.

The third question, what was the question?

ABDEALI SAHERWALA: The third question was could this be used on Facebook and stuff like that?

KUSHAGRA BHARGAVA: So the general framework, definitely you can use. But our model is more focused on the features that we collect from one social network. So when I say Twitter, the features of a sure profile will be number of followers that the user is gaining. Tweets, the frequency of the tweets, the region from the user that the user belongs to. That might not be the same features in other social networks. Of exam[le, Facebook doesn't have the concept of it's not very popular. The concept of followers is not there. It's more of a bidirectional network where you have friends, you send a friend request and you get back when the user accepts you are connected.

But Twitter is more of a unidirectional network. You follow somebody and you are able to see their content. So there is a need for the friend features that we might need to take for a user profile. So the overall general framework can be applied, but the features have to be different according to different social networks.

[SEUNG JAE LIM]: Wow, very impressed by your presentation. I actually have the question about the e-commerce area. Like if I remember correctly, e-commerce has the characteristic of multi-homing, so basically, the people can kind of choose what kind of e-commerce platform to use, or actually use all of the platforms existing but that means there may be some people who want to kind of misuse the less transparency existing in some of the platforms, I think. So in the long run, I believe the invisible hand will kind of kick in and those platforms will be gone. But in the short run, such kind of dangers may be existing in the market. So what can policy do is the number one question.

Number two question is I believe we're revenue generation of the black markets. Like if cryptocurrency will kick in immediately and what should the involved stakeholders to do in order to minimize the problems that can occur from cryptocurrency?

KUSHAGRA BHARGAVA: Thank you for the question. So when you say that even the e-commerce websites are affected by these kind of activities, we're not talking about what reviews are being affected on one e-commerce website or on

some other e-commerce websites. We are more focusing on different domain names that are existing, which help users to affect different e-commerce websites. So we are more focusing on the newly registered domains which are open to affecting multiple e-commerce websites and not just one. So even if one is transparent, the other is not. Our focus is on finding those bad actors which have acquired some domain name. So that is our focus on.

Cryptocurrencies, I am not knowledgeable in that area so I would not like to comment on that because little knowledge is dangerous so I would not like to comment on cryptocurrencies.

UNIDENTIFIED MALE: So my question here, and take me as a little bit as a motivation question, so you mentioned that the way we might do this would be through policy and reflection on that area. But on the other way, on the other side of the table, you have to think about the way social media works. So black markets arise from the need and from the interactions created on the social networks. So up to a point, they are not illegal, an illegal way of obtaining the followers. So are you really fighting the black markets? Or are you perhaps fighting the way the interactions were created online social media?

And then the question would be shouldn't we be regulating the interactions on the social media platform itself, the way we communicate with each other, the values we create through the online social media rather than identifying that specific problem.

KUSHAGRA BHARGAVA: Thank you for the question. So when we say that it's the need of the users, and because of that, these black market services exist, I might not agree to that because or maybe definitely users need to boost their social reputation and that helps these black market services to grow. But users or a general common man might have so many needs and they be interested in doing so many nefarious activities.

So we might, it's not always right to say that since it's the need of the users, it's not illegal because we need to understand that difference between what is good for the network, what is good for the Internet, and what is not and if some services, some nefarious activities are affecting the opinions of the masses in a negative direction, or in a negative context, I think there's a much important need to at least address the issue with more focus. I'm pretty sure ICANN and ISOC are dealing with this issue. But they have been more providing a kind of direction to the registrars to look at the issue and figure out whether you can do anything about it. There should be a more stringent check on it.

Definitely, the directions should be given to the users on the social network as well. But if a user is given some tools, no matter how much direction you give to a child, a child definitely would like to explore all its options. So I think the work should be done on both the sites and not just one site.

MODERATOR: Okay, [Abdeali], final question.

[ABDEALI SAHERWALA]: During this amazing research, did you find any kind of software that can be used to detect these black market sites or that doesn't [inaudible] yet?

KUSHAGRA BHARGAVA: So during this research, we found more software and algorithms which are promoting these kind of factories and lesser of the software that are trying to prevent it. There are some domain regeneration algorithms which generate large domains, a larger number of domains in a second for you.

Similarly, you have these kind of follower gaining services here just one run command can gain you 100 or 500 followers in a second. So these kind of services were [more there].

We were not able to find any solution for Twitter, but I'm proud to say that my research group only introduced one service, a similar service, for Instagram so we're looking forward to doing more in this domain. Thank you.

MODERATOR: Okay, thank you so much. Obviously, people are very interested in this subject. Okay, we are going to go on to our next presenter, Lukas Bundonis. Lukas?

LUKAS BUNDONIS: Good afternoon, everyone. My name is Lukas Bundonis. I'm a second year Masters student at the Fletcher School of Law and diplomacy studying emerging technology policy.

Before I begin, I'd like to thank the ICANN NextGen program, Deborah Escalera, Dawn McKnight, and several others for giving me the opportunity to attend ICANN66. It's been a privilege and an honor to participate.

My presentation today is titled, "Huawei or the Highway: How the Chinese Telecon Giant is Shaping the Future of the Internet." This isn't an original title nor is it a comprehensive one. I think I just wanted something with just a little bit more punch than usual. Let's begin.

A brief disclaimer, this presentation reflects my assessment and my assessment alone. It does not represent any official viewpoint of the Fletcher School in Law and Diplomacy, the United States government, or any affiliates of either organization.

So I'd like to begin with a comparison of sorts. I pulled a pretty descriptive paragraph of Huawei's overall mission from a white paper on innovation and intellectual property which the company put out this past summer. I won't read the whole thing I might hear some highlights. Huawei has brought network connections to 3 billion people around the world, does everything it can to support, secure and stable network operations in every lace where it operates, including [austere] environments and areas affected by natural disasters. And its vision is

to bring digital to every person, home and organization for a fully connected, intelligent world. So that's [Huawei's] mission. Sounds like a good, noble company, right?

Well, not when you look at its headlines in Western media outlets. These I'll read for effect. Germany's refusal to ban China's Huawei from 5G is dangerous for the West. Huawei consumers want to ignore Trump's blacklist. That just got harder. Huawei's 5G isn't worth the risk and Huawei's five gear might have to go, FCC tells U.S. telecom firms.

This last one isn't western, but Russia and Huawei team up as tech cold war deepens. So I have a concern. At the beginning of the fall semester, I began to design a couple of project proposals around destroying the preconceived Western notions that Huawei is up to something.

I examined the opportunity to conduct mobile forensics on the latest Huawei devices, consulting some folks currently and formerly in government about how best to make that happen. I also looked at what a 5G network looked like if it were both A, owned in large part by Huawei, and B, deployed over an existing telecommunications network in a Western country.

However, I was quite frankly dismayed when I heard the expression "Once they're in somewhere, they're in everywhere" repeated over and over again among the international relations professionals with whom I engaged. Did they think that once machine or network node is compromised, it allows an intruder unfettered access to the whole network? Is computer security completely foreign to them?

So I looked for an alternative argument. Fortunately, my second degree colleague, Priscilla Moriuchi, of Recorded Future was close at hand. About two months before Huawei issued the white paper I referred to earlier, she published her report called "The New Cyber in Security: Geopolitical and Supply Chain Risks from the Huawei Monoculture". In it, she argues that the chief threat emanating from Huawei is not purely a malicious power grab to enable Chinese espionage, but instead, a perfect storm of unintended consequences waiting to happen. I'll unpack that statement a bit further later on in the presentation.

So where did Huawei get its start? Founded in 1987 by Ren Zhengfei, a former deputy director of the People's Liberation Army Engineering Corp, Huawei is at least primarily a telecommunications company, focused [inaudible] days on manufacturing phone switches, Huawei's work of reverse engineering foreign technologies was central to government efforts to modernize China's underdeveloped communications infrastructure, or at least underdeveloped at the time.

Where is the company today? It currently has products and services deployed in more than 170 countries. Its networks reach one-third of the global population. It overtook Ericsson in 2012 as the largest telecom equipment manufacturer in the world, a shortcoming which Ericsson executives are still trying to remedy in their efforts to develop competing 5G technology.

Finally, it boasted an annual revenue of $108.5 billion USD in 2018. If you're wondering what happened between 1987 and 2018, as well as why this graphic focuses on growing Chinese technological threat,

you're not alone. North American companies, government officials and academics are currently scrambling to counter Huawei's rising global market position under two key strategic initiatives around which the Chinese government has organized its foreign policy.

The Belt and Road Initiative, or BRI, and made in China 2025. First, the BRI is China's global development strategy to reconnect old silk trade routes over land and see via infrastructure and development and investments in 152 countries and international organizations. Thus far, these investments have focused on Africa and Latin America, two regions which have already seen a lot of focus earlier on here at ICANN 66, but they include Asia and parts of eastern Europe as well.

Made in China 2025 is destined to comprehensively, or designed – excuse me – to comprehensively upgrade Chinese industry at home making it more efficient and integrated such that it can occupy a leading role in the highest parts of global production chains. Sound familiar?

At this point, I think it's important to reorient you all a little bit. While Huawei has a leading role in both initiatives, this role is not by any means comprehensive. Other Chinese state champions, as they're commonly referred to, are helping advance these initiatives in equal and sometimes larger ways. By [do], its search engine, Ali Baba, a mobile payments giant, and WeChat, a social media powerhouse, all have their part to play. Huawei though, still seems to grab all the headlines and with increasingly hostile flair.

Let me tell you why that's a problem. Going back9 to Priscilla's report, the new cyber and security, the real world corporate and personal consumer risks in Huawei building 5G networks have largely been genericized and misunderstood.

Do you remember my frustration with the expression, "Once they're in somewhere, they're in everywhere?" Put simply, they're not. No intruder is. Any hacker or intelligence officer worth their salt knows that there's no free lunch. Free lunch is a decidedly American expression that means their job isn't an easy one. However, American pundits and policymakers alike too often get scared instead of getting smart.

Priscilla once again says it best when she offers her alternative argument. Today most companies contract some substantial portion of their business operations including their supply chain to external providers. The breadth of products and services provided by Huawei places much of that supply chain within the domain of one company, exposing its customers to cross-technology risks.

The distinction between that risk being espionage as opposed to flawed hardware or another vulnerability means very little so long as domestic or in-house alternatives to Huawei's offerings do not exist.

In closing, I'd like to offer my current assessment of the Western attitude towards Huawei and towards China more broadly. Huawei will be a force in the information and communications technology market for years to come. Banning the sale of their technology, blacklisting the companies that contract with them, and shutting Chinese graduate

students out from the university research system will only hurt the West in the long run.

Eric Schmidt, former CEO of Google and current Chair of the United States National Security Commission on Artificial Intelligence, appears to agree with my assessment according to some very recent remarks. “I believe there is a better way forward. Corporate competitors, western governments and others must reexamine Huawei’s potential as a force for good in keeping the Internet healthy and stable, a key component of ICANN’s core mission.

However, I’d like to offer my final criticism towards ICANN itself. Countries with an alternative model of Internet governance seem often talked about at these meetings only in whispers and in side bar references.

Invite them in. Your repsonsibility9 is not to show them why they are wrong, but to jointly build a better concept of right.

This last slide just has my contact information as well as a few of my current projects. As of last week, I was going to model the effects of Huawei’s infrastructure investment for a social network analysis course I’m taking this fall. Though that might change to something admittedly more light-hearted next week.

I also currently do some artificial intelligence research for an outfit we affectionally return to as the Cambridge Project back home. Back home, if you have questions or comments on this presentation or

anything else, please don't hesitate to reach out or just ask now. Thank you.

MODERATOR: Thank you, Lukas. Okay, we'll start here.

[DAVID MARGLIN]: Hi. Great presentation. So in today's Globe and Mail, which is the Toronto paper, there is an opinion piece by John Ibbotson that says "Trudeau has no clear options when it comes to Huawei and 5G in Canada," and if you get a chance to read it, which I'm sure you now will since it's today's paper, he suggested it's for basically racism, that it's some kind of fear of China that is making Canada uneasy or Canadians uneasy. And I'm gathering that that's kind of, you didn't use the word "racism" per se but I'm gathering that that 's what, that's the boogeyman you're attacking in your presentation, that you're saying old fashion racism has got to go in this modern era and there are ways to get around it, right?

LUKAS BUNDONIS: So I'm not looking to necessarily play a game of "Gotcha" with the word racism, but I will say that countries with alternative models of Internet governance include nations like Iran so the racism label could be applied there but not necessarily to Russia which also has its own alternative model of Internet governance. So I wouldn't necessarily say that my presentation captures that.

Directly referring to this issue of is it something against China specifically that isn't to do with the actual security of its technology? This whole idea that Chinese companies copy stuff relentlessly. They steal it, they copy it, they imitate it, and then repurpose for their own purposes.

Kai-Fu Lee in his book, AI Superpowers, admittedly this is mostly about artificial intelligence. But he goes into detail on how he believes it's kind of inherent to Chinese culture to do with copying characters and learning the actual language itself that flows in through this baseline of copying things first and then moving forward with that. That's typically the baseline which a lot of critics use to jump off and say, "Hey, let me construct this alternative argument that may or may not be because I'm racist but this is kind of what I'm looking at." They just steal stuff. They always steal stuff. They're not innovative.

My presentation is mostly around the idea that that's not true and we need to get on board or let the train run us over.

MODERATOR: Okay, are there questions from the audience back here?

Okay, Abdeali.

ABDEALI SAHERWALA: There was an article in Reuters, well, it was one of those anonymous sources, in which they said that the Trudeau government postponed a decision of Huawei and the two good Chinese citizens, meeting two

Canadians detained in China, so how should the government of Canada deal with the Huawei situation here considering that we have no other alternative, or a 5G network in place, meaning like a system to put a 5G network here in Canada?

LUKAS BUNDONI: I don't have any official opinion on that. I'm not going to tell the government of Canada how to conduct its business. That's not my responsibility nor my mandate so I think on the question of, I think a better question to answer, to completely dodge what you just asked is, what should western countries do if there's no company that can provide that technology? And the answer is develop it in tandem with current experts on ICT infrastructure. So just because Huawei is offering a cheaper alternative right now, I won't name names and I won't quote sources on this but the whole reason why we are rushing to implement 5G technology in the first place is that ability to parse and send data more quickly across a spectrum that's currently unoccupied.

So that isn't, the pressure that governments feel to implement this technology right now is kind of a fairy tale. It's something that isn't necessary. I mean, if you are presented with this, if you believe that you're presented with this unchooseable choice of, "Hey, it's literally Huawei or the highway," then that's your prerogative. My presentation's arguing that cutting Huawei out and cutting China out as a result of this fear that Huawei is going to enable this mass espionage empire to expand is a little short-sighted. Does that make sense?

ABDEALI SAHERWALA: Yeah.

MODERATOR: Okay, thank you. Are there any final questions?

Okay, thank you so much. Okay, yesterday, we realized that some of our presenters who used the handheld mic, although they were recorded with the audio, they didn't show up on the video recording so one of them is choosing to present again today.

So our final presenter is [Akshay Bhuta] and he will be presenting. Once again today, Akshay, and this is our final presentation. Thank you.

[AKSHAY BRUTA]: Good evening, everyone. My name is [Akshay Bruta]. I am a final [inaudible] graduate student at the University of Colorado, Boulder in the United States. I am pursuing my Masters in the interdisciplinary telecom program with a major in network engineering. I am here to give the audience a high level overview of GDPR and the right to data [portability].

I come from a technical background and I have a basic knowledge about online privacy laws. And this is one of my initial steps for understanding how the Internet is governed.

Before GDPR, we had the data protection directive which was adopted in 1995. The main aim of the DPD was to protect the personal data of

users from being misused. It had loopholes and it lacked the detailed and [inaudible] turnaround on online privacy laws, and hence, a new law was proposed.

The GDPR, the first draft of the GDPR was a legion to [inaudible]. It was [adopted] in the [inaudible] in 2016 and finally, it was enforced in May 2018.

What is GDPR? GDPR is a law which regulates companies and businesses and protects the consumers' personal data. It provides transparency, openness, and empowers the users to have more control over their own information. Companies which fail to achieve GDPR compliance are heavily penalized up to 4% of their annual global income or up to $20 million Euros. It is applicable to companies which are either based in the EU or outside of EU but connecting their business for users living in EU or the European economic area.

Why do we need GDPR? The EPDP was proposed before the invention of smart phones. In [inaudible] '19, reports suggested we have close to 5 billion mobile devices in the world. These mobile devices generate a massive amount of data. A few of my NextGen colleagues regularly verified and confirmed the fact that data is the new oil. Using technologies like AI and machine learning companies can find common patents in the users' life. This particular information can be used in a good way by targeting some particular products and can also be used in [inaudible] for more nefarious purposes like spreading hate or manipulating views.

We need GDPR because there was a lack of transparent and detailed framework and people did not have control over their own personal data. GDPR helps in this perspective and ensures that people have more control over their own personal identifiable information.

So this slide talks about what are the main objectives of GDPR and what these rights are which enable the users to have more control over their own data. The objectives of GDPR do include the right to transparency, our right [inaudible] lock-in, our right to misuse of personal information. IN order to ensure that these objectives are met, the GDPR grants the following rights to its users.

Also, the GDPR obligates that the data [continue] to be transparent in data collection practices and the purposes of which the data is being collected. The data [control] is also responsible to report any data breach to the user within 72 hours.

There have been many benefits of GDPR. Many people believe that it has been a tremendous success since it came into effect on 25 May, 2018. It enables a digital single market. Many companies who have offices in various cities across the European Union have just need to follow only one single rule in the GDPR. It's like one continent, one law. It's just, there are too many benefits that are 2.3 billion Euros per year.

It maintains technological neutrality which means that any other technology which is [inaudible] to the rules of GDPR, it can foster that innovation under the new rules.

So I'll be focusing on the [inaudibto data portability. The data portability is the ability of the people to use that cross-devices and services. It is mentioned in the GDPR Article 20 the right defines that an imposter refuse his or her data. If a user is currently using services of a company and now wants to switch services of Company B, he or she can do so as per the right to data portability.

The data transfer has to happen within a machine [inaudible] format and within a certain period of time which is 30 days. However, the critics believe that the definition of data portability, the right to data portability is [inaudible] and here are some other critical points.

The data provided which is the Tom data provided which is mentioned in the definition can be interpreted in two different ways. One of the ways is restrictively and another one is extensively. By restrictively, I mean that any information which is imported by the user in terms of Google Forms or any kind of forms on the Internet.

By extensively, I meant hat any data which is dated by the online company or online business by using cookies or any other [inaudible] outcomes. Also, there is no definition of any [inaudible] form which allows the possibility of no transfer between controllers which use different data formats.

Also, in the definition that is [inaudible] [Tom] which is mentioned like very technically feasible. This [Tom] allows the data [inaudible] to prevent users from exercising the full power of data portability. By this, I mean that if the controller in a [inaudible] situation can prove that the level of technological development of the organization makes it

unfeasible for the transmission of data to another controller, it's legitimate. So these are some of the loopholes in right to data portability which needs to be addressed.

In conclusion, the right to data portability has been one of the most remarkable novelties of GDPR. It can be an opportunity to foster interoperability of services, increase competition between digital services, and to double up more and more users in [big] platforms. Also, it represents one of the first [theoretical] steps towards default ownership of personal data to data subjects. In a broader sense, the GDPR has had a tremendous impact in Europe and [inaudible] as well.

The GAFA, also known as the Google App Facebook and Amazon are under scrutiny. We all aware of the Facebook so I can't bitch on it because Karen does, as well as Facebook's role in U.S. elections 2016.

This only confirms the view, confirms the fact that laws like GDPR are essentially very, very important in today's scenario and if nothing but being able to keep making sure that companies follow the GDPR and that these rules are maintained across the board. Thank you.

MODERATOR: We have questions for [Akshay]. Okay, there is actually an online question for Lukas. Lukas, during your presentation, have you researched how Huawei participates in the ICANN ecosystem? Is it an active stakeholder? Lukas.

LUKAS BUNDONI: I actually don't have the information to answer that question but I'll definitely to look into it in my future research.

MODERATOR: Okay, thank you. Are there any additional questions? Okay, go ahead.

[NIKET]: Actually, I am [Niket] from [inaudible] for your own record so I am ICANN 66 Fellows and I am speaking on my own capacity. I do not have any questions, but I skipped all my sessions just to attend the NextGen presentation because I would like to know about this NextGen actually.

So [inaudible] be NextGen but I would never be because I'm too old now, and actually I'm very, it was very, a great presentation from all of you and having [inaudible] doing great work. And it is a great work among all this NextGen ambassador as well and the presenter. And I think you have a great career ahead and an opportunity to work for the Internet ecosystem because [inaudible], of course, we are going to retire. One day will not be for lifelong within the ICANN. We will not be for lifelong within ICANN, but you should continue the great work of our leaders and for the betterment of the Internet ecosystem.

So I think you all need to clap for you because you all did very great work. Thank you.

UNIDENTIFIED MALE: Thank you so much.

MODERATOR: Thank you very much. Well, I just want to say thank you to everybody who attended today's session. Thank you to the NextGen. You all presented very well today. You did an incredible job so give yourself a hand.

Also, thank you to my ambassadors for your support and that concludes the ICANN 66 NextGen presentations and I look forward to working with you for the rest of the meeting. And that concludes our session. Thank you so much.

[END OF TRANSCRIPTION]