ABU DHABI – NextGen Presentations
Tuesday, October 31, 2017 – 13:00 to 15:00 GST
ICANN60 | Abu Dhabi, United Arab Emirates

DEBORAH ESCALERA: Okay, we're going to start in a couple of minutes.

UNIDENTIFIED MALE: NextGen presentations at ICANN60, Abu Dhabi on October 31st, 2017 in Capital Suite 3.

DEBORAH ESCALERA: Okay, everybody. I'd like to welcome you to the ICANN60 NextGen presentation. I want to particularly thank my ambassadors, Jackie, Daniel, Awal, Matthias, and Olga for joining me to support the NextGen. Our first presenter today is Francis Nwokelo of Nigeria. Francis, you're going to start us out today.

FRANCIS NWOKELO: Okay. Can you hear me? Hello. Alright, my name is Francis Nwokelo from Nigeria. I'm here because I'm a NextGen fellow at ICANN60 in Abu Dhabi. I'm to present a topic on cyber financial security. Before I continue, first of all I'm going to say a very big thank you to ICANN for making me be part of this program. I'm saying a very big thank you also to Deborah and also the travel

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

coordinator, I believe Joseph De Jesus. I'm saying a very big thank you to you guys.

Actually, I'm supposed to make this presentation at ICANN55 that took place at Marrakech in Morocco, but the Moroccan government didn't give me a letter of [inaudible] It was very unfortunate, so I had to apply for this one, and fortunately for me, I got it. I'm so happy for my voice to be heard. [inaudible] Thank you very much.

Like I said before, I'll be making a presentation on cyber financial security. Let me quickly discuss the things I'll be talking with you guys. I'll be talking on the reasons for cyber financial security, the summary of the reasons, the simple solutions [excluding] jargons. The process of financial data protection, my project which is a security initiative I'm working on and question and [answering].

I want to talk about the reasons for cyber financial security. We have big companies that have a very solid security on their systems, and you often see users whenever they want to make financial transactions on the Internet, they feel like, "Okay, these companies are too good for us so we are not going to have any issues in order to make financial transactions." But there is this other group of people who don't even understand what cyber financial security is.

What I'm trying to say is that you see somebody who wants to use their credit card but doesn't know where or which sites to go to make financial transactions. For example, somebody wants to make online banking, somebody wants to buy something on the Internet. A typical example for example in Nigeria, if you are going to have an ecommerce in Nigeria, I bet you are definitely going to fail. The reason being that over 90% of Nigerians are really scared of making transactions on the Internet, so they won't give you their credit card or their debit card. Whenever they want to buy something on the Internet, when they make purchase online, they are not going to pay you. So all you need to do is just to bring that thing to their doorstep, they see, they look at it before they give you payment.

So now we're looking at the reasons for cyber financial security. One reason is the organizations. Now, the example of the organizations we have, we have the banks, we have the online retailers. Now, the second one is the Internet's community, which involves online shoppers, website visitors like you and I, and the third one is the cyber threat actors like the hackers and phishing attackers.

So now let me talk about the organizations. So please there's something very important. I want you to pay attention to some of the quotes in the slide. It's really important. Here we have "More than 90% of corporate executives said they cannot read a cybersecurity report and not prepared to handle a major attack." This is a very big problem.

For those of you who want to make transactions – I'm not the one who said that. It's coming from Nasdaq survey. I don't know if you understand what I'm saying. I was discussing with somebody yesterday and the person was telling me, "Don't worry, those big companies, they are doing their best in order to take care of security and stuff like that." Who told you that? Now Nasdaq is telling you that over 90% of corporate executives are not ready to read about – they don't have business with anything that has to do with cybersecurity. I don't know if you get what I'm saying.

Now, the next one is, "I think the most shocking statistic was really the fact that the individuals at the top of an organization – for example the executives, the CEO, the CIOs and the Board members – didn't feel personally responsible for cybersecurity or protecting the customer data." The person who said that is Dave Damato, the Chief Security Officer of Tanium. I'm not the one who said that, he said that.

So what he's trying to say here is that the transactions, for example let's take a payment platform for example, a payment gateway. If you are making transactions online with them or are making transactions online [inaudible] or stuff like that, their feeling is that you should take care of the security, not them. But these guys are the people who are supposed to take care of you. I don't know if you get what I'm saying. They're supposed to take care of your security. They're supposed to protect your financial data. You understand? But they don't feel like that. So they are pushing everything to you. So if you are going to do this [inaudible] you're going to take care of your security yourself, not we.

Now, the next one, "The findings came at a time when companies around the world are losing $445 billion USD due to cybercrime." This took place in 2015 from Center for Strategic and International Studies.

The next one is, "The frequency and severity of cyber penetrations, as well as the sophistication of hackers, has increased dramatically. What has not kept pace with that is the education level, the understanding of the impact of cyber across all industries." I'm not the one who said that. It's coming from Nasdaq. So this means that these big organizations, the organizations where you are giving out your financial data, they are supposed to know exactly what they are doing, but these guys don't have any knowledge.

For example in Nigeria now, you walk up to a banker and you complain about – these guys don't know what you are saying.

They'll tell you, okay, they are going to work on the problem, they're going to do this. But these guys, for example bankers, they don't have security experts. You're on your own. When you call these guys on the phone and complain to them, they're like, "Oh, we don't know what you're talking about." Imagine you are talking about a technical thing, you are telling them this that – okay, call your bank for example and tell the person just call [inaudible] probably phishing. They tell you, "What is phishing? Do you mean fishing in the river or something?" They don't know what you're talking about. But these guys are meant to take care of your financial data, but they are not doing that.

Now, let's look at the next one. "A vast majority of the businesses think that they are at risk of hacking threats." This one is actually coming from online shoppers. This is a 2017 report coming from Thales Data Threats. These online shoppers are scared. They are complaining that – sorry, I mean not online shoppers, I mean the online shopping malls. They are doing business, they are collecting your credit card information for you to buy stuff online and stuff like that, but they are still scared. They themselves don't have that 100% confidence that they're going to protect the data. But you yourself are feeling like, "Oh, no, these guys are good. These guys are big companies. They can take care of [inaudible] any time you want you can just give them your credit card information and buy stuff online." But I'm not the one who made this report. This report is coming from these people. But they are telling you that they are scared, they are even worried about security threats.

Meaning that if you want to make financial transactions online, if you want to buy something online, you should know who is good enough to protect your information before you start to give out credit card. Not just any company [inaudible] “Okay, I want to buy this.” No, you have to do thorough research before you give out your financial data. It’s very important. I’m not to one who said this. It doesn’t [inaudible] It’s coming from this, so if you want, you can make research on that.

Now, the next one is, “65% of banks failed the 2017 online security test by Online Trust Alliance.” 65% of banks failed this online security test. Make the research online and find out. I was discussing with someone who said, “Oh, no, banks are good. They are taking care of the security” and stuff like that. Who told you? How do you know? Now look at it. 65% of the banks failed [inaudible] 2017 online security test, 65%. So if 65% of banks fail this test, then you should do what? If you are going to make online banking, you should know the bank you should be banking with, not every bank. I don’t know if you get what I’m saying. Not every bank.

Now, let's look at the next one. The next one is basically the banks use the move online as an opportunity to dump fraud risk on the customer. Before, there was nothing like online banking. You say, "Oh, let's go to the bank, I'll make you a transaction" and stuff like that. But now, we're talking about online banking. So what they now do is that the smart thing they did was they had to move that risk and dump it [inaudible]

Before, if you had something like maybe you discovered that somebody tampered with your account and stuff like that, your money is missing, you can just go to them and [tell them. It's] very simple. But this one, that's a very smart move for them. So they push everything to you, so when you just tell them that, "Man, I'm looking for my money." They say, "You're not serious. Somebody just called you on the phone, you just [inaudible] your details and give the person. [The person just asks your carrier.] It doesn't concern them.

So when you are banking, you need to be very careful, meaning that everything is on you. The whole risk 100% is on you. It's not on the bank. The bank has no business. Look, let me tell you. The bank is not protecting your data. That's the truth.

DEBORAH ESCALERA: Francis, I'm sorry, I don't mean to interrupt, but you have several slides to go and your presentation should only be 10 minutes, and you're already 12 minutes. So you need to speed it up.

FRANCIS NWOKELO: Okay. Alright, so crucially, and contrary to what we find in the banks' marketing materials, if you fall victim to an online fraud, the chances are you will never see your money again. It's very simple. You know what I'm talking about? Okay, now the Internet's community. The second problem, the second reason for cyber financial security is the Internet's community.

The Internet's community has been trained to look for the padlock in the browser before submitting sensitive information to websites such as this, such as passwords, credit card numbers and stuff like that. However, a displayed padlock alone does not imply that a site's using transport layer security or Secure Socket Layer. If you see something like HTTPS which is Hypertext Transfer Protocol Security or Secure can be trusted or it's operated by a legitimate organization.

This is very simple. You see banks telling their customers that, "Look, be aware of online fraud. Before you give out your credit card information, just make sure that you see the padlock. If you see the padlock on the browser, you are good to go." Who told you that? That's not true. Because right now, even hackers are using free SSL, free Secure Socket Layer certificates. You understand? For example, we have less encrypts. We have very cheap ones. So ones that use that and they do whatever campaign they want to do and get to you, so you want to give out your credit card information, you just look at the padlock and you give them the information. It doesn't work like that. You need to do some background check before giving out your information.

The next one is, "The more people know about the risk of fraud and how to protect themselves, the less likely they are to become a victim." This is coming from the British Bankers' Association. This is very simple. What this is trying to say is that if users begin to know about this, when they begin to get education on that, regarding online fraud, how to protect their financial information and stuff like that, I don't think they'll ever become a victim of online fraud.

Now, the third one is cyber threat actors. "88% of hackers can break through cybersecurity defenses and into the systems they are targeting within 12 hours. More than 80% say they can identify and steal valuable information within a further 12 hours, but the chances are that the breach will not be discovered for hundreds of days." So those of you who are feeling like, "Oh, this company is really good," you understand? But this is a research coming from Nuix telling you that a lot of hackers can tell you that within 12 hours, they can break into [the company,] bypass the security measure and enter into a system. And in next 12 hours, a lot of things are going to happen. And even when they break into that system, it could take hundreds of days so the company doesn't even know that there's a security breach.

The next one, "Data breaches will take an average of 250-300 days to detect if they are ever detected at all, but most attackers say that they can break in and still target data within the first 24 hours." It's just like this, what I just said, this is just basically a continuation. Now, cyber attackers are one step ahead of the defenders. So those of you who are feeling like these companies are really good, they are taking care of your information and stuff like that, just bear in mind that these hackers are always one step ahead of security.

One thing that will make you not really fall a victim is for you to have knowledge about this. It's really important. You need to have knowledge of protecting your own financial data by yourself so that if the company is doing your own job, you should be doing your own part, not just putting everything on the company to take care of your data themselves.

So this is just basically a summary of what we just discussed, so because of that, I'm going to jump it. So what's the way forward? Now, just three process. The first one is the online financial data protection process, it's just three steps. The first one is what, who, and how. You want to buy something online, you need to find out for example reviews. You need to make a little research. Okay, for example you want to shop online, you need to make a little research on this particular company you want to buy product from. You understand?

So you see people saying that, "Okay, wow, this company is good." They like their product and stuff like that. So that is the words. So that will take you to the next step. So you need to carry out a little test before giving out your financial details or stuff like that.

The second one is "who." Now you want to use your card to make transactions online. Now, who is the body? Who is the company behind this website? It is very important, that's the who.

The "how" is, how are they taking care of your security? How are they taking care of the security in that organization? How are they protecting your data? That is the "how," and that is what we're going to quickly look into right now.

So now, just like I discussed, what's the "What, who and how?"

DEBORAH ESCALERA: Francis. I'm sorry. I'm going to have to stop you. You have way too many slides here. I didn't realize you have 46 slides, you were only supposed to submit 10. You're 20 minutes in already, so if you could summarize to the last slide. Your slides will be posted online. So I apologize. If you could go to the end and summarize so we can get to the rest of the presenters. I cannot let you go through 46 slides. So please summarize and finish. Thank you.

FRANCIS NWOKELO: Okay. How many minutes are you giving me to summarize?

DEBORAH ESCALERA: Just summarize to the end. Thank you.

FRANCIS NWOKELO: Okay. So like she said, you can take a look at the slides. Okay, these are the words, "Who, how," like I discussed. Like I said, the first one you need to research the body, company, before you make a transaction. You need to check out some reviews, WHOIS lookup and stuff like. The next one is SSL or TSL. The SSL is Secure Socket Layer, or Transport Layer Security. So these things are the things you're going to look on the browser before you make your financial transactions. This is very important.

So right here, please, there's something I want to say, it's very important. So if I'm going to say this, I'm not going to say the rest, that's no problem. Now, please, before you make transactions online, this is very important. You need to find out the domain, for example www.google.com, what SSL certificate are they using? Are they using domain validated, are they using organization validated? Are they using extended validated SSL certificate?

For example, Let's Encrypt only issue domain validated, meaning that hackers can just get a Let's Encrypt SSL certificate. That one is just domain validated, so they don't even need to know you, they don't even need to know your name, and they don't need to know who you are. So this other one is just the organization. They might just want to like know either the organization or you as a person before they give you the certificate.

But I'm going to advise you that, please, if you want to make transactions online, make sure that they are having this extended validated SSL certificate. It's really important, because the process by which they are going to verify you, they are going to verify your domain, is really serious. They have to check you, they have to know your name, they have to know your organization, they have to know your company, your country and stuff like that. So before you make transactions, make sure it has this extended validated SSL.

So this is just – let me just quickly run to a particular slide. One thing that is really going to help you if you don't want to stress yourself checking out the browser, please go to crt.sh and put in the name of the domain. It's really important. It's going to bring out, it's going to tell you, is it domain validated, is it organization validated, is it extended validated? This is coming from I think Comodo Certificate Authority, so I think they are the one who developed this platform. So this is really a very great tool for you.

My recommendation, please. Just give me – okay, PCI, please read up PCI. It's really important. PCI is how does that company protect your financial data. Make sure that that platform you're going to make transactions on is PCI DSS certified. What I'm trying to say is that the PCI is payment card industry data security standard. It's more of a council, they come up with more of like a framework that they look into card owners' data protection. It's really important, please. So make sure you do your research on that SSL security connect – oh, [inaudible] I wish I had [inaudible].

DEBORAH ESCALERA: Don’t worry. This is all going to be on the website, and I can see that you worked extremely hard on this, and it’s a lot of good information. We can see that you’re very passionate about it. So we want to allow people to ask you questions, and I know you’re very lengthy in your answers.

FRANCIS NWOKELO: Please, you guys [should bombard me any and all questions.]

DEBORAH ESCALERA: I understand. Obviously, you’re very passionate about this. We want to allow the audience to ask questions. NextGen, you can ask them questions after the session, because we know that Francis has very lengthy answers. First of all, Francis, you’re very passionate and we can see that there’s a lot of information here. Thank you for your presentation, that was fantastic. Let’s open up questions to the audience now, because I know they’re very interested in what you have to say.

MOHAMMAD: Hello, my name is Mohammad [Amosawi] from Kuwait. You said if the site has SSL and TLS certificate, we have to trust them.

FRANCIS NWOKELO: Is that [inaudible]

MOHAMMAD: The website.

FRANCIS NWOKELO: No. I didn't say that, I never said that.

MOHAMMAD: So how can I make sure that I'm secure when I put my information?

FRANCIS NWOKELO: Okay. Certificate authorities normally issue three different types of SSL certificates. The first one is domain validated, the second one is organization validated, the third one is the extended validated SSL certificate. So you go to crt.sh and put the domain there so you don't need to stress yourself. Just put a domain there, then you make sure it is organization – if you're not too conscious [inaudible] make sure it's at least – the minimum should be organization validated.

Then if you are so conscious about security, make sure it's extended, because before the certificate authorities issue a company or an organization a certificate, it goes through a lot of process. They must know you, your organization, they must know what you are doing, your location, your country, so you must keep providing, you must keep sending a lot of documents. It's not funny, it's not easy, unlike domain validated where they don't even know who you are. It's just automatic.

MOHAMMAD: The extended one – yes. The extended one you're talking about?

FRANCIS NWOKELO: Okay. So another thing is, please, for those of you who normally come to a site and see SSL and they tell you that the site is SSL secured, look, please, that site does not mean security. It doesn't mean that that – look, for example if a website has an extended validated SSL certificate, which is the highest, and that site doesn't care about security that much and stuff like that, it doesn't mean that if a site has extended validated, it doesn't mean that that site is secure, no.

How are you going to know that that site is secure? You have to make sure that that site is PCI DSS certified.

MOHAMMAD: PCI DSS?

FRANCIS NWOKELO: Sorry, the SSL there is just, "We are sending information between your browser to the website." It's just to encrypt it for you so the hackers don't break into your data. So as soon as he gets to the database or the platform, it doesn't mean it is secure, so you have to go and make sure that company is really securing your information. That is the thing. Thank you. Any other question?

DEBORAH ESCALERA: Okay. Thank you. We're going to move on to the next presenter. Okay, next we have Hamideh Farahani.

HAMIDEH FARAHANI: Hello, everyone. Is the sound okay? Hello, everyone. I'm Hamideh from Iran, and –

UNIDENTIFIED FEMALE: [inaudible]

HAMIDEH FARAHANI: Okay. Nice to meet all of you. I studied computer science in bachelor and master's, and I was interested in data science, so I did my thesis in machine learning and data mining, these kinds of things. MIT says, "We are looking for finding influential users in Twitter." We crawled six months' data of the Twitter. We crawled users' activity, and we used some algorithm and other things to find influential users, and we analyzed their behavior and what they do to –

Okay. Yes, we analyzed their behavior, and we got some reports, and some of them were interesting so I put it here to show you. To see how important are social networks, we have 7 billion population on Earth, and 3 billion Internet users, 2 billion social network users. Every user has 3.5 accounts on average, so we can see there's a big potential for working in social networks. We chose Twitter because Twitter has many good options, for example the data are clean, there is no private message in Twitter, everything is on the wall. So that's a good point for data mining.

As you see, we have 67 million American users in Twitter, 26 million Japanese users, 28 million Brazilian users, so we chose Twitter and we were looking for influential users. Influential users are very important nowadays because everyone are looking to influential users, what they're doing, what they eat, what do they do, what do they wear? Finding these users can help us in marketing, in predicting, in many areas.

For finding influential users, we used some measures based on these three. We used retweets, followers, and replies. We used many measures, but they were based on these three.

I think I should briefing my presentation, yes? Or I have time? Okay.

We did many things. I don't want to go to the details, because we used many measures and we used Gaussian mixture models, I think that's not very suitable to talk about it here. But after we found the influential users, we analyzed their behavior.

As you can see, this one is original tweets, and that's through the time. We have it for six months. So as we can see, when they have more tweets, other measures are based on – their tweets go up and go down. So the original tweets that user have is very important.

I've put a few of our models which the result was interesting for me. For example, you see when original tweet goes up, the retweet impacts of the users goes up too. They have linear relation with each other.

The number of tweets which will be retweeted has a linear relation with original tweets too. These are for influential users just. About the number of followers but it was somehow different, because when original tweet goes up, when the user puts more tweets, it doesn't necessarily go up. Up to one point, it goes up, but suddenly the growth stops and it goes up slower. And it means that the audience, the followers can be more, but in one time maybe they will stop and they don’t increase. These are based on our data.

The mention impact was somehow different too. When original tweet goes up, it doesn’t necessarily go up. The good point that I can tell is if you want to be influential, tweet, tweet, tweet. Yes. Finished. Thank you.

DEBORAH ESCALERA: Okay. Are there any questions for Hamideh? From the audience? Okay.

ADEEL SADIQ: Thank you for your presentation. Adeel from Pakistan. I have two questions. The first one is, where did you draw the line of influential and not influential? That’s the first one, and the second is, where you are going to –

HAMIDEH FARAHANI: Could you please repeat the first one? Because I didn’t get that.

ADEEL SADIQ: You said that you did the test for the influential tweets, right?

HAMIDEH FARAHANI: Yes.

ADEEL SADIQ: So how did you decide, where did you draw the line that until this point, you will consider the tweets influential, and after that, it will not be considered influential? So there has to be a threshold value someone, yes? And after that, how and where are you going to use that data? What's the way forward for your research?

HAMIDEH FARAHANI: You mean where did I bring the data?

ADEEL SADIQ: How are you going to use your data? Like in some practical aspects or something like that. Your research is good, it's valid, everything is okay, fine. So now, how are you going to use your data and your research in some practical way?

HAMIDEH FARAHANI: I don't know, because it was an academic, so we published a paper, and I don't have any special plans for that, honestly.

ADEEL SADIQ: And back to my first question –

HAMIDEH FARAHANI: But I'm working on that to use it in other ways, but actually – and now I didn't do any special things.

ADEEL SADIQ: Back to my first question, how did you decide at what point you were considering a tweet to be influential, and below that, it's not influential?

HAMIDEH FARAHANI: You mean these? It has gone.

ADEEL SADIQ: From the formula, I believe. Right?

HAMIDEH FARAHANI: Yes.

ADEEL SADIQ: From the formula, you decided that –

HAMIDEH FARAHANI: I can't hear you, I don't know why. [inaudible]

UNIDENTIFIED MALE: I think he's asking about the threshold number of followers that you decided this is influential or not.

HAMIDEH FARAHANI: Oh, the number of the influential, you mean how many are there?

UNIDENTIFIED FEMALE: Oh, he's asking what's the difference when you decide that someone is influential and somebody is not.

HAMIDEH FARAHANI: Oh, yes. I said we had many algorithms, many measures. For example, we used – it has a mathematic algorithm behind that. We use a Gaussian mixture model which is suitable for this. For example, it removed the outlier users. We have some users who are spams, they are not influential. They just retweet others, and we remove them. We use some mathematical things that are standardized. Yes.

DEBORAH ESCALERA: Any other questions for Hamideh?

HAMIDEH FARAHANI: [Yes, he has.] Hi. I can't hear you.

BARRY LEIBA: It was turned off. What would interest me in this, clearly, Kanye West for instance is going to be influential because he has millions of followers, and he can say garbage and people will listen to him. I'm not picking on him but that's just that's the case. But there are people who became influential through Twitter. They started off, no one knew who they were, and by tweeting, they became influential. I would be interested in – for future work – determining what pattern that follows, and how that happens.

UNIDENTIFIED MALE: [inaudible]

BARRY LEIBA: So it's not a question about the current work, but something I'm suggesting for you to look at in the future.

HAMIDEH FARAHANI: Thank you so much.

MATTHEW: This is Matthew for the record. The answer to your question about the application of such research is that there are many services who are using such data to find influential users, not just celebrities. This is not limited to celebrities. So they can find those influential, and connect them to some businesses, to allow them to make money and allow the businesses to use them, in fact. So this research – and if we can find an algorithm or something on this – can be helpful for those services. So I think this is a quick answer to your question. It might be.

I'd like to add something to this. I think you need to add a factor to your study. I'm not sure, but this is my suggestion. Being verified on Twitter is a factor to be influential, so if you can add this and analyze if being verified has a positive or negative maybe impact on being influential or not, it would be good. This is my suggestion. Thank you.

HAMIDEH FARAHANI: Thank you so much.

DEBORAH ESCALERA: Thank you, Hamideh. Next up is Heather Costelloe of Australia.

HEATHER COSTELLOE: Good afternoon, everyone. My name is Heather Costelloe and I'm a final year law student at Murdoch University, which is in Perth in Western Australia. My presentation covers the issue of the definition of a well-known trademark in ICANN policy.

My presentation today will cover the international trademark law framework which governs the protection of well-known trademarks. I'll then explain the difference between a standard trademark and a well-known trademark, explain how ICANN currently deals with these trademarks, and explain what I suggest ICANN does.

To start off with, there are two different types of trademarks: standard trademarks and well-known trademarks. When a trademark is registered, it's registered with respect to a particular class of goods or services, for example, perfumes or beverages. Those standard trademarks are only protected within the same or a similar class of goods or services, meaning that someone cannot use that trademark in the same or a similar class. A well-known trademark, however, is protected across all classes of goods and services, no matter which class it's registered in.

This protection of well-known trademarks stems primarily from two international intellectual property conventions. The first is the Paris Convention. In 1925, the Paris Convention was amended to include the protection of well-known trademarks. However, the Paris Convention did not contain any provisions providing for the definition of a well-known trademark. Subsequently in 1995, the TRIPS Agreement extended the protection of well-known trademarks to all goods and services, which is now. However, the TRIPS Agreement still didn't provide for a definition of a well-known trademark.

Now, the context in which the definition of a well-known trademark is particularly required is the domain name system. Trademarks can appear in domain names both in the top-level of a domain name, and also on the second level. So as you can see in the two examples I have here, in the top-level www.shopping.gucci, the top-level .gucci is a trademark. In the second example, www.facebook.com, Facebook is the trademark.

Now, with the recent increase and the New gTLD Program, with the increase in the number of top-level domain names, the instances of trademark infringement in the new gTLDs has significantly increased than all of the trademark infringement in the legacy gTLDs. Because of that, the issue of a well-known trademark is of particular importance in the context of ICANN stating that it is committed to increasing or to continue expanding the top-level of the domain name system.

So certainly, ICANN does at this stage have a number of Rights Protection Mechanisms to protect trademarks in the DNS. You can see these on the screen. However, none of these Rights Protection Mechanisms differentiate between a standard trademark and a well-known trademark. ICANN did in 2009 attempt to implement a policy which would have provided for the protection of well-known trademarks, and that was called the Globally Protected Marks List, or the GPML.

The purpose of the GPML was to act as a reserved name list so trademarks which had a certain number of registrations across ICANN's five regions would be part of this list, meaning that users couldn't register a domain name that included one of those trademarks. However, ultimately, ICANN rejected the proposal for the GPML, and one of the primary reasons that the GPML was rejected was because there was no definition of a well-known trademark which could have been used to guide ICANN to develop criteria for a mark to qualify for the list.

However, what the GPML has done is it has influenced a number of registries to implement nonmandatory GPMLs which apply only to their TLDs. For example, DONUTS' Domains Protected Marks List and the Minds + Machines Protected Marks List. Trademark holders can register to prevent other users from registering their trademark in a second-level domain. What this shows is that it is technically possible to implement this type of reserved name list. The issue is that there is no definition of a well-known mark which could assist ICANN to implement one that doesn't just apply within a certain range of TLDs but could apply to all new gTLDs in the next expansion of the DNS.

So as I mentioned before, there is no current definition of a well-known trademark in international law. However, in 1999, the World Intellectual Property Organization with that in mind put out a list of joint recommendations which were nonbinding, nonmandatory recommendations for what national jurisdictions could consider when determining whether a mark was well-known. So my research takes into account all of these factors and looks at the test use in national jurisdictions in order to create a more precise definition which could be implemented by ICANN.

Now, if ICANN were to take on a definition of a well-known mark in its policy, this would have clear benefits both within and outside of ICANN. Most notably within ICANN, the definition of a well-known trademark would allow ICANN to implement some form of Rights Protection Mechanism to specifically target the infringement of well-known trademarks. The flow-on effect from this is that it enhances user faith in the domain name system because there are less cases of infringement of well-known marks.

Outside of ICANN, there are also clear benefits. Most notably is that the definition of a well-known trademark would clarify an area of international law that has long been suffering from a lack of clarity. The flow-on effect from this is that it would seek to harmonize the international and domestic law on well-known trademarks. Because there has been no definition of a well-known trademark in international law, it has led to a number of jurisdictions taking vastly different approaches to the protection of well-known marks and to the definition of well-known marks. So an international definition would seek to harmonize all these jurisdictions. And finally – and similarly – as a flow-on effect, it would reduce the instances of infringement and would enhance consumer faith in well-known brands. That brings me to the conclusion of my presentation, but I'm happy to take any questions.

DEBORAH ESCALERA: Thank you, Heather. Do we have any questions for Heather?

BARRY LEIBA: Hi. Clearly, you're focusing on the well-known marks, but it seems to me that the gTLD system kind of turns this a little bit on its head, that standard marks in the real world are reusable resources. If I use a name in one context, in advertising in one class, and someone else uses the same name in advertising in another class, we can do that. With gTLDs, they are limited resource. Once I get that name as a gTLD in my class, no one else can get it in any other class. How does that affect trademark issues? As asked by somebody who doesn't really know trademark laws.

HEATHER COSTELLOE: Yes, that is right. So in the domain name system, once someone registers a domain name, no one else can register it. So in effect, standard trademarks are actually afforded a slightly higher level of protection within the domain name system. The issue however still stands for well-known trademarks, well-known brands, that they suffer a higher level of infringement in the DNS. And because of that, I argue that ICANN should react and should implement a policy to create a mechanism that provides an enhanced level of protection to reduce infringement.

UNIDENTIFIED MALE: Hello, this is [inaudible] from Pakistan. My concern is that as you mentioned, there is no internationally accepted definition of well-known trademarks. So how can ICANN on itself decide which trademarks are supposed to be well-known trademarks and which are not when they are trying to implement this policy? We already mentioned that there is no international definition of well-known trademarks so far? So do you think ICANN has that capacity or resource to actually identify the well-known trademarks and implement that policy within the ICANN world?

HEATHER COSTELLOE: What I recommend is that ICANN Policy develop a definition of a well-known trademark. So within ICANN – yes, they could draw on the WIPO joint recommendation factors, make those more precise, and implement that into ICANN policy to develop a Rights Protection Mechanism. Now I know this doesn't actually create any form of international law, because ICANN is not a lawmaking body. However, if ICANN were to take on a policy, I argue that ICANN Policy develops a form of soft law which could be influential to members of the Paris Convention and the TRIPS Agreement which could influence them to amend the TRIPS Agreement or the Paris Convention to include this ICANN policy definition, as therefore forming part of international law.

DEBORAH ESCALERA: Okay. One last question.

JACKIE EGGENSCHEWILER: Sorry, this is Jackie Eggenschewiler speaking for the record. Just a follow-up on the question, actually. So would you argue that it's almost a type of customary law that would emerge that would influence those two bodies of law that you mentioned?

HEATHER COSTELLOE: It could be argued that it's a customary international law. The issue that arises with that is whether ICANN Policy meets the level of opinion juris, which personally I don't think it does. So in that sense, I wouldn't say that it is customary international law, but forms a type of soft law which is influential on governments.

JACKIE EGGENSCHEWILER: Also, I guess there would have to be some state practice in that sense for it to –

HEATHER COSTELLOE: Yes, that's opinion juris.

DEBORAH ESCALERA: Thank you, Heather. Very well-presented. Okay, we're going to pause for a minute. We're having a little technical difficulty. One moment, please.

Okay, our next presenter is Muhammad Abid from Pakistan.

MUHAMMAD ADAN ABID: Good afternoon, everyone. I'm Muhammad Adan Abid from Pakistan. Currently, I'm doing my master's in management. I have always been interested in the economical aspect of Internet. Therefore, today I'm presenting ecommerce in Pakistan.

Louder? Okay.

So first, I would be talking about the global ecommerce growth, and what is the current trend going in global ecommerce. Then, I'll be talking about the current ecommerce trends in Pakistan, what are the current market trends, and what is the expected growth. Then, I will be talking about what are the current issues and challenges that we are facing in Pakistan related to ecommerce, and then what's the way forward.

If you see this graph, in 2016, the global ecommerce market stands at 1.8 trillion, and it's expected to grow to 4.5 trillion in 2021. In between 2016 and 2017, there is almost increase of 25%, which means that ecommerce and market almost grew 25% in one year. As more people come online, the next billion are coming online, which means that this is an open field for everyone.

The major change came in Pakistan when 3G, 4G services launched in 2014. This graph shows how ICT sector evolved in Pakistan. So the major change came in 2014 when 3G, 4G services launched in Pakistan. So Pakistan has great potential market for ecommerce. Pakistan's population is almost 200 million. The total broadband users in Pakistan are 45 million. Before the launch of 3G, 4G services, there were only 2% broadband users in Pakistan, but now, it stands at 22%. 75% of population has access to 3G, which means that if anyone wanted to access Internet, 75% of population of Pakistan can access it.

During last four or five years, Pakistan's government and private sector has played a very vital role in developing Internet. Almost 85,000 km of fiber has been deployed all across Pakistan, and there have been multiple fiber optic links to connect with the international Internet.

The current market size of ecommerce in Pakistan is between $60-100 million. The business model that's most used by consumers in Pakistan is cash on delivery model. 90% of people in Pakistan use cash on delivery model. The major players in Pakistan related to ecommerce are daraz.pk, zameen.com, olx.com and pakwheels.com.pk. Recently, there has been use investment in these all major players, which is very positive point for Pakistan ecommerce industry. There's no major international ecommerce player in Pakistan like Amazon, eBay. There's no PayPal and Stripe in Pakistan. Every minute, 26 Pakistanis access the Internet for the first time.

As we see, there is no international player in Pakistan of ecommerce, and there have been huge investments in the local major players. So there is huge opportunity for entrepreneurs to invest and to build their businesses online. Pakistan, the ecommerce industry is expected to grow 72% in near future. It's stated statement of the government of Pakistan that they're going to achieve $1 billion market until 2020. By 2020, there will be more than 65 million 3G, 4G users. Government has committed that they'll roll out 5G by 2020.

The fun fact is that almost 60% of population of Pakistan is youth, and population below 35 is the most inclined towards new technology and its use in online shopping. Recently, Alibaba group signed an MoU with the Trade Development of Pakistan to explore ecommerce opportunities, which is a huge positive point for the ecommerce industry of Pakistan.

Challenges. As I mentioned earlier that 90% of consumers in Pakistan use cash on delivery model, there is less usage of credit and debit cards in Pakistan. There is a lack of an e-payment gateway as I earlier told that there is no PayPal, there is no Stripe available in Pakistan. People in Pakistan are not able to buy online on Amazon or AliExpress because there's no PayPal or Stripe.

The major problem the ecommerce industry right now is facing is that integration with delivery channels. There is no speedy delivery of the product. There are weak consumer services. In July, Pakistan Digital Forum was held in Islamabad, and the major issue that was discussed there was that there is no government framework in Pakistan related to ecommerce, which means that if something goes wrong online, on ecommerce stores related to ecommerce, then no one can be held accountable.

What's the way forward? Ecommerce policy framework is in process. E-payment gateway is under process. We will soon get our own e-payment gateway. Interoperability in mobile banking. Since now, we were not able to send money if we are using different mobile payment gateways, but soon, we will be able to send money. If I'm using JazzCash, I can send money to Easypaisa. Since now it's not applicable.

There has been huge increase in the startup and entrepreneurial culture in Pakistan. There has been a huge increase of incubation centers and angel investor platforms in Pakistan, which is a plus point. If we want to grow our ecommerce industry, we need these kinds of platforms. Our provincial governments are very keen to develop and build the capacity of [youth] related to ICT, and according to the statement of State Bank of Pakistan, there are only 15% of people who have bank accounts in Pakistan, but until 2020, they have made a plan, [they have merged] strategy that they will get this statistic to 50%.

At last, I want to say that vision has been set, strategies are being made, policies are being made, and soon we are going to see unicorn ecommerce company in Pakistan, just like U.S. and China have. Thank you.

DEBORAH ESCALERA: With the audience questions?

UNIDENTIFIED MALE: Yes.

DEBORAH ESCALERA: [inaudible]

VAHAN HOVSEPYAN: Thank you. Thank you for a good presentation and thank you for your development in Pakistan. Vahan Hovsepyan [second time] ICANN Fellow, Armenia.

MUHAMMAD ADAN ABID: Thank you.

VAHAN HOVSEPYAN: Do you have any signature systems and invoicing systems in your country? And second one, do you develop any digital transport corridor concepts, and do you think that it will be implemented in the nearest feature in Pakistan to connect Pakistan to the outer world, like China or Europe? Thank you.

MUHAMMAD ADAN ABID: I don’t think so, as Pakistan is in its early digital revolution evolution stage. So I don’t think in the near feature that could happen.

DEBORAH ESCALERA: Any other audience questions?

DANIEL WOODS: I have one.

DEBORAH ESCALERA: Okay.

DANIEL WOODS: I wondered if you had any kind of personal predictions on whether it will be U.S. firms like eBay and Amazon, or maybe Chinese firms like Tencent or Alibaba, or even Pakistani local firms which you felt were most likely to succeed?

MUHAMMAD ADAN ABID: I think U.S. firms are not inclined towards Pakistan's ecommerce industry. As you know, PayPal is in almost every country. Pakistan still doesn't have PayPal, and not even Stripe so far. And as I have already told, Alibaba group has already signed a MoU with Pakistan's Trade Development Authority. I think if there are going to be more investments in the local entrepreneurial and local businesses, local businesses would be, yes.

DEBORAH ESCALERA: Okay. Any more questions? We have time for one more. Very interesting. There was a lot of information contained in that presentation that I was unaware of. Thank you so much.

MUHAMMAD ADAN ABID: Thank you.

DEBORAH ESCALERA: Okay, next we have Padma Venkataraman from India.

PADMA VENKATARAMAN: Good afternoon, everyone. I'm Padma, and I'm a third year law student from India. I've done a bit of research with regard to ICANN's participation in litigation, and so I've decided to make my presentation on how we can sort of use ICANN's participation in the discovery process before trial in order to sort of assess its general approach to disclosure in context of its other disclosure policies.

Throughout the course of my presentation, I will first just address the general concept of discovery and give you a brief overview of discovery in the U.S., and then as ICANN is subject to U.S. laws, federal and state laws, and I will proceed to talk about why it's important to analyze discovery participation in context of disclosure policies, and how ICANN's approach to disclosure is in general. Then I will proceed to talk about one case in particular, the .web case, and the arguments that played out in that with regard to disclosure of information that is not readily available to other parties. And after that, I will talk about the concerns that arise from ICANN's participation in such disclosure. And after that, you can ask me any questions you would like to also.

There might be a lot of information in this, so feel free to ask me detailed questions either after the session or later, because I may not be able to explain the basics of many legal terms that people may not be familiar with, especially if you're not from a legal background, and there may be many things that I can't answer satisfactorily as well because I'm still learning. I sort of apologize for the plain presentation. I couldn't figure out how to include infographics and fancy diagrams with my topic.

UNIDENTIFIED MALE: Maybe you can explain the legal [inaudible]

PADMA VENKATARAMAN: That's too long a process. Okay, maybe I can just start. My first slide, I explain the concept of discovery in general, and then I briefly trace the history of evolution of the discovery process in the U.S. When coming to the concept of discovery, for those who are not familiar with it, it's basically pre-trial disclosure of evidence that's relevant to any issues with regard to the dispute at hand by both parties or all the parties who are part of the suit.

For example, if I make certain allegations against another party, I would want evidence that was in support of their defenses to such allegations, and often, I don't have access to that defense, so I would be completely unprepared going to court if I don't know on what evidence they're going to base their defenses, right? So that was the entire point behind discovery in general.

So the idea behind the development of discovery rules was that there's just the determination of all matters and remedies to the suit in order to sort of remedy the imbalance in information distribution, so that both parties can gauge their tactical strengths and weaknesses and come better prepared in order to ensure litigational efficiency and fairness.

So now tracing the history of discovery in the U.S. – this is going to be a bit brief – you had two sorts of courts: you had courts of law and courts of equity. They dealt with different remedies. The importance of bringing in courts of equity here is just to say that whatever limited discovery tools you had available in the 1800s were restricted to courts of equity. So you couldn't file for interrogatory, so that you couldn't submit a question to the other parties seeking an answer until the federal rules of civil procedure were legally [later] down in 1938.

So before 1854, all that was available was the facts and allegations made in your individual pleadings. So the entire case was decided by the judge only based on the allegations and facts available in the pleadings submitted by both parties. So there was no assessment of the allegations before the trial began, which is why the need for discovery developed, so in 1854, and in 1873, over those two years, there was the courts of law and courts of equity, their practices merged, especially with regard to discovery tools, which is why your interrogatories, depositions and availability of limited discovery tools became more available to the parties.

But given U.S. legal system, it's also important to know that different states had varying laws with regard to adoption of discovery tools, because it was according to each state. They could decide whether the courts could decide whether to adopt those tools or not. And often, your federal courts in each state did not adopt these discovery tools. So in different courts in different states, some allowed interrogatories, some allowed depositions, but it was not uniform.

In 1912 when the Federal Equity Rules were introduced, your interrogatories were allowed in federal courts, and then in 1938 under the Federal Rules of Civil Procedure, here the main aim was to bring in some sort of conformity with regard to federal courts and state courts in the same state as well as uniform procedure across federal courts. Also important to know here that a discovery conference is under rule 26 of the FRCP that's 1938 allows the parties to actually confer with regard to different issues they may want to file for discovery, different issues regarding which they may want evidence from the other party.

So that was until 1938. Here onwards, there was lower reliance on the pleadings themselves as the parties could avail of evidence via employing discovery. So in 1946, the scope of discovery was slightly expanded to include relevant inadmissible evidence. That is evidence that can't be submitted or introduced during the trial but that could reasonably aid in preparation of a party's case. In 2000, there was an amendment to check discovery abuse or excessive discovery requests filed by one party, and it was decided that information discovery requests would be allowed only with regard to information relevant to the claim or defense of any party, and not just any subject or matter relevant to the dispute. Only if that information pertaining to the claim or defense of a party proved inadequate would a request be approved for evidence relating to any relevant matter to the dispute, and this would be allowed only if a standard of a good cause was satisfied.

The problem with this is there has been no guidance in the rules for what constitutes good cause, considering different states have varying laws and often under the Federal Rules of Civil Procedure, the burden is on the courts to sort of self-regulate and develop their own rules, especially with regard to discovery, these standards are not uniform as well. For example, if different parties sue ICANN in different states, the burden for proving good cause would be slightly different.

Just a few other things to note. With regard to discovery, a lot of conversation just surrounds discovery abuse and how discovery is a huge problem in the U.S. because excessive discovery requests are often filed. I think we regard to ICANN, the concern is that your generalized objections with regard to discovery that are employed in litigation in the U.S sort of reflect in its disclosure policy. So you have general objections about discovery requests being vague or nonspecific, the information requested is not reasonably accessible, it's overly burdensome, the request is vexatious in nature, things like that that are normally employed by defendants to disregard a plaintiff's motion to discovery in the U.S.

And you will see that in ICANN's documentary information disclosure policy which is its version of a right to information policy, any request that is filed that comes under these broad categories of not reasonably accessible, overly burdensome, vexatious, not in the right format, not available in processible formats, all these reasons can be sort of employed by ICANN to deflect such requests for information. I'm sorry.

UNIDENTIFIED MALE: Go ahead.

PADMA VENKATARAMAN: Okay. Right, I think I'll just continue. So that was my first slide.

UNIDENTIFIED FEMALE: [inaudible]

PADMA VENKATARAMAN: No, that's okay. So that was my first slide. My second basically talks about ICANN's approach to disclosure in general. Generally, when you talk about disclosure, there are two kinds of disclosure. You have reactive disclosure and proactive disclosure. Reactive is when [inaudible] information, you give it to me, and proactive disclosure would be broadly you would – sorry, you willingly provide information without me having to ask for it, right?

So my first point on that slide is about ICANN's disclosure policies. Now even though it has one specific disclosure policy which is the documentary information disclosure policy, you can sort of broaden the scope of disclosure policies in general to include uploading of, say, transcripts for meetings, minutes of meetings, background checks for applicants for the gTLD processes, for Board members, for a lot of things. Disclosure of information in general with regard to the functioning of ICANN in order to sort of enhance, enable transparency, as well as financial disclosure, things like that, granular income.

So with regard to the [inaudible] which I'm going to refer to as the [inaudible] just with regard to, say, financial disclosure, so the organization I had interned with has I think – I forgot the exact number, but it has filed the most number of requests under this policy requesting a breakdown of revenue, historical revenue that has accrued to ICANN, and from 1999 to 2014, and you can see that prior to 2012, certain lobbying disclosures and detailed revenue by source, those documents haven't been uploaded.

Now, the thing is ICANN has consistently said that it cannot upload a breakdown of historical revenue simply because the data for the years preceding 2012 were collected in formats that they're unable to process and sort of publish right now. The raw data for those years is stored on systems, and we cannot process the information according to your requirements, which is why we cannot publish reports that are consistent with the formats for post-2012. Right? And they've also said that [inaudible] that it's overly burdensome and it's not reasonably accessible, and it's difficult to prepare the reports.

So my next point is about the effect of disclosure policies. It has as huge effect on the information available with regard to financial transparency and accountability in general. It has an effect on fair competitions, so for example, information disclosure and competition value might not always just immediately draw a very tangible link between the two. In context of Verisign's really complicated relationship with ICANN given the Root Zone Management Agreement, that Verisign owns .com and most recently .web, and that the .net renewal was tied to the renewal of the RZMA – that is the Root Zone Management Agreement – it's sort of impossible to understand or gain a holistic understanding of that relationship without having some sort of information available.

Even in the .web case, the fact that Verisign finally did finally manage to secure the rights of .web would – well, it's reasonable for the community to want to have access to any communication between Verisign and ICANN with regard to .web, right? And with regard to decision making processes inside ICANN with regard to, say, the .com, .net, .org and .web, awarding of those rights. Oh.

UNIDENTIFIED FEMALE: [inaudible]

PADMA VENKATARAMAN: That's great. Okay. The third slide – the next one, [inaudible] Next. Okay, this one. Oh, this is great, here.

And there are concerns about jurisdiction as well, because you have waiting laws, and the fact that ICANN is subject to U.S. laws and not an international convention or international laws that have been agreed upon by most countries is also slightly worrying with regard to accountability, and commitment to proactive and reactive disclosure which can generally be gauged by discovery participation as well, which is why it's really important to analyze discovery participation and – sorry.

Alright, so here I'm going to be talking about one case in particular, which is the .web case, so I'll just give a brief overview of the facts of the case. In 2012, after the new gTLD auction process was initiated, seven applicants filed for the rights of .web, and they were placed in a contention set which is required when there are multiple applicants for the same gTLD. And just a quick note here, every time any applicant applies for a gTLD, there's a participation fee of $185,000 that's required from each participant.

Normally, there's a private auction that's a voluntary settlement amongst the various bidders, and if it's decided via private auction, the participation fees as well as the winning bid is distributed amongst the bidders. However, if a private auction is not possible and ICANN gets involved, that becomes a last resort ICANN auction wherein the final winning bid as well as the participation fees accrues to ICANN. So in 2012, it was supposed to be a private auction, but somehow after four years in 2016, NU DOT CO which was one of the applicants – I'm going to refer to it as NDC from now on – NDC sought to withdraw from the private auction, requiring a last resort ICANN auction. At this point –

UNIDENTIFIED FEMALE: [inaudible]

PADMA VENKATARAMAN: Okay. At this point, Ruby Glen, another applicant had asked NDC to reconsider their decision to withdraw from the private auction, at which point NDC made a representation to Ruby Glen that there was substantial material change in its financial management position, its Board and ownership. And when Ruby Glen communicated the same to ICANN, ICANN initiated an inquiry on Ruby Glen's request which was extremely limited in nature because it was just a confirmatory e-mail sent to NDC asking them to confirm status quo and that no substantial change had been made, to which NDC said, "Yes, no substantial change has been made." And ICANN proceeded with the auction.

On July 27, the winning bid of $1.35 million, NDC won. The bid goes to ICANN, and VeriSign immediately came out with a public statement saying that it had been behind the .web application the entire time, and it was involved in the funding of NDC and had used NDC as a front to acquire .web.

And as we can see here, ICANN's defenses in court about the complaint made by Ruby Glen being vague and unsubstantiated are sort of surprising given Verisign's own confirmation about its involvement in this funding, and given how the screening processes for applicants require that [inaudible] checks be made, and that any change in the application that is financial position or anything, or third-party funding, is liable to be notified to ICANN.

However, ICANN may, at its will, if it thinks it necessary, sort of carry out a further screening process after being notified of such change. It's important to note here that a lot of things within ICANN's policies and Bylaws with regard to carrying out actions with regard to accountability are often discretionary in nature. There's nothing that actually warrants accountability simply because of the nature of the organization as a whole. If you talk about accountability to the community, it's hard to sort of gauge how the community can act as a check to irregular procedures or lack of substantive compliance, because the community often doesn't have a lot of information available with regard to lack of financial transparency or communication. If you talk about – I'm sorry.

DEBORAH ESCALERA: Padma, you have one minute. Thank you.

PADMA VENKATARAMAN: And it's funny, ICANN has repeatedly said in court that the liability with regard to breach of foundational documents such as its Bylaws don't – it is not liable for such with regard to applicants and application processes, but only with regard to officers, directors and Board members.

So for example, [inaudible] not to sue, which is basically a legal way that exempts it from any liability with regard to any damages caused during any application process is a precondition for entering into application process. So all gTLD applicants have to sign that legal waiver before they enter the entire system. There is no negotiation on that.

And given that ICANN's – well, you can call it a monopoly over the DNS, and the fact that it is the sole global operator and allocator of this, and often there's a huge [inequality] as well as [inaudible] with the involvement of the U.S. government and private interests with regard to Verisign and other registry operators, you will see that that legal waiver is actually procedurally and substantively unconscionable, something that ICANN heavily disagrees with. It always says that the legal waiver is valid, enforceable, conscionable, because we provide remedy via internal accountability mechanisms, none of which are independent in nature, none of which are binding on the Board or on ICANN as an organization. Something which I think came up in yesterday's public forum where the [inaudible] not sure. Sorry.

I'm not sure I can finish my presentation, but generally, concerns arising from ICANN's discovery history – right? You have your lack of uniformity due to varying laws because of the U.S. legal system, you have insufficient evidence to fulfill the burden of proof with regard to intentional wrongdoings or intentional misconduct, you have a really high standard for proving the unconscionability of the [covenant] not to sue, something that may vary in different countries and under international law.

And to conclude, so how can discovery history inform the community? It's really important to sort of understand that discovery is a means to an end, and when people talk about how discovery abuse in such cases, discovery becomes the main focus of the entire judicial process versus the main merits of the case. It's really important to understand here that often, parties taking ICANN to court cannot succeed merely on the merits of their case simply because of the lack of information available through its disclosure policies in general, which is why discovery is so important.

So if this information is not available [inaudible] in general, then when you take [inaudible] to court and seek a discovery process in order to avail of that information and you [inaudible] that ICANN is not – really? Are you taking it from me? I'm sorry, one last line. Just know that ICANN doesn't really have a supervisory body. The closest thing that could be created with that would be the community, and with lack of information, it's hard to sort of act as a check. If the community is not informed, you cannot hold ICANN as a whole accountable. You cannot sort of see whether its actions are inconsistent with its Bylaws and commitments to competition, fairness, transparency and accountability.

Also that generally, a lot of obligations that it now holds itself accountable to are voluntary adoptions, especially one example being the human rights obligation that it recently adopted due to the nature of its legal status. It's not required to do a lot of things it has chosen to do so because of the community wants to do so. And that's great, which is why it's so important to sort of bring up concerns and inconsistencies in its operations. And –

DEBORAH ESCALERA: Okay. Padma –

PADMA VENKATARAMAN: [inaudible] anything more, please ask me later because I haven't finished my presentation. Thank you.

DEBORAH ESCALERA: I know, Padma. We have three more presenters, so I'm going to have to stop you. But again, your presentation will be online. Just keep in mind, the presentations are supposed to be ten minutes each. But very fascinating information here. Thank you, Padma.

Okay, are there any questions from the audience for Padma? I think we have just time for one. Okay, because there is another session at 3:00. We're at 2:35 and we have three more presenters. So thank you, Padma, very interesting. Okay, we have Pierre Dordhain from Australia. I'm sure I butchered your last name.

PIERRE DORDHAIN: [That's alright.]

DEBORAH ESCALERA: I'm reminding the presenters, you have ten minutes to present. Thank you. And we need to be out of here at 3:00 and it's not 2:36. We have three presenters. So please.

Eight minutes per person. So I apologize to those that did get cut – I mean your presentation did run long. So again, all these presentations are on the website embedded, so if you would like to take a look at the presentations, please do access them on the website. They're embedded in the schedule.

UNIDENTIFIED MALE: [inaudible]

PIERRE DORDHAIN: [Yes, I don't want that, actually.]

DEBORAH ESCALERA: It only allowed me to upload ten, but I'll see tech after this session to upload the additional five.

PIERRE DORDHAIN: Hello, everyone. My name is Pierre, and I'm from Australia as you can probably tell from my dreadful accent, and today I'm going to present on amending UDRP. Some of you may or may not know what that is. Interestingly enough, I'm going to have to change slightly what I'm going to say in light of a couple of interesting conversations I've had since my time at ICANN.

I spoke to a man called Jeff Neuman who's actually on the Intellectual Property Constituency, and after discussing my presentation, he said, "Look, that's actually a very interesting issue that we're going to look at the next ICANN." So they've already got sort of a proposed amendment. So I guess what I will be doing is discussing the issue with the UDRP, as he's sort of already aware of, which is a shame. And yeah, I'll talk you through that.

So essentially, we all know, we're all here. Websites matter. They're of a lot of importance. So throughout this presentation, I think what's best for you all is to consider sort of in light of a few certain people. So if we look at this person, this person and this guy here, they all have one thing in common, and they're all small business owners. Essentially, what I'm saying is let's look at it from the perspective of people who don't have unlimited funds, and I guess it highlights the point a little bit better.

So in the interest of time, we won't go into too much about that, but essentially, small business owners do make up about nearly 78% of – well, not users, but 78% of small business owners do use websites or intend to use websites. It's a pretty prevalent issue. So on that note, how do we protect these users? If a small business owner wants to register a domain name, how do they protect themselves? This is primarily through the UDRP. This is the Uniform Domain Name Dispute Resolution Policy in ICANN or with ICANN.

Let's consider a scenario. We've got small business one who's got www.webuild.com – he's probably some kind of construction worker – and second one is www.webuildd.com. So we look at that and we think there might be an issue there. So how does this guy resolve that issue? Well, we look to the UDRP. So he'll have to make a complaint and he essentially has to demonstrate three things.

Firstly, that it's identical or confusingly similar. So if we think about that, I don't think there'd be too many issues there. Secondly, that there are no rights or legitimate interests. That would depend on whether they have a registered trademark there, but we won't go into that. For the purposes of this presentation, we'll look at the third element. That is whether it was registered and is being used in bad faith

Now to establish the third element, the onus is entirely on the person making the claim. They have to prove on the balance of probabilities that when it was registered, it was in bad faith, and when they're making the claim that it's still being used in bad faith.

To establish that, that's really about establishing intent. So at the time of registering the website or at the time that the defendant registered the website, they have to show what they were thinking at that time. You might think that's a bit of an issue. Particularly if you think that the time of registration could have been six months ago, if not years ago. How do you look back in time and establish what that person was thinking when the burden is on you?

Let's look at a recent example. I won't bog you down with all the details, but essentially in this case, I don't know if any of you have heard of the brand ALO. They're an international brand, they sell mostly active wear, fit wear, that sort of thing. And what happened was the defendant registered a website called alo.com. So the claimant didn't have that. They had aloyoga.com. But when they looked at the website – so if anyone typed in ALO on the Internet which you can still do now, you come up with alo.com or alo.net. And on that website, all they have is a bunch of clickbait. I don't know how familiar you are with that, but essentially, it's just advertisement, somebody clicks on it and they generate revenue for themselves.

So what the claimant argued was they were used in bad faith and it was registered in bad faith because they just wanted to use their global brand to attract people to click on their website, click on the clickbait and make a bunch of money.

However, essentially, that failed. They were unable to show two prime issues. Firstly, they couldn't establish that the defendant was aware of the brand, and essentially they couldn't establish what was on the mind of the defendant at the time of registration.

So again, this just sort of highlights even though ALO was a huge brand, lots of resources than your average Joe, they still couldn't prove what intent that person had. So how do we change this? Well, I had a proposal, but after speaking to a couple of people, essentially, that's not likely to happen. What they are likely to do is change the "and." If we go back to the elements here, they're going to change the "and" to an "or." What that would do is it would make it much easier for a claimant to establish the bad faith element, because they don't have to establish both the intent at the time and the intent later, they'll only have to establish either the intent at the time or the intent later. And that will just make it much easier than it is at the moment. So yes, that concludes my presentation. I hope it wasn't too long. Any questions?

DEBORAH ESCALERA: Thank you. Okay, so we'll take one question from the audience.

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED FEMALE: [inaudible]

UNIDENTIFIED MALE: Okay, how about now? Okay, because of time. Interesting presentation. [inaudible] for the record. I would have loved to get your opinion on what you think are some of the inherent flaws in the current UDRP process, and the statistics that you showed I think on slide two [inaudible] reference to that. Yes, that slide. Otherwise, nice presentation. Thank you.

PIERRE DORDHAIN: Certainly. So just for your second question, what statistics were they? Sorry. I'm not sure what statistics you're referring to.

UNIDENTIFIED MALE: [inaudible]

PIERRE DORDHAIN: Oh, right, yes. That was basically just to highlight how important websites are to the use of businesses, it was nothing overly significant. But I think that was from the Bureau of Statistics in the U.S.A. So if you want to look into that, have a look. So the inherent issues with the UDRP at the moment is really just about its application. So if we look at how difficult it is for a claimant to demonstrate that element because it's up to them to show it, what we call the burden of proof is on them to demonstrate the element, and that's on a balance of probabilities.

So if there's more chance than not that, say, a person registered in bad faith, then the claimant has proved that onus and they've satisfied the element. Because the third element which is about intent really, it just makes it very difficult for them to show that when it's sort of in the mind of the defendant. So that's what I suggest is an inherent flaw, given that they have to do both at the time and current, when it's usually much easier to show the current or at the time.

DEBORAH ESCALERA: Okay. Thank you. We're going to have to forego questions, and then probably forego questions for the next two presenters. And then perhaps convene outside if you have questions. Our next presenter is Razoana Moslam from Bangladesh. Razoana?

RAZOANA MOSLAM: Good evening, everyone. My name is Razoana Moslam, and I was expecting to talk about ten minutes, but now I think I have six minutes left. Anyway, it's just I think the slides are a little bit dark, but my topic of my presentation is basically the Internet governance. It's an analysis from the developing countries' perspective. Like as a developing country like Bangladesh, like other developing countries who are still struggling with Internet, getting connections and the governance sort of things, how they are participating in the main issues.

The first, it's just as brief history like what are the basic laws that describe the rights in the privacy and protection sort of things. We had the UDHR which is the Universal Declaration of Human Rights in 1948. Then it came out as a European Convention of Human Rights, then the American Convention of Human Rights, then on the African perspective we have African Charter on Human and People's Rights as well.

But for the privacy and protection, you can see that there are OECD guidelines. That's basically the privacy and protection, basically the personal information sort of law that deals with that. And then we have the directives of European Union which is basically on the protection of individuals with regards to their personal data and then the free movement of such data.

Now, what roles are developing countries playing in the internet governance sort of things? Firstly, developing countries are mostly part of the international organizations like intergovernmental organizations like ITU, WTO, these sort of things. But such organizations are frequently – they pay attention to the connections about like communication policy and development. And then we have the developing countries that are really underrepresented in nontraditional decision-making venues, and for example, in ICANN. Then we have other technical groups where the representation is not as much as we expected it to be. Then when it comes to take the decision-making thing like when it comes to the governance decision making thing, the developing countries are not represented at all, by the way.

So then we have the other Internet issues in our country itself is like cybercrime, it's most common one. Then we have intellectual property rights, that's very common as well. There are very vast concept about these things. Then what are the barriers that developing country are still – their participation are – still to be overcome? The first one is – there are some recommendations that I have made that if you follow these sort of policies, then the participation can be improved a little bit.

So first, we have to build a technical and policy capacity. We have to increase the policy awareness of the people. Then we have to strengthen our national policies that we have. Then we needed some financial support as well to build that sort of support, and we need to participate in international policy making things, for example, international technology-related policies. We have to participate in those sort of things as well.

Then these are some other proposals that I have made. I'd not go all of them, but just a brief of that, we need to adopt some sort of treaties internationally so that the participation can be ensured more. Then we need to participate in ICANN, IGF, then ITU. We need to increase the participation here as well. And then we need to promote the international connection, like cooperation of the cybersecurity. We need to increase the cooperation between the countries. Then we have to offer some prizes for solving critical cybercrimes, and for example, like in developing countries, they are still struggling with cybercrime sort of issues. So we need some help from the developed countries as well so that we can resolve those issues.

And then we have the liability. We have to create the liability regime so that the burden doesn't fall into just the country itself but internationally as well. So this was the brief of my presentation. I want the developed countries and developing countries to work together to make a connected, better world. Thank you so much. I hope that was brief.

DEBORAH ESCALERA: Thank you, Razoana. Again, if we have questions for you, perhaps we can convene outside. And I truly apologize for you, final presenters, because I feel like you've gotten short changed with the time. Okay, our final presenter is Sophie Hey from Australia. Sophie.

SOPHIE HEY: While my slides are loading, I'll just say it quickly. So as mentioned in my introduction, I'm from Australia. I've just finished my final year of law. So the work that I'm going to be presenting here is about how to engage youth in ICANN. So the approach I've taken has been based on my work as a tutor at the university for voluntary support programs for students.

The topic of my presentation is one world, one Internet, one classroom. First of all, we go to ICT in schools. So at the moment, we have – there's been a global movement to incorporate ICT skills in education through primary schools and high schools. To do this, there needs to be a certain amount of resources available to the staff and teaching staff to be able to do this.

My suggestion is that for ICANN to be able to engage with the youth, they look at moving towards expanding the scope of ICANN Learn. So as you'd all be aware, ICANN Learn provides a range of facilities and materials to be able to introduce people to ICANN and the different work that they do. However, it's targeted at an adult audience, and it's targeted people who were already familiar with ICANN in some sense. They've had someone explain it to them before they go and look for ICANN.

However, given my previous point that we're looking to have – that schools are introducing ICT programs in schools, ICANN looks at developing ICANN Learn so that it has school-aged learning activities on ICANN Learn, so that from the beginning and during school, teachers have access to resources that they can use in classrooms and teach children about how ICANN operates in a way that's relevant to them.

So the reality is that we're now looking to have Internet natives. The people who are in NextGen as it is, most of us have grown up only knowing having technology in our lives, and this is only going to increase moving forward. So by having these programs available online like the NextGen program, potentially looking to expand programs so that, for example, academic competitions for children – it's not unfamiliar to other global organizations such as the U.N., for example, it have programs that engage youths before they get to 18 years old and have options for them to engage with other people their age around the world.

So again, I haven't actually worked out how to adapt the resources into school-aged resources for children, however, it's something that can be considered, especially given that the role of the Internet in our lives is only going to continue to grow as we move forward, and making those resources available and ready and providing them from ICANN to schools as a ready-to-use resource enables ICANN to engage with people before they turn 18 and are able to engage in an adult capacity in programs such as NextGen, and then later on through fellowship programs. That concludes my presentation. In the interest of time, if anyone does have questions, I'm happy to take them outside.

DEBORAH ESCALERA: Thank you, Sophie. Perhaps you can engage with Betsy with ICANN Learn. It's very fascinating. Okay. Thank you, everybody, for joining us today, the audience members and the online members. I would like to ask the NextGen to please clean up your areas here. Thank you very much. Good job.

UNIDENTIFIED FEMALE: We still have four minutes left.

FRANCIS NWOKELO: Four minutes left? Let me finish my presentation. I wish what happened to her happened to me. I would have loved it. I say what happened to her, I wish it happened to me. I'm the person who couldn't have a presentation [inaudible] I wish it happened to me. I would be so happy, because she spent a lot of time.

[END OF TRANSCRIPTION]