FINISHED FILE

APrIGF 2017
"ENSURING AN INCLUSIVE AND SUSTAINABLE DEVELOPMENT IN ASIA PACIFIC: A REGIONAL AGENDA FOR INTERNET GOVERNANCE"
BANGKOK, THAILAND
JULY 27, 2017

ROOM 202
TRENDS IN CYBERCRIME LAW: COMMON LEGISLATIVE DEVELOPMENTS AND CONCERNS IN THE REGION
12:30 AM

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
www.captionfirst.com

***

***

>> RAMAN JIT SINGH CHIMA: Just checking. Can you hear? Great.

Welcome to the session on cybercrime law and legislative development in the region. My name is Raman Jit Singh Chima, I'll be moderator for this. I'll give a little bit of context. We have three participants here. One will be joining us remotely. And also one person from here in the audience who will also be talking a little bit about a project, but let me introduce everyone who is here in person. Gayatri leads the project, a lawyer by training. Malavika Jayaram has been associated with the society. And Apar Gupta is a public policy fellow, and also a legislative aid to a member of parliament in India. Joining us remotely is Haroon Baloch, leads policy from Bytes for All and will be joining us remotely. We also have one more person assisting Gayatri, who is there.

Let me give you further background about why we got

together here. You all heard specific discussions around cybercrime legislation, whether it's section 66A, discussions around the earlier prevention -- the ECB, which is now the cybercrime act there. You've had discussions around countries as diverse as the Philippines. And what's been interesting in many of these conversations is that it's very rare to discuss at one level are the trends missing legislatively across the region. Are there top level concerns with respect to how this impacts rights, particularly privacy, free expression, others that we hold dear. They tend to be either about cybercrime cooperation, particularly in the law enforcement space, or there may be conversations around cybercrime trends in terms of number of crimes and the idea that we need to take urgent action. But it's a very different discussion on the actual content in many of these very specific national conversations.

The idea of this session is to talk a little bit about what each finalist is seeing in terms of top level concern in their sphere of responsibility, and with that, we'll first start out with Haroon, who is going to talk a bit about Pakistan and what's happened to the cybercrime law there. Haroon, just going to check if you can unmute him and let him speak. Haroon, are you there?

While we fix that, I want to start with Ananta. As we discuss the cybercrime legislation that has been passed, there's a draft law that's being proposed. One that most people has not been tracking again has been a particular bill proposed in Bangladesh. I know there are participants from Bangladesh here, many of who may have thoughts about the current forms of the law. But a little top level analysis in terms of what the contents of that law talk about, and it's interesting because it's a law which is specifically titled digital security, although it came at a original cybercrime conversation. So with that, I'll give Ananta space to give a few comments and we'll try to bring Haroon in to try to talk about Pakistan.

>> ANANTA SHARMA: Hi. So the draft, the security act -- okay. Hello? Can you hear me now? Hello? Hello? Yeah.

So the draft, the security act 2016 --

>> RAMAN JIT SINGH CHIMA: I think we have Haroon. Can you hear us? Haroon, if you can hear us, just indicate yes.

>> HAROON BALOCH: Yeah, I can hear you, but there is a lot of noise in the background.

>> RAMAN JIT SINGH CHIMA: Let us try and figure that out. If you could mute in the meantime, that would be great.

>> ANANTA SHARMA: Hello. So the draft of the security act, we all know that the Bangladesh law already exists. And because of the growing concerns regarding the security in Bangladesh, the government decided to form the digital security act, which is a draft as of now. So upon my analysis, I stumbled upon a lot of troubling definitions, first of all, there are a lot of definitions, which risk freedom of

expression. They also allow for (?) in the name of national security. And then there is the digital -- then there's the digital security agency, which is the competent authority formed by the government, which looks into all the digital security concerns in the country.

And that digital security, the director general of the digital security agency, he has the authority to order any private entity to give away information in matters for national security. The fact here is that there is no kind of judicial oversight whatsoever in this particular draft. Lots of violations for freedom of expression and the definitions are very broad. So basically, appropriate safeguards have not been provided for the citizens. That's it. Thank you.

>> RAMAN JIT SINGH CHIMA: Thank you, Ananta. Do we want to try Haroon again? Haroon, if you can unmute, try speaking now. We will try to see if your audio is working fine. Haroon, speak now.

>> HAROON BALOCH: Hello?

>> RAMAN JIT SINGH CHIMA: Great. We can hear you, Haroon. Go ahead.

>> HAROON BALOCH: Thank you. Cybercrime, a prevention of electronic crimes act 2016. The government has done everything to stifle expression in Pakistan, and these can include everything from monitoring activities, summoning social media users, the confiscation of their devices. And even in some cases early in this year, we are seeing the adoptions of five bloggers, and they were subject to charges as well. Then we have also seen the cases where journalists and activists were also attacked on phone calls for their expression, and especially their political dissent, and some of the terrorists who were also making commentary on legal issues were also taken and their activities were monitored. And especially since January of 2017, a comprehensive campaign against blasphemy has been in progress, which has the (?) of the interior Ministry and communication authority, who publicly have been making statements and media campaigns and sending mobile messages to warn social media activists, users for producing and sharing of, quote unquote, objectionable content. And now this objectionable term is very vague and broad. Like anything can be referred as objectionable content.

This may also include less blasphemy content. Any criticism of military and other institution, criticism on courts, or criticism on friendly states, which is the language actually of the cybercrime act in Pakistan. Specifically, these etymologies are mentioned in section 37. However, the government is more focusing on social media users, getting out, and expressing their political content online.

So, this all begins from the adoption of five bloggers, and taken into custody for three weeks and also subject of torture. During this custody, a smear campaign was also run by the cyber

armies promoting agenda, and director for establishment and that campaign was to paint these bloggers as blasphemous, who were truly criticizing the military and other institutions for their wrongdoings or their policies. This campaign (?) against progressive in the country, because it certainly has defectors of government and the institution in general, and it has cultivated the environment, which has resulted in violence cases as well. We have seen one of the cases was related to one of the students from a university, and he was actually killed because of his expression and criticism on the university administration. They named it blasphemy, which was the wrong allegation leveled by the people who were actually against him.

So in the meantime, a petition was also registered when the blogger that was abducted. The judge explicitly expressed his religious bias during the case and ordered the government to publish blasphemy expression online. He remarked that he would have blocked all the social media to protect the sanctity of Islam.

After that, on the data chains of the interior Ministry, FIA, the Federal Investigation Agency, and the authorized investigation agency on the cybercrime act of Pakistan, and the anti-terrorism wing, they started crack down on social media. They have been monitoring and cracking down on social media users and summoning them at police stations for investigations. So also, you know, it's very threatening when states start -- (?) these sort of campaigns to stifle expression for what they believe it's an additional freedom of speech being exercised by people. So in this context, government of Pakistan, the FIA, they have produced at least 100 activists and social media activists and political activists, and also this includes the names of some of the journalists who were active in criticizing and exercising political dissent. And this is being made public on social media.

So what they've been doing, these people whose names are in the list, they are being projected as blasphemous. You know, really sensitive in Pakistan, and we have seen that anybody who was being presented as blasphemous, the decisions of these allegations are done on the road, and then sort of -- it's a very threatening trend.

Another thing that we are seeing as it relates to either cyber armies who are closely affiliated, their job is to harass, bully, intimidate social media users expressing political dissent, and make disappear any narrative, confronting a certain narrative. So we have also seen a rise in blocking of all content as well, and we have seen that telecommunication and FIA, they are making excessive efforts to Facebook and YouTube to block and censor online content under -- the cybercrime bill of Pakistan. So these all are freedom of expression in Pakistan, and definitely they are having chilling effects on the expression.

>> RAMAN JIT SINGH CHIMA: Thank you so much for that, Haroon. We might come back with some specific questions as well, based on how Pakistani authorities and others are using the law there. But with that, I think that's actually a good setup for Gayatri, who has been tracking developments across the region. Many of these happen in the shadow of legal frameworks. Can you talk a bit about what members are seeing as the framework you're working on?

>> Gayatri Khandmadai: Thanks, Raman. Let's leave the question of what we mean by cybercrime. That's a different discussion as such. But one thing that's clear is that the legislation on cybercrime is oftentimes not one comprehensive legislation, yeah? Cybercrime is pretty much broken and discovered by a whole gamut of laws that we all have in different jurisdiction. Another point that I wanted to clarify is that it's not only laws, like, for instance, the ICT law in Bangladesh or the PECB law in Pakistan. It's also the traditional offline laws we have. So, for instance, the penal legislation, any other legislation that has been traditionally used for offline activities or crimes is also used in online spaces. So what in a sense happens is that they're sort of convenient. When the government wants to use an offline legislation to address an online activity, they do that, and then when it helps them, they use the online act as well. So, say, for instance, if you have a specific cybercrimes act, you use the cybercrimes act, but you also use the penal act, and the instances of the Penal Code, you use that as well.

What happens is oftentimes these two acts are not really complementary. They have contradictory provisions. Definition of crimes itself can be quite different in the two acts here, so then it creates a lot of chaos. Now, this is also what we're facing in Pakistan as well as Bangladesh and India and Myanmar, Thailand, Cambodia, many of the countries in Asia. Therefore, we kind of at APC, what we decided was we kind of took a look at all the different activities that's being criminalised on the Internet, and we decided to have a meaningful sort of analysis or understanding of it. We decided to pick one particular right and look at it a little more seriously. We decided to go with the right to freedom of expression, because oftentimes, that's the right that's most targeted online, yeah?

And what we decided to do is, we also decided to break it up a little bit, because it's hard to look at different aspects of legislation right away when we're dealing with one particular right.

So for the first stage, we decided to look only at the laws and how the laws came about and what they are saying. There's a whole other side to it, which is how the laws are applied, and that's the point Haroon was making as well, because a lot of these definitions are extremely vague and overbroad. So then how courts are interpreting it, whether you see sort of a

reaction there or no. What we certainly can say is that the online space kind of exploded, no? And states as well as people found -- are still finding it hard to sort of reconcile or values, how we exist, otherwise, with what we are given space to do. And in the rush to kind of address that, there's a lot of things that's being done without really thinking through in the sense of what was going to be a long-term impact of that.

Now, with this study, of course, Asia is too wide, so we picked about six countries in Asia. We're looking at India, Malaysia, Pakistan, Myanmar, Thailand, and Cambodia, and this study, we're doing with digital Asia help as well as the Southeast Asian Press Alliance. We'll be starting -- the starting point is to look at a range of expression that's being criminalised. So what is the basis on which it's being criminalised. For example, blasphemy, hate speech, defamation, national security issues, public order. These are all some of the most common ones. But what is also striking is the attack on sexual expression, specifically through two aspects. One is obscenity laws, and two is outraging modesty of women, which you see in traditionally British colonized jurisdictions.

We're looking at the definition of all of these different aspects, and seeing how these terms are being defined, and what kind of expression is being covered by it. But another very important aspect of this is to look at what is the punishment or the penal provision that's being ascribed to each one of these offenses, and to also get a sense of let's take that for online spaces, so if I say commit blasphemy online, then what's the punishment that's being prescribed for me? If I commit blasphemy offline, what is the punishment being prescribed for me and how are they dealing with it?

Now, the reason why the study is important, or studies like this are important, is that throughout Asia, we are sort of in a -- in terms of how we deal with the Internet from a legal perspective, and for us to get a perspective of what is the jurisprudence that is going to evolve as a result of all of this legislation is really crucial, and this sort of initiative is not only new to Asia, because one of our members, the social media exchange in Lebanon has already done the study for that region, and there are studies like this that are ongoing for different regions. It's really important for us to then compare these studies across regions and see where we are falling, you know, in different places.

So I think that's sort of the starting point. But I think another really important piece to this puzzle is to look at how strategic litigation and how jurisprudence around Internet rights, which is essentially the human rights that we exercise in digital spaces, is being shaped.

>> RAMAN JIT SINGH CHIMA: Thank you so much, Gayatri.

[Applause]

Gayatri's last point is perhaps the most understated, the

litigation efforts across the region. One of the challenges we all face is there is very little opportunity to sometimes learn about what people are doing. The best lit gators are not the ones who will be there at EPIG. They are often the ones involved in cases, but will not be able to speak to this. But that's the challenge. How are we able to share this, how can we find out more about what's going on, not in sometimes the law, but in terms of how legal frameworks are being used.

I want to toss it to Malavika. Sometimes people say, is there an Asia region to study when it comes to this? How can people collaborate and share and work on this? I know you're partners with EPC on this, but perhaps we talk about next how people respond to this and how can we both, not just in the Indian government space, but perhaps in the public interest community, be able to balance effective analysis of what is happening in the cybercrime space and protecting the rights that we see so valuable.

>> MALAVIKA JAYARAM: Thanks, Raman. So we at the Digital Asia Hub by design, we're a hub, so we'll never have 50 or 100 researchers working in-house. The idea is that we partner with in-country experts who understand their context, their region, their language much better than anyone we could hire, so the whole idea is to grow the network to work with experts in countries and also to sort of share knowledge. So we're all about knowledge sharing, capacity building and doing networked research. So those are our three core AMs.

One of the things that's really interesting in the cybercrime space is -- well, a couple of things. One is that I think you often conflate cybersecurity and cybercrime. People talk about them as if they're the same thing, when actually, they're not. You know, you can say that certain elements of cybercrime are part of a cybersecurity strategy, but to think of them as the same thing and to refer to cybercrime law as if it's just about security, or the other way around, I think it really does the whole field a disservice when people don't even understand what it is we're talking about.

Gaya alluded to the fact that even the definitions can be really complicated and we don't all agree on what it is, but I think we can agree at a very fundamental level that cybersecurity and cybercrime are not the same thing, and they have elements in common, but they are not the same thing.

And I think what's also really interesting is that at a time when crime, the old-fashioned crime that didn't involve computers is at an all-time low in most countries that we look at. People feel safer than they ever have been. Other kinds of crime are diminishing everywhere, despite the rhetoric in a lot of countries that oh, my god, it's all scary, and there's terrorism everywhere, and we need to shut everything down and kill every kind of freedom we have. But what you see in parallel is just when, you know, regular crime statistics are

falling to all-time lows, cybercrime is going through the roof. So regular crime might be 10% in a country, but 70% is now cybercrime. And I think what's happening is you see a little bit of a gap with institutions that used to address this.

Policemen, cyber criminals are kind of a new thing for them, right? Some countries are better at it than others. Singapore may be really good at it. Myanmar may be very terrible with it because they haven't had to deal with it before. It's very sophisticated, it's new, it's something they're trying to get a hold of, and it also comes at a time when in a lot of countries, we're defunding these kinds of activities. We're investing less money in critical infrastructure, we're investing less money with public services. Policemen are getting lower and lower wages. But we somehow magically expect them to have Ph.D.s in cybersecurity and cybercrime overnight. They don't have the tools or the technology and they often turn to private companies to help, you know, which comes up with a whole set of other issues.

I think the third thing that's really interesting for me when I look at it across the region is we talk about the need to tackle cybercrime, but we don't talk about the need to have data protection and privacy standards and laws in place in parallel. So a lot of cybercrime either comes from hacking, it comes from theft, it comes from, you know, all kinds of errors, fraud, impersonation, all kinds of other things. Many of which can be stemmed, if you have standards around data protection. If you have principles saying data minimization, don't collect more than what you need, delete it once you don't need it anymore. Why are we creating stockpiles of data that are there for hackers to want to, you know -- you know, you create this honey pot and then say, oh, no, you should be disciplined about not attacking it. So that's completely unrealistic.

The same countries that are pushing for really strong cybercrime legislation, if you ask them what they're doing about data protection, it's like oh, I never thought about this before. So I think that kind of disconnect is really crazy, because we keep incentivising and encouraging the collection of data. We tell people that data is gold, and data is the new oil, and without data, you can't do anything. We have this sort of fetishisation around data, and at the same time, we don't create systems that prevent it leaking. We don't, like, tackle the cybersecurity side of things and the data protection side of things, but we want magically crime to be eradicated overnight. So I think if we want cybercrime legislation to work, Gaya mentioned how intersectional this is and how the problem bleeds into other areas that are not just about cybercrime, and where the acts that are criminalised are also criminalised across different pieces of legislation. They can be economical. I live in Hong Kong. Try and open a bank account if you're an NGO. Good luck. They assume you're a criminal from the get-go

and they put you through all kinds of compliance checks, which is great if you're trying to combat fraud and money laundering, but what about the little guy on the street who isn't actually a cyber criminal, but is being treated like one?

So the solutions come from different sectors, often disproportionate, and we know that when you sort of mention crime, it's a very passionate thing. People sort of think we're, you know, cleaning a country of crime, it's a big public service, we want to secure our borders, we want to prevent terrorism, these are all horrible things that are happening. So, of course it's a very visceral response, and people will accept all kinds of invasions into civil liberties when you say, we're under threat all the time. We have a traffic. It's threat level red. It's not even regular red. It's not even orange. When we start coming up with this scary distopian rhetoric. And are we criminalising behavior that really shouldn't be on the radar at all.

We also know that cybercrime is used for attacking things that are socially conservative issues. You don't want pornography, even the kind that doesn't tackle children, even like regular good pornography for entertainment, you know. Oh, I only read "Playboy" for the articles, that kind of pornography. Even that gets swept up in this thing. So people want to criminalise different kinds of activities that they deem anti-social. You want to crack down on LGBT communities, why don't we use cybercrime rather than using oppression laws. Right?

So I think when you look at cybercrime, you need to have a very holistic lens about what we're classifying as crimes, could they be better off dealt with as civil issues? Maybe there's a monetary damage that's adequate. You don't need to criminalise this act at all. I think that's why projects like the one Gaya mentioned, this impact project, is so important because it's literally sifting out those strands and saying these things should fall into a criminal bucket. These things are really much better off dealt with as civil things. We have systems, we have laws that deal with them. We have institutions that are really good at dealing with economic issues, right? Or consumer protection issues. Or negligence or fraud. Why are we not sort of seeing this as sort of a spectrum?

So I think making everything a criminal act just because it's easier to legislate, it's very hard to push back against. I think it ends up being -- it has a tendency to lean towards the draconian. It needn't. There are good examples of how that can be done, but I think there is this tendency of overcriminalising and having very broad legislation. You have to have some sympathy for lawmakers as well, right? Because you want to keep definitions as broad as possible to cover things that you don't know yet, right? Because criminals are evolving. They use technology way better than official government

institutions do. So it's always a bit of an arms race. You're always trying to play catch-up, and you try to crack down on one kind of activity, it's going to move to a different forum. It's kind of like whack-a-mole, you whack this one, it opens up somewhere else. It's a constant game of catching up.

But I think when you look at everything through the lens of crime, you're actually going to lose out on a lot of things that could be very well-solved using other instruments that we already have. So I think this kind of project where we're looking first at the impact on free expression and saying are there bits of expression that are being criminalised that shouldn't be, that's sort of one's starting point. But you could look at other kinds of issues that are being criminalised that really have no business being considered a crime at all.

So I think those are the kinds of issues that we want to look at, and I think we're really interested in looking at it at a regional level, because if you look at it purely through a national lens, there are certain things that might make sense that might justify it. But I think if you telescope it out one level, you can actually look at trends, even simple trends that are really valuable, like who are the vendors selling all these solutions to governments, right? Who is providing all the surveillance technology? Is it the same two companies going and convincing government that we really need to use surveillance as a tool to crack down on crime, not because it's effective, but because they have a product to sell. And then governments also play this arms race with each other saying, oh, you know, Singapore has it so maybe we should then we can become like Singapore in every other way. We're not doing the things that turn us into Singapore in other ways. We're not creating smart cities. We're not having enabling legislation about other things. We're not providing social welfare and good healthcare, but we want to be like them only when it comes to tackling crime.

So I think it's really important that we look at good examples and bad examples, and I think I'll end by saying in Silicon Valley and in other parts of the world, there's this huge sort of mantra among start-ups that you should fail faster and you should, you know, talk about failure, and failure is a great, you know, wonderful thing. There's a huge positive spin. And they come to Asia and say we should do the same thing here, and I think, do you understand anything about Asia if you're saying we should take pride in failure? People will kill themselves before admitting they failed. You know, we're embarrassed as a society about so many things. We're not going to admit that we failed. You lose your job in a government hierarchy if you say you failed. There is no culture that promotes people sharing the terrible lessons, right?

As a community, as a region, we need to get really good at talking about this, and, you know -- I always use this example

saying that if you want to talk about things that can go wrong in the Internet space and start-ups, if you talk about failure, it has no resonance in Chinese cultures or Indian cultures, but if you talk about it as gambling, saying, you know, we gamble for Chinese New Year, we gamble in India, we take risks, that kind of risk taking is good risk-taking, right? And people can say, oh, yeah, that's how start-ups work. Some win, some lose when you talk about innovation. Why can't we find Asian metaphors and Asian things that are more relevant to our social context? We're not just importing some other person's idea of what it means to tackle crime and to tackle these sort of social issues.

So I think that's what we're trying to look at across the region, to look at trends, to look at ways that we can make this conversation a more equitable one and something that actually has resonance for us in the region, to tackle the kinds of crimes that might be emerging here as a solution to things that aren't working elsewhere.

So, I hope some of that will help solve the problem.

[Applause]

>> RAMAN JIT SINGH CHIMA: Thank you for that. I'll book end a couple of things with privacy, data protection. Often, maybe the same officials, but they won't talk about it in a similar way. There's a unique opportunity this year, because the international conference is coming back to the region after a long time, and they're having a meeting in the region, and you should ask your governments how they're engaging, who are they sending. I find it very telling that many governments who are willing to send officials everywhere do not send people for this conference, if they don't have a data protection authority, and even there, they limit their resources. We have talked about data security and cybercrime being different, and that's one thing, again, I think many people who are not officials in that space, may be the same people, but they will often try and say that let's talk about differently, or let's do everything together.

We started a bit late because of the previous session, so with that, let's take questions. Just in the interest of time, maybe we'll collect two or three, and then take it to the panel. I encourage you to address any questions through the participant if you have any questions for Haroon about what's happening in Pakistan or any other points the panelist mentioned. Please announce yourself, and use -- there's a mic there.

With that, maybe we'll collect three questions.

>> Can I start? I am from Pakistan. This is more a comment. Actually, you can't have a culture value as a standard for whole world. In one part of world, child porn production is a subject discussed widely. But in another part, you can't discuss, because you talk about -- because Pakistan, they are banning and restricting the access to that content. Not

encouraged for children to see.

My question is about cooperation of cybercrime, more important for me as a discussion. In recent past, only one sort of -- I can say that Budapest, because most of the country (?) but what actually I suggest is to you -- I can say that starting from article 51 and followed by article 2 and 4 and imposing -- taking advantage of article 27, and take care of these like whatever is happening in cyber space, to come up with some message for cooperation in cyber space. Thank you.

>> RAMAN JIT SINGH CHIMA: One comment, one question, one session. Other speakers? And I ask you to limit yourself to one question or comment, if possible, just in the interest of time.

>> Francis, National Privacy Commission. On behalf of the commission, I guess I'd like to thank the panel for recognising the importance of data protection and privacy and the whole spectrum of how these things happen.

Just want to note that, at least in my experience, where cybercrime legislation is headed, the other issues which are definitely within the realm of cybercrime, such as child pornography and I guess hate speech, and use that to try and rein in other dissenting speech, and sometimes that hate speech is to nonstate actors. So there are people who try to suppress dissent using agents that are not part of government.

I guess the question is, how do you see data protection legislation moving forward in the region, because we'd like to reach out also naturally and create a more stable ecosystem.

>> RAMAN JIT SINGH CHIMA: I think we'll take one more question.

>> Hi. Mine is more of a comment. I work with an organisation called Point of View in India. We're actually working on a final draft of research, in which we looked at section 67 of the Information Technology Act. It's a multi-pronged -- we used multiple methodologies.

>> RAMAN JIT SINGH CHIMA: I'm sorry, can you explain to those who are not familiar?

>> Sorry. It says that publication or transmission of obscene material using an electronic medium is a crime. That's the provision, and we haven't specified what is obscene or any of that. So in recent times, particularly section 67 is being extensively used, and using media reports, national crime report bureau data, case studies, we have -- we worked on our research. Some of the things which came up is that section 67 in recent times is using -- is being used more and more as a tool for censorship, including political, religious, as well as sexual censorship in the online space. It's also used often by politicians to silence people who speak up against them on social media. It's also being used as a dust pan of sorts for a crime that has even more of a digital component. The problem with this is multi-pronged. It's not rights based, because you

don't say what is obscene. It's also very moralistic.

We're actually presenting the research along with our partner organisation from Nepal and Sri Lanka at 4:00 today in this room. It's an open forum, so please come for it. But I thought I should say a little on this here. Thank you.

>> RAMAN JIT SINGH CHIMA: Thank you so much. So we had two comments and a question. One was on, you know, commenting about different social cultural context, but also a comment later about how laws on obscenity are being used on people in the region and more data on that, 4:00 p.m. in this room later. And then a question really on cross-border cooperation, can you move beyond the Budapest convention. Should the UN intervene in this space, and where are the protection laws going to. So would people like to address it?

I'll take one thing on Budapest. Those who aren't familiar, the Budapest convention on cybercrime was an attempt at trying to show cybercrime cooperation uniform standards, and not just in Europe. One of the few treaties which the U.S. signed on to and many other countries in the stages of potentially signing on. Many of you who follow international discussions on this are familiar that the U.S. government has been, at least in the previous administration, very keen for many countries in the region to sign on. I know succession talks involving Singapore and India and others.

What might be of particular interest to communities outside of government and societies that there's actually an additional protocol being drafted for the Budapest convention, which is being formally discussed this year, which would be about legal assistance and where can companies and others cooperate with entities. Many law enforcement people would love that and many lawyers, and I am a lawyer by training, and I also really like that. It's also basically law enforcement directly cooperating with companies, and that can place people in particular situations, and that's one thing where it might be for many organisations in this region to engage. I can share from access working with other organisations, we're just starting to engage with some of the U.S. and European discussions on this. It might be very good for an Asia Pacific in whatever sense civil study conversation on where countries would like to go to that.

There were two specific questions out of that, should the UN be involved, and where is the legislation going. So maybe first one to you, Gayatri. And second one, Malavika, would you like to talk about data protection?

>> Gayatri Khandmadai: About the UN, that's a loaded conversation. We'll need a whole hour to deal with that, so let's park that for now. I wanted to say about the data protection law. That's actually a really good example from the region we have for addressing data protection, right? Indonesia is currently drafting -- you know, drafting a bill on data protection, and we are doing research in Pakistan that Haroon is

also involved in, which looks at mapping good standards on data protection laws and combatting those good standards against what is not necessarily even a semi-good draft in Pakistan, because Pakistan has a draft, data protection act as well. So I think that's also one -- we really need regional exchange, to look at what are the overall good practices we have. What are the current examples we have from the region, you know? So I think that's one good area.

But I also wanted to take one other question about these values and cultures and all of that. Personally, I'm really wary of the Asian values, Asian culture, coming from an Asian culture perspective. I would really -- I have several questions about that. What is Asian value? I mean, there's not a single value that we can say that's across all of Asia in value. So I think we have to be very careful when we are even saying Asian experience or Asian perspective. We really have to take into the account that there are multiple experiences and multiple perspectives within that. So it's not necessarily the cultural context from that point of view, rather than realities, the ground realities that I'd be more concerned about. And it's precisely this cross-border and data protection related questions that bring us back to the key question here. Do we need more laws? Because drafting a law is the easiest thing for legislators to do. For every problem, it's okay, let's come up with a law, and that's also the easiest superficial solution they can provide us. Then we come to them with a problem, they say okay, I've come up with a law for it. But that's nothing.

So then the question is for many of these things that we're talking about as cybercrimes, we have to really question, do we even need a new law about this when there's all of these existing laws? The problem with coming up with the new laws is not only coming up with new definitions, but coming up with new limitations, which, you know, we've established over years and years of jurisprudence and international advocacy and national advocacy.

>> RAMAN JIT SINGH CHIMA: And the joke that many police officers say is that oh, there's a new law, I don't need to look at this earlier court ruling saying that I can't arrest someone because of free speech concerns. Parliament has passed a new provision. I don't need to care. So that's something that's concerning.

>> MALAVIKA JAYARAM: In terms of what's happening in the region with data privacy, two things that are influencing change here. One is the new (?) which is forcing people who are inheriting regimes from the western idea of privacy or countries that have looked to data protection standards in the European Union and cut-and-paste certain elements, principles, standards from that, who are now saying, wait, my whole law is based on the old, you know, data protection directive. Now there's this new GDP, which is overhauling everything we know about data

protection. Do I need to go and change my own law to now be in compliance, or is there going to be a disconnect? So I think the GDPR is forcing a lot of people to confront the issue, and I think companies are leading this fight as well, saying, oh God, do I now need to do different things to be in compliance because I'm dealing with data around the world, so I think companies are actually helping to push for more global compliance standards. I think the GDPR plays a huge role in what's going to happen.

And the other thing is this whole evolution of the right to be forgotten, which is a very sexy, interesting part of the debate. I think people are getting very concerned about that and saying, wait, are you going to do geoblocking on content? Does that right to be forgotten only apply in Madrid or in Europe? Does it apply to me here? And I think people also are thinking well, really, we don't have it yet, why don't we have it? Should we have a right to be forgotten in different Asian contexts? So I think those two trends that we're seeing -- and I think as of yesterday, the fact that passenger information that airlines share, that's been deemed illegal in Europe. That may bleed into a lot of discussions about how we share intelligence from a cybercrimes perspective. So I think those are three things to watch out for in terms of regional trends.

>> RAMAN JIT SINGH CHIMA: And I'll add two things to that.

>> The government claims that they are currently in the process of drafting one, although we haven't seen a draft yet. And currently, there's a very important judgment, which is going to be part of -- the Supreme Court is deciding whether Indians have the right to privacy or not.

>> RAMAN JIT SINGH CHIMA: That's what I was going to note. You notice that in a complicated way, it's either courts or enforcement actions. For example, right to be forgotten. Hong Kong was not a policy discussion, but the privacy commissioner took it up as an issue in terms of enforcement action. In India, as Ananta mentioned, the government has had a privacy bill because it's not been public, despite 11. But the Indian Supreme Court has formed a bench looking at whether Indians have a fundamental right to privacy. Whatever comes out of that will color what parliament will pass, which is also maybe a point to us, that we need to get ahead of the game. Sometimes it might be better to come up with clear principles and statements and let that take shape particularly in conversations, because as Gayatri mentioned, people will pass laws that may not always be a good thing. Even if you pass a law in the privacy space, that's not yet enough. Is data protection authority actually empowered? Is there enough resources there to other agencies to actually listen to them. These are constraints.

And, in fact, in an ironic way, we are kind of -- in the course of what Europe is doing, because the GDPR is very clear, and I think what's also clear the last two years, as you've seen from the ruling, is that European court of justice will enforce

it to the point that they will tear up international treaties if they force -- if they do not match European data protection requirements, and in a sense, we are now in that -- the European commission, in a sense, there's many governments in the region whether they're reaching a standard, and perhaps we need to get ahead of that game. Perhaps therefore it's good for us to have that particular conversation around what sort of privacy standards do we want. Is it engaging with issues, is it not just about standalone law, is it about previous provisions and how do we engage with that.

The many interesting comments, and I know we are out of time, so what I want to do is end that. At 4:00 p.m., there is research. Please come and talk to people about that. Many people on this panel have stuff to share. Access has a document on the right to conversation globally, and I know Stanford has been doing research in this space and may and want to speak to people. And I think there's one researcher you wanted to point out was working with you.

>> Gayatri Khandmadai: Yeah. I thought Gita was going to Speak. If you'd like to meet her, please meet Gita. She will be chatting tomorrow morning between 9:00 to 10:30. So please come to that session and we can talk more about the research.

>> RAMAN JIT SINGH CHIMA: I want to say thank you, not say goodbye, because we are here. Come and talk to us on the lunch break or in other sessions. Thank you, Haroon, for joining us from Pakistan.

[Applause]

And thank you, everyone, for staying.

>> Thank you all for staying through the lunch break.

[Session concluded at 1:38]

***

***