FINISHED FILE

ASIA PACIFIC REGION INTERNET GOVERNANCE FORUM
TAIPEI 2016
A NEW INTERNET ERA

29 JULY 2016
ROOM 401
9:00 A.M.
MERGER 7
THREATS TO FREE EXPRESSION AND CHALLENGES
FOR REFORM IN SOUTHEAST ASIA

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
800-825-5234
www.captionfirst.com

***

***

>> IRENE POETRANTO: Good morning, everyone. I think we're ready to start our panel now. Since the panel is moderated by an Indonesian, in typical fashion, it's ten minutes late. So, thank you more taking the time to attend our panel today. My name is Irene Poetranto, and I work with The Citizen Lab, a cybersecurity and human rights research lab, in Toronto, Canada. It is my pleasure to moderate this panel today. I am joined by five esteemed panelists from Taiwan, South Korea, and the Philippines. For those of you who are not familiar, I'm just going to give a brief background and introduce our discussion today.

So, The Citizen Lab was founded in 2001 at the University the Toronto. We conduct research on threats to free expression online, such as internet censorship and surveillance, as well as targeted digital attacks against civil society groups. Together with the Berkman Center at Harvard University, and a group based in Ottawa, Canada, we formed a initiative, and we're working in 77 countries. 44 of them, including democratic states, implement some level of filtering. We continue to do research today.

We publish reports on a Canadian company that provides web filtering technology. They have stated that their products can be used to block inappropriate content to meet government rules and

regulations based on social, religious, and political ideals, end quote. We know that Netsweeper is providing technology to Pakistan, and other countries. In Pakistan, the blocked websites are considered blasphemous by the government as well as sites that feature pornography, or political discourse, such as separatist efforts.

Our research has on covered numerous cases of human rights activists targeted by advanced digital spyware, such as FinFisher and Hacking Team. We have found FinFisher servers in Bangladesh, Indonesia, Mongolia, and Taiwan, and Hacking Team's system in South Korea, Malaysia, and Thailand. As Susan Pointer noted, the internet's global center is moving east and south, and yet some of these countries contain zones of conflict considered to be failed states.

In addition, many of these countries do not have structures in place to ensure accountability and transparency, which are important to guard against abuses of power. So, reason we convened this panel is to monitor, discuss, and raise awareness of the threats to freedom. It is important that governments are becoming heavily involved in internet governance, including establishing domestic-level internet controls. So, we'll start our discussion today in Thailand, followed by South Korea, the Philippines, and Malaysia. And we'll return to South Korea again at the end to discuss an administrative censorship move.

Each panelist will have ten minutes, followed by a Q&A session. I'll hand it over to Arthit from Thailand. Please go ahead.

>> ARTHIT SURIYAWONGKUL: Hi, everybody. Thanks for coming this morning. I would like to give you an idea what has been, like, what's going on in the past two years since the Korean military government has been in control. So, just, like, briefly the history. So in the 20th of 2014, right, the army announced martial law. On the next day, all the IP has been summoned to control the social media. And then on the next day, on the 22nd of May, 2014, there was a coup. And then after that, a lot of announcements and orders has been announced by the so-called NCPO, National Council for Peace and Order, right, NCPO, National Council for Peace and Order.

There were a lot of NCPO announcements and orders, some of them directly to media, and specifically to the internet filtering. I'm trying to find documents in English, but, like, I cannot really. But, like, so I'm just going to continue to do -- can you do this full screen? Just to give you an idea, I'm not going into details about what these announcements are specifically like, but it will give you an idea how's, like -- goals from the day one, like, since the start of the coup and how it developed into today, and also, like, how it's going to be like after our referendum to the constitution.

So, the military government appointed a committee to draft out the new constitution. And we're going to have a referendum on the 7th of August, next week. So -- and some of the announcements I will explain later. But some of these announcements will be effective even

after we no longer have the military government. So, how to start. Sorry. Okay. I will just go block by block briefly so you can see how the condition, and how it's developing. So, in the first block, this one, on day one, the NCPO immediately on that -- that every social media service provider should stop any content that anti-NCPO, right.

So that's the first block. And then following the NCPO announcement number 17, that's another specific announcement asking the ISP to monitor social media content. And if there is any content that is specifically activities anti-NCPO, ISP should stop them -- should censor that, basically. And then all this block, it's about media. So, those top blocks, it's specifically to the internet content, social media. And around this block, it's more about media in general. So, this one says the NCPO announcement of 2014 say that the media shouldn't interview academics, civil servant, people who used to work for the independent body.

And also asks the media not to criticize NCPO. This block, it say -- so, NCPO announcement number 18. It specifies there's seven categories that the media shouldn't put in the public. And also, like, related to this one about the media shouldn't give an interview. You have another announcement specifically that, okay, this one say media shouldn't interview the civil servant and people used to work for the court. This one say the court itself and the bodies shouldn't give the interview to the media. So it's, like, kind of work together.

This shows some connections. So, this thing is about the conditions to be able to use the RF spectrum to do the television. This is about data television. So there are conditions. Like, if those station doesn't go along with these conditions, their license will be revoked. And all the conditions that are basically, the television and radio should follow these announcements strictly, right. So they shouldn't interview this group of people. They should avoid from these seven category that are anti-NCPO. So these all work together.

Go to the top again, right. So in the first one, they say -- content that should be put online. And later, in 2014, they're setting up a working group. And then by this one, the Ministry of ICT later has been recalled to be under the security branch of NCPO. So this is very interesting in the way that the coup has been in control, they try to reorganize all the ministry, right. So, for example, they have, like, the security branch. They have the economics society branch. And so on and so on. The interesting part is that they actually put the Ministry of ICT under the security branch.

So, under the security branch we have the Ministry of Defense, Ministry of Interior, Ministry of ICT, and Ministry of Foreign Affairs, Right. The first one is understandable, it's external and internal security. But the latter two are about the information law. We can say that, ICT about information inside a country. And foreign

fairs, they are setting up a group of people going around the world to make understand that, this coup is necessary, something like that.

So, by this announcement, announcement 22 says, okay, ICT should be under the security branch of NCPO, right. And by that, later -- go on, right. This is interesting thing. If you follow in Thailand, probably you can see in the last year there's a lot of discussion of so-called gateway about the control of the information to be passed into the country, and probably something. By all this announcement and setting up of the -- so, by putting ICT under the security branch of NCPO, the Ministry of ICT is also setting up another working group.

And that working group to monitor social media, later setting up another working group for equipment about how to -- so, in this announcement of -- in this order, MICT order, they say because there's a lot of encryption on social media, the goal of this committee to monitor internet and social media, it's not that effective. Because they cannot censor a lot of website. So the way it works right now, because, like, Twitter, Facebook, YouTube, a lot of social media website, they use HTTPS, so it is difficult for ISP to specifically block a specific website.

The only way they can do it, they have to block the whole thing -- the whole domain. They cannot block a specific page. So, in this MICT order, because of that, there should be some way for -- to allow the officer, according to that committee, to be able to look into the message. So they test the equipment. And also, this working group duty -- another duty of this working group is, like, after the test, they should also cooperate in Thailand to see if they're working well with the configuration.

So you can see, the development into all these more and more. So this one is more in general. And then, like, a principle -- what kind of content shouldn't be allowed on line, and other media. And from this principle about the content, they're going on, let's setting up some working group. And after the working group, they're saying, okay, we have identified some of the problem, but it doesn't allow us to block some of this content. So let's introduce some technical measure here. I will stop here and say that, like, all this announcement, like, according to our draft constitution, in the last section of our draft constitution, in the code, 27, it say that all the NCPO announcement and order should be in effect, even after the military government has been gone.

So, basically, even we have election and have a new government. All this order will be still in place. And this is the last clause. They say, okay, but just like all the laws, it can be amended. But it can only be amended. If the Senate agree, and in the first five years all the senators will be appointed by NCPO -- so you can see it's going to be very difficult to amend this law in the first five years, even after, like, we -- the constitution, like, has been

passed -- has been approved, because all the people in the city will be appointed by the NCPO anyway in the first five years. Thanks.

(Applause)

>> KYUNG-SIN PARK: There, there. Above. Right there. Yes. Good. There are many threats to free expression in Korea. I'm just going to talk about criminal ones, or ones based on criminal law. Now, many of this criminal law threats to free speech are packaged or justified as a protection for right to personality. And people should not be mislead, because right to personality is praised as something good, something important for human rights. But, in reality, it can be abused to the extent that I'm going to describe. So, article 311, we have insult law. Article 307, paragraph one, truth defamation. Falsity defamation, and the Personal Data Protection Act, and portrait right cases, also to free expression.

On the surface, seems like there is a strong protection of one's right to personality, but that affects other people's freedom of talking about that person. Insult law. So, any public epithet against another is indictable to one year in prison. And every year we have, like, 9,000 indictments for insult which lead to about 50 incarcerations every year. About 10% is for insulting police officers. It mostly results in fines. And the requirement is that the supposed victim of the insult has to file a complaint for the case to move forward.

Now, you can compare that to German or Japanese situation. Germany also has a strong, vigorous prosecution for insult. But it's done through a private prosecution which does not involve police or prosecutors. So, the effect there is much less. Japan also has an insult law, but it's a petty crime. The highest sentence will be, like, ten days in jail. Compared that to one year in Korea. Now, insult law. You may think that, okay, well, the state trying to protect people from feeling insulted may be a good thing. But think about it. When do you get insulted?

When did you get insulted most, so insulted that you lost appetite, and stopped sleeping? For me, that's when I was dumped by my first girlfriend when I was 15. Or when I got C+ coming out of an exam that I thought was getting an A. All feelings of insult come from the discrepancy between how you want to be treated and how the external world treats you. So, this project of trying to protect people from feeling insulted really cuts against how the society operates, because all true evaluations -- if you want to be evaluated, you have to risk receiving lesser evaluation than you expected.

Now, hate speech revelation is something different. It's designed -- it's not designed to protect people from feeling insulted, but it's designed to protect people from discrimination, violence, that may be caused by hateful words. Truth defamation -- any non-false statement lowering another's reputation is indictable for three years. And there's an exemption for statements made solely for public

interest. But this -- so, many people justify this provision by pointing to this exemption for public -- exemption for statements that are made solely for public interest.

But the chilling effect is great because it's a true statement. You have to say it. You want to say it. But without being sure that it will be considered "made solely for public interest," you cannot say it. You withdraw yourself from public discourse. And in Korea, the public interest has been interpreted as narrow. For instance, a worker criticizing the employer for not paying his wages was considered not making a statement solely for public interest because -- right, because he was considered -- he was deemed to be saying -- making the statement to get his wages paid.

So it was not solely for public interest, right. And then other cases also are equally nonsensical. Some people will say, well even so, if you are using a public sphere -- if you are entering a public sphere with your ideas, don't you have to have some public interest to enter the sphere? But think about it. Why should we be restricted in speaking truth even if they are uncomfortable to others? As long as, you know, you are not, like, forcing other people -- you are not, like, doing some sort of, like, forced coming out of, you know, sexual minorities or revealing some confidential information of others.

And if you impose that public interest obligation on people trying to say something that are truthful, that are not confidential, then you are losing a lot of important debate. And you are basically making something impossible in that society. And public interest can be defined only in a collective manner, which means a collective -- it's kind of average concept. But freedom of speech is there for individuals, right? Individuals far on one end of the spectrum should be able to say things as long as they are not harming others. As long as it is lawful, people should be able to say things.

And the truth definition is a narrowing that pluralistic spectrum that the society should enjoy. Falsity defamation. So, you know, this one, many country has falsity defamation, but the problem with Korea is that every year there's like 2,000 indictments which lead to, like, 50 incarcerations. And I did the statistics for, like, a 20-month period back in 2005. In that period, the 50 incarcerations accounted for 28% of all incarcerations around the world, which makes Korea the capital of criminal incarceration for defamation.

And then, many of those falsity defamations are seditious, liable case, which means defamation -- liable case is designed to put down sedition, which means defamation prosecution is designed to protect the state and state officials from defamations. Now -- so, U.N. knows about this. So, U.N. Human Rights Committee has issued a general commitment 34, because Korea and many other countries have truth defamation and insult law, and also vigorous prosecution for falsity defamation which threaten free speech.

So they issued this general commitment. It's general commitment 34. It says many things, but three relevant things is that there should not be criminal punishment for statements not subject to verification. What are statements subject to verification -- not subject to verification? Statements of feelings, statements of opinions. So that statement bans insult law. And truth must be sufficient defense. The defense should not require things like public interest. And also, try to stay away -- I'm sorry. Try to stay away from criminal prosecution for defamation. And also, Korea in 2015, also recommended to abolish truth defamation, free speech, La Rue also noted that many defamation prosecutions are for protecting state officials, and also recommended to abolish truth defamation.

So, I'll stop here. Again, this is only one of the threats -- criminalized threats. But, criminal is really important because it has the most oppressive, chilling effect. And other threats my colleague Jiwon will cover. Thank you.

(Applause)

>> JAMAEL JACOB: Hi, good morning, I'm a lawyer, I represent a foundation for media alternatives, which is a civil society organization based in the Philippines working towards the promotion of communication rights. Currently, in particular, internet rights. So, the Philippines actually, supposedly, the oldest democracy in Asia. And one would think that as such, freedom of expression would be well-protected in our particular country. But then, as probably many of you are aware, we did have that dark period in the 1970s wherein martial law was declared and freedom of expression was suppressed or curtailed.

And then a few years back, we had what's called the massacre, that allowed 58 individuals, most of them journalists, were killed in an election-related killing -- killings, for that matter. And just this year, supposedly the Philippines is the second-most dangerous country for journalists in the past 25 years. So, so much for democracy and freedom of expression, right? And then right now, we have our new President, which at some point actually made a controversial statement wherein one very vocal critic of his, a journalist, as it happens, was killed extra judicially.

And there was -- he made this particular remark wherein he alluded to the fact that some journalists actually deserve to die -- they're corrupt, for that matter. And then later on, his people -- and I think he himself -- clarified that statement was taken out of context. But then, you look at the entirety of his statements these past few months, and it's difficult really how much of that clarification or justification one would be willing to believe, given the many other outrageous and controversial statements he has made while as a mayor, and as a presidential candidate, and now as a sitting President of the Philippines.

So, this is the context that we have right now in the Philippines. And one could -- when one can already somewhat gauge what is in store, I suppose, for freedom of expression in the Philippines. As of now, we can probably identify a number of specific laws that has a large impact -- a negative impact, for that matter -- in so far as freedom of expression is concerned. We have the -- our Cybercrime Prevention Act passed into law a couple of years ago, which was challenged in the Supreme Court. A couple of its provisions have been declared unconstitutional, but one of the more contentious ones, the one on cyber libel was upheld by our Supreme Court.

We have our anti-child pornography act, which while its objective is laudable, it has also some controversial provisions, including the imposition of mandatory installation of filtering software or programs on telecos or ISPs. We have a specific provision, ironically enough, in our Data Privacy Act wherein it is actually made a punishable offense to maliciously disclose, supposedly, personal information, which one comes to think of it, that's really -- could actually translate to another libel-like type of offense.

And then, we have our old Anti-wiretapping Law, which is probably our oldest and still most-cited anti-surveillance legislation. And then the Human Security Act, which partially amends the Anti-wiretapping Law in the sense that terrorism or those suspected of committing or engaging in terrorism may now be subjected to surveillance. As far as the state agencies or state organizations or offices engage in what one would consider as either censorship or filtering, or surveillance, among those one could readily point out would be our Department of Justice, under which there is the Office of Cybercrime. And our National Bureau of Investigation, the counterpart, I suppose, of the U.S. Federal Bureau of Investigation.

We have our Philippine National Police, and Armed Forces of the Philippines, and a slew of other little-known but quite active, in fact, intelligence agencies, which very few in the public are aware of what they're doing and what legal authorities they are operating under, like the National Intelligence Coordinating Agency. So, what are subject to all these censorship, filtering measures? Surveillance mechanisms. As I mentioned earlier, cyber libel or those offenses that may be considered libelous in the context of ICT, the internet, and other cybercrimes are supposedly now subject to surveillance.

And given that they actually make these specific offenses punishable, like the statements supposedly online, then for many, since we have -- it's a very vague provision -- our libel laws actually has been contested for quite some time now, amongst censorship. Again, we have child pornography which is being used by our government as justification for imposing that filtering software, or the

installation of that particular software or program, malicious disclosure of information.

And then the offenses you have here, actually, the ones -- the exceptions in our anti-wiretapping or surveillance law. When law enforcement authorities are investigating individuals for any of these offenses, they would actually be exempt from the anti-wiretapping or surveillance law. And then finally as I mentioned earlier, the Human Security Act expanded the coverage of that exemption by including now terrorism.

So, given that, with those government agencies and those laws, what instances of censorship or surveillance do we now see -- currently see in the Philippines? Ironically enough, it's not based on any of those particular laws. What we have right now just this past couple of years are actually forums, or actions that somewhat amount to censorship, but they're not being committed by the government, but actually by a very private corporation or company, for that matter. In this case, you have Facebook. And fortunate for Facebook, I suppose their mechanism for ensuring what would actually constitute as something worthy of censoring, or being taken down, it's not that effective in the sense that many that one would consider as valid expressions of one's free speech or freedom of expression have actually been subjected to such take-down actions by Facebook.

So as you can see, in these examples, statements or posts by journalists have actually been removed by Facebook. One in particular became quite newsworthy in the Philippines. There was one journalist who simply aired his opinion as to his opposition to the current president, our current president planning to allow the burial of our former dictator in this cemetery that's reserved, actually, for heroes or soldiers, for that matter. And for the longest time, the public have been opposing that precisely because of his role in the imposition of martial law, and the many human rights violations committed during that time.

So this journalist made the post, or aired his opinion on Facebook. And then Facebook took it down. He repeated -- or he made a similar post, and then Facebook took it down again. And then suspended him, actually, for 24 hours. And they later on sent a very short apology saying that one member of its staff actually made the mistake of committing all those take-down actions. And so, this particular case highlights one of the more common occurrences right now in the Philippines, in so far as censorship is concerned.

As regards surveillance, we have a history of our military agents engaging in surveillance against our very own presidents. Gloria Macapagal Arroyo and the late former President Corazon Aquino, as you will see. And then a slew of other cases wherein you have whistle-blowers having their conversation -- phone conversations wiretapped by who? It's not very clear. They just fall into the hands

of the media, or in some cases, politicians. So, with that all happening right now, what are the emerging threats?

I mentioned this once already in a previous panel. So we have the proposed National ID System, which is not surprisingly being supported by our current president. We have another proposed measure which is the mandatory SIM card registration, which, other than threatening one's right to anonymity, actually translates -- although one could say not directly -- but to a threat as well to freedom of expression, because as many of us know, anonymity actually enables freedom of expression in many instances.

And then finally, even more exceptions or exemptions to our anti-wiretapping law. So I think I'll end there, and I'll be more than happy to answer any of your questions later on regarding our situation in the Philippines. Thank you.

(Applause)

>> All right, testing. Testing, one, two, three. Okay, let's stop. Okay. So, let's get this over with. We have 99 problem, but cybercrime law, unlike other country, does not contribute to censorship and digital rights problem, so, yes. But we do have other law. So, fun fact, two of three laws that involve in -- that violate digital rights is -- does not involve blocking the internet. But, you do have to go to jail. So, the first one is sedition act. You can read the text. Essentially, it's down to this. Insult, you go to jail. If you insult the government you go to jail. It's a trap.

So, people that are actually being charged by the sedition act is politician, activist, lawyer, and cartoonist. I believe that it is political ones, that draw comics. So, the second one that's involved in digital rights is actually the multimedia and communication act. Very cool law, actually, because this actually allows the creation of a commission which is essentially the FCC of Malaysia. So, it achieved more than censorship, actually. It manages the spectrum, gives license to ISP, manage the radio, television, etc.

So, the cool thing about this -- actually, that's another thing, not very cool, they have a contract license. They have a way they can actually censor the internet. They have a way to do so. There's a fourth cause of concern for this law. So, if you insult person in real life, you're fined 100. If it's online, it's 50K, a lot more than that. So, it's better for you to insult a person in front of their face than on the internet. So trolling is bad. Okay. Forget the other thing down here. I've actually had an amendment for the same law. We only have rumors, we don't have proof.

So the concern is there is suggestion that the registration for bloggers, website registration. And the second one is actually log-in on ISP. Yeah. I think that's the main one that I forget to add in here. So, another interesting thing about communication multimedia is we have a very wide exemption of what intermediary is. So in this

case, it's really just ISP. So, website provider don't count. Data center don't count. Cache don't count, etc. So, whatever it is. So essentially the only person that is liable is essentially an ISP and teleco and radio, television, etc.

So, okay. So here, this is actually a big case. This person is actually got charged on the Communication Multimedia Act for abuse of network usage, but this guy, what he does, he comment on a forum. He had three charge of -- okay, I don't remember the count, the full charge. It's essentially a mix of sedition, charge under Sedition Act, and the abuse of the Communication Multimedia Act. Next. And, oh, this one. For the publication, printing press and publication act, this law a merger of the printing act and publication act of 1984.

So what this does is it actually monitor the printing press, newspaper, book printer, etc. Oops, one back. Fun fact, publication includes documents, anything you can form shape in any manner, that has an idea. So this is right. They're literally talking about any form of media from television, radio, internet, etc. And fun fact number 2, we really believe that the law might cover smoke signals, flags, and homing pigeons. But I'm just a system administrator, don't take my word for it.

So, okay. So the next one is the surveillance law. Okay. So we do have some surveillance law. The first one is the Prevention of Crime Act. This is a law from the British, sorry. So this is actually a law that is used for preventing secret society, criminals and whatnot. So, it allows two things. If a person being charged, they have to -- a device, and the government block them from using the internet, apparently. So, they got sent back to the Stone Age.

So this law, the Security Offenses Act, is used for political movement, etc. So this one, they got a law for terrorists, but terrorism can be charged on here. So what this does is allow the authority to do wiretapping, and if you are a terrorist, known terrorist, you'll be attached with -- to trace you. So, this is the SOSMA. This is known to be used against bloggers and whatnot. So this is actually a pretty bad law.

And finally, we've got the Prevention of Terrorism Act, an extension of SOSMA, the law just now. Except, a known terrorist -- with a release, attached with a GPS bracelet on their leg. But on the other hand, the good thing about being a terrorist, after release, you won't be sent back to the Stone Age. So that's cool. So, we have two methods for censorship. This is a bit technical. The first, DNS blocking. So, there's actually a list of domain that's being blocked on the ISP -- DNS server, run by the ISP.

An interesting thing is, we've been trying to ask for the list, so the commission asked us to check the ISP, and the ISP asked us to check back, so we never got it. Fortunately, we can bypass it using open DNS servers, like Google DNS and whatnot, unless you're on a

phone, in which case you're screwed, sorry. Also, here's the rule, you try to get DNSSEC, here's the thing. DNSSEC has two things you can use. One, it return a set of key that register to a domain name, and also, I think they encrypt the communication. I need to double check on that.

So, this make detection of interference on DNS level easy to find out. But unfortunately, the adoption has been low. We hope to get more people to adopt this tool. Okay. The next -- packet manipulation is on ISP level, this is an attack. So it only happens once. And actually, they're manipulating -- I think a sequence number. So what they do is they take the last number of one packet, so the packet takes too long to reach the destination, therefore, the packet get dropped.

So it's one of those attack that -- actually, it's a very cool attack, by the way. I shouldn't say this, but this is actually very cool. But it's also very scary at the same time. So -- but fortunately, because this can easily be solved by using HTTPS, just encrypt the packet using SSL and whatnot. So, HTTPS is encrypting, the free DNS. We just stopped a very scary attack in Malaysia.

And finally, this is actually what's happening with our project. Ooh, I've got time. One, it is a Digimon project, we collect information like internet blocking, maybe monitoring. Also, we are similar to CERT, because CERT do not handle these kind of issues. We have the technical capability to handle that. So that's another one. And second -- okay. So this is one of our network censor, we call this the censor sensor because it sounds funny.

So, this is a small computer that automatically runs testing scripts to test for censorship. So -- and we actually get the data to be analyzed. There's a reason why we use these -- because no one in the their right mind going to spend 24 hours to click on a website every single minute, it's just insane. So we automate it using a small Linux computer to keep testing the network. And finally, the global campaign. Keep it on campaign is a project about access. Again, it's international. So, here's the deal about international -- it does not mean you can shut down the internet. You can't.

It does not mean blocking internet from a country. That may be crazy, but that really happened. But in this case, the definition also includes taking down of a service, website, parts, etc. So this one, a meta tool, the OONI script, an observer -- interrupt interference. What they do is provide a set of software scripts to measure internet censorship, DNS test, packet test, etc. And this is actually the same script that we use on our network sensor.

And we encourage everybody to use these tools to set up VPN on the network, so if a site get blocked, just bypass it on this. And two things, one, which is scarier, internet block or going to jail? That's what's happening in our country. Finally, currently, we hack

around this situation. How far can you hack your way around this? And with this, thank you for listening. So, sorry for my rambling. Yeah. I did not make this up. You can look it up on the internet. Happy sys admin day. Thank you.

(Applause)

>> JIWON SOHN: Hi, I'm the Project Manager of Internet Reporting. I'm going to talk about the problem of the current administrative censorship system. The system will not acquire a criminal penalty, but will pose a significant risk to freedom of expression, because it can easily be used to control public opinion by directly deleting posts, thereby critically infringing upon freedom of online expressions. South Korea has the administrative body called the KCSC, and it can make decision to take down online information. The decision is called the correction request, however, the decision has -- resulting in the rates -- with almost 100%.

In cases -- members are all appointed by the President, and -- party -- by the opposition party. It has made about 150,000 decision in the last year. The standard is to make takedown decision -- illegal things, because the provision allows the KCSC to regulate the commission -- ethics. Thanks to this standard -- can take down not only illegal content, but also, allegedly harmful lawful content, more specifically -- contents as follows, using -- language and -- content -- insertment of social (inaudible), etc.

The most serious problem is that it has a high risk of -- government in attempt to suppress the oppression against the government. I will share some examples. The Twitter account which sounds like an epithet against President Lee was brought -- excess of swearing. And a post that blames the government's incompetence over the last year -- very -- was deleted because that post contained some swearing to the president and high-ranking officials. The standard causing concern is social unrest -- after forced applying -- last year has been deleting numerous content that pose question on the facts by the government.

The first claimed that NIS was involved in -- was responsible for -- was deleted. And the post claiming that South Korea government -- incidents of North Korean -- deleted -- to turn the media attention away from controversies at the time surrounding the government was deleted for the reason of incitement of social unrest. An administrative agency -- people's expressions based on abstract and other standard is -- an abuse of power -- mindset while criticizing states and controlling public opinion is. As such, there exists a rising concern that it is unconstitutional.

There are more problem cases which just deleted the North Korean statement, or from the North Korean servers. For the reason of it being a site that poses -- and glorifies the North Korean, and the

illusion -- conservative -- National Security Act. KCSC block access to certain website. In violation of this article. This is a kind of media blog that is run by British journalists -- North Korean -- for academic and reporting purposes. So it's quite -- unique expertise on the North Korea ICT rules -- by various media including -- BBC and even in the (inaudible).

The website just because some information in the blog, or post linked to the reports and they confirmed the North Korean media. The Korean Civil Society team is working on challenges against censorship cases -- in order to reduce -- system. The panel includes several -- against -- takedown decision have been conducted -- success. However -- highlights -- consensus. KCSC decide to -- website that provides file sharing and streaming services, citing it's a violation of the law. And in this -- some illegal copies of Korean content.

In general, this -- the decision is unlawful that find -- whether the whole website constitute illegal information should be conducted under a strict and narrow standard such as -- operating the website -- legal activities itself. So it's -- the entire website just because an illegal content was distributed therein. It's a very natural conclusion (inaudible). Illegal website blocking process. This case is ongoing on a pilot as KCSC appealed.
And -- blocking -- also underway -- information -- internet citing this report as the source. And we hope that the current -- risk -- article seven of the National Security Act, we hope.

And we have recently discovered that -- also -- deleting post in violation of -- Act -- in many aspects. The Korean reaction -- disseminate those facts by candidates including a person who intended to become candidates and his or her family. And dissemination of even true facts are also prohibited as long as it slander. As such, this information that may be found to be -- in this act is very wide, and even -- criticism and suspicion of politician may also subject. The current answer to the request was discovered that over 17,000 post was deleted by the order only in relation to April.

We also work revision of this act. To find out more about the status of the issues of Korean censorship, please visit our Korea Internet Transparency website. Because of the nature of expression -- and feel that it can easily take down such online expression based on arbitrary standard. And policies are also implemented under this law, I think. And many -- mentions -- many have urge to control the online information, and try to -- censorship system.

So stakeholders should continue the discussion on the censorship issue in order to prevent -- abused -- to infringe our online freedom of expression and rights. Thank you.

>> IRENE POETRANTO: Thank you to our panelists for their presentations. I'd now like to open to the floor in anyone has any questions, or even to panelists to ask each other questions. Go ahead.

>> AUDIENCE: Good morning. I'm Oliver from the Philippines, representing the American Bar Association Initiative. I question this. I'm just curious whether in your jurisdictions, there's this concept called the right to reply wherein if somebody makes a commentary, a political commentary in whatever medium, whether it be in the newspaper or online, the person who is commented to has a right to equal space to reply to the commentary or allegation. So to cite one example, if you write a blog post about a political figure, that political figure has the right to insist on replying on the same space.

Meaning that you have as a blogger the compulsion to post that figure's response to your post. This was a concept in the U.S. which was discarded only in the 1980s for broadcast media. I'm just wondering whether this concept is also present in your respective jurisdictions, and what you think about the concept.

>> KYUNG-SIN PARK: The fairness doctrine in broadcasting regulation in Korea, we are proposing to abolish it, because many broadcasting stations start out as state entities. Even if they are somehow changed a little bit and labeled as public broadcasting as opposed to government broadcasting, the government continues to exercise influence on programming of the so-called public broadcasting. And on top of that -- so, in that situation, review should be used to neutralize what is becoming government propaganda. But that has not happened, because who will conduct fairness doctrine? Who will appoint the officials conducting fairness review? The point is, they serve the interest of the power that has appointed them.

So, in Korea, for the past three years, there were, like, between 30 to 40 fairness reviews of broadcasting content. All of them -- all the disciplines made for the review were made against content that were critical of the government. And the broadcasting stations already under the influence of the government. Broadcasting, programming content without scruples. The fairness review committee is punishing the content that's critical of the government. So you can see the end result. So, I'd be very careful in instituting fairness review on broadcasting company.

>> AUDIENCE: Hello, I'm from Nepal. I'm a lawyer. I started my career a journalist. I was also one of a team member of online journalists in Nepal. There's a big debate of criminalizing our expression online. Do you think there should not be any criminality of any publication online? Because any news matters, or any content published online could be very offensive to someone, or may damage the privacy of an individual. In that case, should not apply criminal law? Thank you.

>> Did I understand your question correctly? Your question is, in my opinion, at least, do I believe that online -- should online publication deemed very offensive, or something like that to a particular person, I suppose, be held criminal, may it be criminally liable, or the person that posted it may be criminally liable?

>> AUDIENCE: Yes, yes. Sometime it's very critical, very offensive. Any content could be very offensive online. And in that case, many countries are using criminal defamation laws to curb this, so do you advocate criminal defamation online, or there's some need of some level of need of criminal defamation?

>> JAMAEL JACOB: Well, I can only speak for myself, and I suppose our organization, since I guess it would depend on who you ask.

>> AUDIENCE: Yeah.

>> JAMAEL JACOB: For instance, in the Philippines, if I'm not mistaken, actually, there's this global trend towards the opposite, I suppose, you could say, towards the criminalization of libel, whether it is online or offline. So, to that extent, I would think that the trend right now is in favor of the criminalizing that particular -- this particular act. Given that I am fully aware, of course, that cultural differences usually factor in, which makes things complicated, I'm not saying that it should be used as justification right there and then as a constant justification in the situation.

But in my opinion, I still move towards the criminalization. In the Philippines, for instance, there has been a U.N., rather, written I suppose, comment, regarding a particular case wherein the Philippines was actually instructed or advised to work towards the criminalizing or abolishing its libel laws, ironically enough. This is why I'm saying, it depends who you ask in the Philippines. Ironically enough after that U.N. opinion, so to speak, it was actually the time that the Philippines enacted the cyber libel law. So instead of abiding, complying, or acknowledging the United Nations, the Philippine government went the opposite direction.

And even because cyber libel compared to regular, offline libel in the Philippines is actually given a heavier penalty as opposed to offline libel. So, in our case, we are moving towards the opposite direction. But as of now, our government appears to be moving towards the opposite direction.

>> Here's what I think about offensive publication online -- no, offline, online, to me, it's the same. If somebody is offensive, you can come to write a counterargument. Don't block it. Don't criminalize it. Free speech doesn't go only one way. It goes both ways. So somebody can say something. If you think it's offensive, you have the right to talk back to the other person.

>> Actually, come back to the question that the guy from ABA was asking about right to reply. In Thailand, to my knowledge, I just

searched this. I mean, our broadcasting regulator doesn't actually have the power -- I mean, so, say this first. That kind of concept, it's allow in the journalist circles, right. But it's not actually in the law. In the law it only say about something, right. So the other thing that actually, our broadcasting can do, according to the law is that, like, they can interview -- only if the media -- content that could be something like inside the national -- only, like, the industry categories -- license.

Anyway, the -- can send -- ask the media ethic board -- which is another body -- under the control of the regularity to ask the media to actually, sort of, regulate themselves, if they cover any -- on its -- so, thanks. There's nothing to specify specifically about the right to reply.

>> I want to share a feeling I have about these sessions. I have been to plenty of sessions similar to this setting. And as an audience -- and noncitizens of either Thailand, Philippines, South Korea, or the other countries, it's very difficult for me to judge what kind of stories you are telling me. And so the informational value, to put your stories in some kind of a context, is really difficult. So, I wonder -- I think it would be much more interesting for me if I had somebody from the Thai government agency sitting here talking to you.

And then we have, like, a real discussion and some fighting, you know? And then, of course, maybe each of you tell lies, but at least I have a kind of -- a better comparison of where you're coming from, what is your reasoning, how're you arguing. Now I hear academics and the people from the civil society organizations, but I don't hear what the government is saying, how are they arguing, how are they defending their measures on how they control the internet, or control freedom of expression? So, I just question how could we make these kind of sessions more balanced, although it's maybe not realistic.

But how could we make it more refreshing to hear also the bad guys from the government?

>> (Off microphone)

>> I know, I know.

>> Yeah. I will also make the same observation. In the case of the Philippines, civil society has been trying to get the Philippine government to engage more at the international level, and international fora such as this one. But unfortunately, so far, they have failed to heed our call. And I guess in the past few years, they have usually alluded to the fact that we have no dedicated ministry or department on ICTs. But now just two months ago, we do have one. We do have the ICT right now, and the national commission was just established this March. So we are hoping that in future events such as this one, we will be having more spaces, dialogues, with our

governments -- not just this one, of course, and more importantly, in our respective jurisdiction we'll be able to engage with them more.

But we fully agree with your observation that it would be better if -- since, I think, a multistakeholder approach is usually what's being advocated in situations like this, that it truly be a multistakeholder -- and in particular, that it includes the states or government representatives.

>> Thank you. I think that was a really good discussion, because you pretty much mapped out all the different challenges, right. Just a couple observations. Southeast Asia has a different set of challenges, and in some cases, a much more severe, sort of, challenge. I would think it would've been kind of good to also have someone from south Asian, whether it's India, Pakistan, Sri Lanka, weighing in on the challenges. If you don't mind, I want to take a minute to flag what's happening there. A lot of the challenges are very similar, but a lot of challenges are much worse.

I think when we're looking at freedom of expression, we cannot be blindsided by what's happening to the bloggers in Bangladesh. The offline consequences for blogging are serious, not only for them, for their families, is and more particularly, for the female partners and family members. They are being killed, literally by now, 24 bloggers have been killed in Bangladesh, including activists. So that's one, for writing online.

The second major challenge is, they're merging ICT laws. Like, a person from the Philippines pointed out, and Malaysia, we have specific laws and ICTs coming up, but then offline laws are also being used. And what's happening is that when they're using the offline laws they're making it even more severe for online expression. And the issue I'm trying to point out here is there's really a pressing need to do a regional analysis on these laws. Because the longer we wait, more jurisprudence is being created on this. And when I say that, it's really dangerous jurisprudence, because courts are coming out saying that the internet is dangerous, they're saying the internet is destabilizing political economies.

So I think there's really a need to step back, and lawyers and civil society look at how courts are interpreting these ICT laws. The third point I wanted to make is in relation to religion, and that's been covered in different panels. In south Asia, that's the most pressing problem we're facing, religion and religious sensitivities are being repeatedly used to shut down expression online. This is both expression about religion, as well as other forms of expression that are being shut down on the context of offending religion, as if religion has a concept of defamation attached to it, which the international mechanisms have been pushing back on.

So, these are the three broad points I kind of wanted to flag.

>> Hi, may name is Said, I come from Afghanistan. I just want to give our perspective. As a government employee, we have some

tactics in terms of public consultation when it comes to cyber law and legislation similar to that. So I completely agree with the approach that the government usually -- they do consult private businesses and civil society, but they have their own tactics of keeping it minimum and quiet. And they do that by -- in my particular case -- they limit the time. And they also use very limited number of publications which are government-only.

And people don't usually read that. So they still publish that. They fulfill the minimum requirement. But who reads that? Do people get back to them? So, that happens. And once, twice, thrice, nobody responds because the channels that they use are the channels that usually don't even read, or -- they're usually like printed publications, which people are not using anymore. Another concern that we have in our country is that when I was talking to the director of information security, the directorate drafted the cyber law, they reduced the age of a minor from 18 to 16.

And that, I think, in itself is such a big challenge of targeting minors who are, according to them, they are usually the larger number of hackers. That in itself is a big indication of criminalization of people, of citizens, through these cyber laws, and not actually protecting them or giving education to them, or giving an opportunity to not repeat the mistakes that they would do again. And I repeat myself that these are usually -- what hackers do usually, they are mistakes. And they would probably revert back if they could. Thank you.

>> All right. Malaysia do have issue with religion. We have fundamentalists, believe it or not. It's not a technology problem. Bad news. Technology amplify the problem. To fix it, you need to fix society, to educate people in more civil way to talk. So, over there, again, that's not a tech problem. Look at it this way. We need better communication. The problem is, even in our country, we do not know any form of consultation on issues -- any issues. But how you solve that is, again, groups of people actually try to find out -- that's what they do.

Unfortunately, we don't have a big -- but a lot of country have the same issues. Again, this is not a technical problem, it's a problem of civil society and society itself. In this case, in your case, the technical solution won't amplify the issue. Again, the different scenario -- in your case, technology going to make things worse. In your case, it might make things easier. Thank you.

>> IRENE POETRANTO: Well, thank you for the questions and the answers. Thank you for coming to our panel today. And please join me in applauding our panelists. Thank you.

(Applause)

(Session concluded at 10:31 a.m.)

***

This text is being provided in a realtime format. Communication Access Realtime Translation (CART) or captioning are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***