

FINISHED FILE

APrIGF 2017
"ENSURING AN INCLUSIVE AND SUSTAINABLE DEVELOPMENT IN ASIA
PACIFIC: A REGIONAL AGENDA FOR INTERNET GOVERNANCE"
BANGKOK, THAILAND
JULY 29, 2017

ROOM 207
ENGAGING WITH THE #KEEPITON MOVEMENT: FIGHTING INTERNET
SHUTDOWNS
11:00 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

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.

>> RAMAN JIT SINGH CHIMA: We'll be starting shortly. Just before that, we're going to do a sound check. Lorenzo, can you unmute and just say something? We're just doing a sound check.

>> Hi, everybody.

>> RAMAN JIT SINGH CHIMA: Lorenzo, you are unmuted. Can you say something? We just want to check the audio so your presentation isn't interrupted later.

>> Hi, everybody. Can you hear me?

>> RAMAN JIT SINGH CHIMA: Lorenzo, we can't hear you, just to confirm. You may need to change your equipment.

>> LORENZO PRIMITERRA: Oh. I can try it again. I don't know.

Can you hear me now?

>> RAMAN JIT SINGH CHIMA: Lorenzo, I know you can hear us. To confirm, switch your device, and we will do a test later in. We will go ahead and start in the interest of time.

Thank you, everyone. With that, let me introduce this

session and the participants. This is an open forum on the KeepItOn movement and on Internet shutdowns more broadly. Some of you may be familiar with KeepItOn. Many of you might be members. Also, the KeepItOn coalition. Others might be interested in a background on that.

Firstly, to introduce myself, and then I will introduce the rest of the panel and people who are also joining remotely. My name is Raman Jit Singh Chima, policy director at Access Now, one of the organizations that help put together the KeepItOn coalition. We are an organization that looking at protecting the rights of users at risk, and in doing so, we particularly focus on your digital rights online and ensuring an open Internet for all.

As part of that, one thing we noticed along with many other organizations now and nearly two years ago was the increase in the number of network disruptions, which is the technical term we use, but more often what you might encounter is entire Internet shutdowns. Entire provinces, cities, sometimes even countries switching off Internet access. Sometimes causing disruption at the mobile Internet layer. And even sometimes connectivity. Act rights Con, two years ago at Silicon Valley, we had a definition of shutdowns that came out due to a community involvement. I see many people in this room who helped contribute to that definition of shutdowns.

Shutdowns is now also something that's been discussed at the international human rights law. Some of you may be familiar with U.N. for free expression, Mr. David Kay. David Kay's most recent report talking about the role of free speech in the ICT sector, has also spoken about the impact that Internet shutdowns have and the role that the private sector, both in terms of telecommunications companies, who governments often ask to block services, where services are disrupted. The impact and the role they have to play in this.

But that's a little bit about what shutdowns are. The KeepItOn coalition is a global movement to try and push back against this. It is an effort to share an information about shutdowns, be able to notify the technical and sometimes news layer when they are taking place, bring visibility to them, but also advocacy objective to prevent the growth of shutdowns. And the many interesting different viewpoints on that. We welcome that. It is an open forum. If you feel forcefully on something, with respect to the speakers, please intervene, and we will have more participants.

With that, let me introduce the rest of the group as well. Ritu Srivastava works on shutdowns in India, as well as engaging in the human rights process. We have Lorenzo, who will be joining us remotely. Lorenzo is a developer, a mobile developer with what a group many know as OONI, the Open Observatory For Network Interference, which tries to do network probe research on not just Internet shutdowns, but broader types of network

disruption or interference with network services.

Kay is a researcher, and they worked on technical information on shutdowns as well as advocacy interventions. And Kay and Lorenzo will be presenting research on the subject.

Here again, back in person, we have (?) many know has come out of the open source network, but worked on digital rights issues, including the tracker for India and global conversations on this, which you can visit at Internetshutdowns.in. Joining us remotely will be Apar Gupta from the Internet Freedom Foundation, engaging in advocacy against shutdowns in that country, including political and legal conversations on that. And Apar also has experience on litigation efforts against shutdowns.

Lastly, but definitely not the least, is policy director with Facebook. Also a global initiative member, and GNI as well as Facebook and other companies have taken positions on Internet shutdowns, expressed concern on that. Many have perhaps also seen GNI statements on this as well as the new primer about when an Internet shutdown takes place, what to do. And will be talking a little bit about the private questions, but also take questions to the best of her ability on that.

With that, we're going to try to keep five-minute introductions from the speakers about their top concerns about shutdowns, stuff they've seen. And, you know, I would mention that most people here have worked on this subject, so you might notice this will be less definitional. It's going to be more about what people are facing, as well as interesting challenges happening in each country. For example, we recognize in Asia Pacific there's massive diversity and massive changes, variance in what governments do, even how shutdowns take place. Shutdowns might be easy to do, versus elsewhere, it might be state by state. We will then have one round -- one can intervene from the audience and we will give time just for that. And then we will keep a little bit of time towards the end to focus again on the solutions piece in terms of what can people do if they want to take a strong position on shutdowns, what efforts are there.

And for those who are interested in the KeepItOn movement as such, please ask questions, but you can catch me or any other members after the session as well, and you can visit the KeepItOn website online, and you will see the hash tag also to give you lots of resources.

With that, we'll start with the first one, Ritu.

>> RITU SRIVASTAVA: Thanks, Raman. So, in India, we have seen about a 93 shutdown, if I'm not wrong, that my colleague will be able to correct me if that's the correct status right now. Two years back, we started doing the research on what is the impact on economically, but also socially, and how it is impacting the lives of the people. Especially when we think about it, in the paradigm shift, or the digital India plan, 15

services, nine services are only talking about digital payment services, so we started thinking about when the work is being disrupted or shutdown has been happening, what are the disruptions that India is facing as well.

I am going to read some of the comments and some of the quotations, what we have analyzed in our research when we are trying to understand the impact of the shutdown. And how it is emotionally and sentimentally affecting the people.

So we did media monitoring and reporting, and what we have seen actually, that there are a grown up of students who have said that if there's a shutdown, they are going ahead. So the semesters are canceled because they are unable to access the information, they are unable to access the point that they want to access when they need to apply for the exams. That's a very interesting case, when we saw that a shutdown has been for 41 days, the student has said that we have gone for a vacation, but due to the shutdown, our plans -- that we cannot plan it out, whether we can continue our travel or we cannot. So we are stuck in some place, actually.

Uttar Pradesh has said we come to the bridge to mobilize the services because a blanket of a shutdown is there, so we come to a bridge just to understand whether we can get the signal or not. So if we think that there's a level of shutdown, it's not a blanket shutdown, but it's also the throttling of the bandwidth services at the same time.

When I go to another state, due to the curfew of all offices, educational institutions are closed and people are facing a shortage of consumer items, people need the medicine, but they are unable to get the medicine as well. So these are some of the impact of the shutdown. We can see that it's impacting the shopkeepers. It's impacting the educational institute. It's impacting small vendors. So it's affecting all the ways of it.

The point is all about what we are doing and when the shutdown is also happening. Some of the cases when we have seen that in the cases, that national security is being given a reason that shutdown is required for that, and the spread of -- just to stop the spread of fake news, that is also, our network has to be disrupted. But what is the definition of that national security is not being defined by the state. It's not being transferred by the state that. Is one of the reasons when we have (?) most of the people are saying that they do want to know what is -- what is the reason behind it that network is being transferred, but they are not clear about it because they do not understand what does the national security mean to them.

What we have seen, they are saying that -- this is the time that the state is trying to give us more time to kill people instead of trying to do productive work as well. So we can understand if it is a longer duration, if it is a longitude duration for the shutdown, that it's also promoting the citizens

to come out and say that these are some of the things which we really want to understand. These shutdowns are not only impacting the human's life, but also impacting socially impacting their lives and their day-to-day lives. Their day-to-day lives.

So these are some of the measurements which we are trying to understand socially, economically, and through our research, and we would like to see how we can give a rapid response to the government and what we can do, when the shutdown is happening at the same time. What we can do, we have also -- in our periodic view, we have clearly said that these shutdowns are not going to make us digital India plan successful until and unless we are providing universal and uniform network to the government.

>> RAMAN JIT SINGH CHIMA: Thank you so much, Ritu. We were going to go to our remote presenter next, but I think we are still sorting out audio. So just to check, is it working? So what we're going to do is come back to the remote participants, because I think there's a problem at this end here, the audio.

So what I will do is jump ahead. Kay will come in later. So would you like to talk a bit?

>> Hello. Is it on? Hello, everybody. I work at (?). We have been maintaining a dynamic tracker at down start IN. So this shutdown tracker, for 2017 itself, we have come to the number of shutdowns is 34. The figures are only the to the month of July, as of the date. So you can imagine the number of shutdowns in 2017, 34. They were only 31. I wouldn't say only, but there were 31 in the whole year of 2016, while there were 14 in 2015. You can see the rapid increase in number of shutdowns that have been happening.

So from 2012, from then, we have been collecting the data. We will see 93 number of shutdowns in India across 16 states. So this highlights the importance and gravity of the situation.

Now, if we can go and do it further, we have also been analyzing these shutdowns on the basis of the kinds of services that have been restricted, mostly Mumbai or (?) on the both of them, also the duration of shutdowns, which they've been for 24 hours, or they have been for 24 hours to 72 hours, or more than 72 hours. Also the nature of shutdowns, whether these shutdowns have been in response to the violence or the reactionary measure, or just for preventive precautionary measure.

So what we have observed, recently in 2017, most of the issues that have been proposed by the government are primitive in nature. That is in participation of something going wrong.

Also, durations of shutdowns have also increased while the kinds of services -- by the way, in India, most of the Internet users are accessing Internet via mobile. So 94% is the mobile Internet base. Also, there are broadband users as well, and governments have been resorting to shutting down Internet, mostly on mobile, and at times restricting both Internets,

mobile Internet as well as broadband, the fixed line networks.

Now, when we look at it, going by the campaign that we are advocating and at the same time shutting down Internet, it has huge impact on people. We have been facing shutdown for 41 days, there are students, the bodies of the teachers association that they have been protesting against, not being able to fill up examinations for giving their board exams.

Similarly, recently, we had shutdown for over 15 days in Rajasthan, when it was reported that (?) people over there, the employees and the businesses incurred 25 flags of -- the loss of 25 flags in those 15 days. Apart from the rupees that were lost by the users because they could not access Internet services, and the Internet services -- the Internet service provider would not give them back their money for not using Internet.

Now, while we have been recording these shutdowns in our Internet trackers, so how we do it, we rely on the newspaper reports, and also has a report of shutdown, through which people in the affected areas may by themselves support a shutdown in their place. So recently, we have been receiving a lot of reports, that yes, we have seen a shutdown in this particular place, and this is causing us this much trouble. We have been denied the medical facilities are essential, and banking facilities, which are really important for the online data rate transactions, considering the economy is increasingly going cashless.

So I think these issues are -- should be, in fact, readily addressed by the governments also, because this issue -- the Internet imposed on the state level, or in the telegraph state action 25. So under section 144, which is a very archaic law --

>> Can we just mention which law?

>> Vaishali: Basically a law for the case of disturbance, to prevent unlawful assembly of India. So the state government, this is imposed by the state government. So state government is also using this law, which is a very archaic law. So government are using this law to apply to the Internet sphere, which I don't think that is justified. So a venue also restricts the freedom on Internet venue -- and also restrict the freedom on your speech, freedom as basic as necessities of life. Example, the essential utilities, banking facility, healthcare, as Ritu mentioned, and also found in a study that when our Internet was shut down there, the hospitals over there could not perform essential surgeries because they could not access the medical records of the patient because the Internet was not there.

So it also affects these essential operations which cannot take place without the use of Internet. So when we see the use application of these archaic laws is one problem, and also, to mitigate this problem, not exactly to mitigate this problem, but, yes, to bring into light the gravity of the problem and to address and to find a solution towards it, we have also been writing -- we have also been writing letters to the CM, also

been campaigning against them, against these laws.

So I think that is something that we can do together, and I would like the panelists also to focus more on it.

>> RAMAN JIT SINGH CHIMA: Thank you, Vaishali. Lorenzo's connection is working, so should be able to jump in. I think it would be a good time. As Vaishali mentioned, a lot of the trackers are sometimes based on reports as well as user notification. That's at the technical level, and I can share from many of the technical members of the KeepItOn movement the efforts of trying to use network probes and other data to get actual data, network data and what's taking place.

As I mentioned previously, Lorenzo works at OONI. Lorenzo, if you can hear me, try and speak.

>> LISA GARCIA: Yeah, I can hear you.

>> RAMAN JIT SINGH CHIMA: We can hear you. Fantastic. Go ahead.

>> LORENZO PRIMITERRA: Okay. I don't know if you can see my slides. So I work with OONI, and I'm the main mobile developer. I joined OONI two years ago. Basically, OONI is a global network for censorship, surveillance, and traffic manipulation on the Internet. I tried to share my screen.

>> RAMAN JIT SINGH CHIMA: If you share your screen now, it will come up at our end as well.

>> LORENZO PRIMITERRA: Am I going to share my slide? Okay. Upload in progress.

Okay. I can see the slides.

>> RAMAN JIT SINGH CHIMA: I think these are the Sinar Project slides. So not yours. Just one second. Lorenzo, I think it's not going to come up, so you may -- Lorenzo, I think what we're going to do is try to get that squared across. So if you ping it across on the meeting room chat, that might be best, and people can access it there. Otherwise, you may just want to keep it to oral comments right now. We can see an upload in progress. Thank you so much. For those waiting, it is working, it is fantastic work. So I will be a salesperson and say it is truly worth waiting for this, as it comes up.

>> LORENZO PRIMITERRA: The graphics are fantastic thanks to Ritu and Maria.

>> RAMAN JIT SINGH CHIMA: While your presentation is up loading, maybe we will jump to Kay's, and maybe come back to you in a minute.

>> LORENZO PRIMITERRA: Okay.

>> RAMAN JIT SINGH CHIMA: So, Kay, I would like to give you an introduction, but would you like to perhaps talk about the specific cases that you all did?

>> KAYYEN WONG: All right. So I'll start off introducing the project and expanding a bit about what we do. We're initiating open technology and data. So this is important information, open and accessible to the mainstream public. So the Internet plays a crucial role in our work and improving

governance and ensuring it remains open and transparent. So it's important to us that freedom of expression continues to remain in the online digital space.

So to that end, we've collaborated with the open authority observatory on Internet interference, OONI, specifically countries where the government has stark control over the Internet.

So I will share some of our findings, starting off with Malaysia. Malaysia has, as of 2016, a million Internet users, over 68 penetration rate. We have ISPs providing mobile or networks at the homes. 39 websites were blocked. These sites include blogs and the entirety of (?) for reporting on the scanner which followed the Asian Prime Ministers, mysterious private dealings, which led to a private trail, being funded into his private accounts.

So the Malaysian government has not -- the Malaysian government has not been discreet about blockings, justifying it as a violation of security under the communications and multi-media act, which authorizes them to ban offensive content.

Moving on to Thailand. Thailand has of 2016 a 29% penetration rate. And what's interesting about Thailand is that the Thai government has long held control over the Internet, due to their relationship with Internet service providers and telecommunication companies. So this means that Thai ISPs are complicit in cooperating with the government in response to the government sanctions censorship requests.

Some of the laws in Thailand are notably the law which penalizes anyone found to have made offensive or defamatory comments against the Thai monarchy, and the crime which penalizes the uploaded content found to be defamatory. These laws have long been used against Thai journalists, activists, and Internet users, and the Thai Internet community.

So we found out 13 websites were hacked by the proxies in Thailand. These sites include WikiLeaks, sites which censorship circle mention tools, and use "The New York Post" in the e-mail. Interestingly, "The New York Post" was only censored in one mobile Internet service, which was D-Tak, and was largely accessible through all of the ISPs.

The same goes for WikiLeaks, which was only censored by one of the ISPs, and this corroborates with reports that of the Thai secret place, Thai secret police's agreements with Thai ISPs to grant the authority to censor Internet content at their own discretion, which gives them an already -- which gives them a lot of power and control over freedom of expression in the Thai space.

Next we have Myanmar. Myanmar has as of 2016 a 19% Internet penetration rate. The people in Myanmar have a very limited choice of ISPs, and both are unfortunately state controlled. Myanmar has the 2013 communications law, which allows the government to set up surveillance. They also have

the very restrictive computer science development act, which requires the permit for the import of equipment, and they have the various laws which are used against the Myanmar people in controlling their speech online.

So detecting the use of commercial for -- to filter content. Though, our most recent in six networks showed no signs of this software being used. We still found evidence of censorship in Myanmar. Most notably with the size of the U.S. embassy in Myanmar and organization American states, which present a song science of TCIP and blocking.

Finally, we have Indonesia. Indonesia has an over 50% Internet penetration rate. Due to their unique geography, over 70,000 islands, they have over 300 ISPs. The providers in Indonesia are telecomm, (?) being partially state owned. So Indonesia has the transactions law, which has been used to prosecute individuals who distribute or transmit indecent content, gambling material, defamatory material. So we found 161 websites were blocked throughout the testing period, with the Indonesian ISPs with the wireless hijacking. Indonesia has -- Indonesian ISPs are authorized to ban online content at their own discretion, so some ISPs were blocked, despite the government having supposedly banned -- lifted the ban on them two years ago.

So most of the censorship appear to have been -- in regards to the enforcement of the cultural norms. For example, blocking LGBT pornographic content, the majority blocked on Indonesian sites. It's all the more improved to ensure that democracy continues to be protected in these spaces. So by collaborating to collect censorship statistics, we are able to map access in regards to affordability.

So Lorenzo, (?) from a technical perspective, so it's important not to just run these, but identify the digital rights violations that are going on, but also because it will be able to understand these blocks from a more technical perspective, in terms of the extent and how they're back. And possibly work around these censorships. For example, the HGDP block. The solution would be to just use HGPDS. So if you'd like to learn more about how to run on OONI in your country, you're free to talk to us or OONI. My supervisor is here. She knows much more about this than I do. So, thank you.

[Applause]

>> RAMAN JIT SINGH CHIMA: And we are going to try with Lorenzo again in a minute. I have one comment on censorship and shutdowns. Often shutdowns very justified that we cannot block certain bits of content. We can't block certain websites. Therefore, we have to shut the entire Internet down. Sometimes it's also provoking the actions, where they say, we can't block specific URLs, specific instances of content, and therefore we're going to try and do more. Kay mentioned the that more technical research is really helpful, because it's understanding

the sort of interest with stakeholders and others.

With that, just want to try again with Lorenzo, if -- I think his presentation will work now. So Lorenzo, go ahead.

>> LORENZO PRIMITERRA: Yeah. Can you hear me?

>> RAMAN JIT SINGH CHIMA: We can.

>> LORENZO PRIMITERRA: Yeah. I can see my slide is loading.

>> RAMAN JIT SINGH CHIMA: Maybe you can give a little bit of background on OONI?

>> LORENZO PRIMITERRA: Yeah. (?) the network with many different techniques. I will describe them later. And basically, apart from just the app or the size, we give data to every person, every activist to write reports or anything they can do with the data.

So we connected millions of network measurements from all across the world, and especially with the launch of the mobile app. So the tests the targeted of blocking website or instant messaging app or even blocking of censorship tools, and detection of middle boxes are just measurement of speed and performance, because this can be a form of censorship throttling.

So available on Linux or macOS, and android and iOS, and RaspberryPi.

So the first time at OONI, confirmed with all the risk connected to running this software, because you can be testing website risk in your country, and we don't know the laws about every country. Like to extend to the user and what is about to run. There's a link here with a risk page. You can get it.

You can make some choices. One is how do you upload data to our collector. If you want to share your IP or not or if you want to share your code, then the type of test to run. And lastly, how to contribute to test lists. We will talk about that later.

So the test lists we use are often on citizen lab and github. We have two global lists. If you want to contribute, there is a link, and you can contribute to your country or to the global list, and it's really important because we need to keep these lists updated and relevant to every country.

So the type of tests we are actually doing are four or five mobile app and all of them in the web app on RaspberryPi. One test of web connectivity, web connectivity is basically a website, if it's blocked or not. A various technique, or TCP connection. And try to compare the controlled experiment. So if one is detected, we tell you which block and how to circumvent it. There can be, of course, a false positive due to DNS server, or the content depending on the country.

Then there is the HTTP invalid request line. You try to send a request line to server, and get the same string back. If you get an error, by middle box, and there is something between you and your connection.

Then, there needs to be field manipulation. I'm skipping over test, otherwise I have too many slides.

So what we collect. We collect the country code, the autonomous system number, data and time, network measurement data, the ITI if we are going to share it, but it can be collected without your consent based on some condition. And to upload data, there are different ways, the HTTPS collector and the cloud-fronting.

These are from the web application. You have the test, you can run it. Then you have the rest of your measurements, the logs, and adoption to configure the web interface.

This is the mobile application. I'm really proud of -- actually, this is the first version. There will be five versions after this. We have two more tests, three now, and you can run tasks in a really easy way. And the final page. Or you can run it on our RaspberryPi. You just install it and run it whenever you want.

So talking about data. The data we collect is open for everyone. It allows independent studies and experiment on the data. And even the public to verify the findings.

So the data is available on OONI Explorer, country by country. Or for more technical people, we have an API, the measurement API where you can download the data and extract it and play with it. I really encourage you to do it.

So interpret the data, you can measure in normal and -- and the content, they are not identified. Like said, a lot of false positives. So if you want to get involved in OONI, you can become a partner of OONI. We are a partnership program. You can join me on a monthly community meet on Slack. Even reporting bugs on github. You can contribute to a test before or analyze the data, tell stories, and who knows? Maybe you will spread the word about us.

As I said, I encourage you to install the app now, because it's a really great app, I should say, and it's really well-done. If anything, you can go to (?) and she will help you to install the right links.

>> RAMAN JIT SINGH CHIMA: Thank you so much. In fact, I'm also going to look for some of the tweets. Many people will may OONI's fantastic partnerships and many organizations also in turn have support for organizations who are trying to work with OONI. Access Now has a grants program. Many other organizations in this space have been in discussions already. I encourage you to work with them, because more technical information is useful. As Lorenzo mentioned, it's sometimes difficult to determine particular website from shutdown. More technical data is better than less. I thought maybe close with one more person on the panel and throw it to open questions.

Apar is there remotely. Apar, would you like to come in now? Apar, could you unmute and try to comment?

>> APAR GUPTA: Hello. Am I audible?

>> RAMAN JIT SINGH CHIMA: You are. Just speak up a bit.

>> APAR GUPTA: Okay. Thanks for bringing me in here. I think to some extent, Internet shutdowns specifically focusing on India. I'm getting a lot of feedback.

>> RAMAN JIT SINGH CHIMA: Mute the mics.

>> APAR GUPTA: I just mute my speakers. So what they are saying is that there's a considerable body of research, which is just existing -- a lot of it has been sourced on the basis of goods which exist. (?) there is a lack of state transparency in issuing orders, which by themselves are the reasons that the shutdown has been done, as well as the period from the shutdown has actually been implemented. And cataloging these legal orders is the triple task, given that they are not proactively published online and open. They are issued in geographical areas, which are fairly small, which are a town that restricts administrative unit in India.

So that's one thing which is important to consider. Now, given that a lot of the existing research in India is based on media reports, a much more systemized process needs to be dealt with, engaging the policymaker of people in government, and also is being stated by -- maybe also look at how Internet shutdowns are existing. Could be also looked at.

So what we need to do is become digital systemized. Come up with litigation strategies, not necessarily to pile issues directly in the Supreme Court, but I think more in terms of what happens with each -- and this goes above and beyond writing to, let's say, people in the government and much more actively examining and reviewing the law. This is a correct implementation of the existing law. Even making the interpretation of existing law come about a little more clearly, that shutdowns -- so given the time constraints, I'll end now. Thanks so much, Raman.

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

In fact, that is a good setup, and we're going to go to open questions. Just a bit on the challenges. How do you respond? Is it courts? Is it policymakers? Is it a mix of institutions elsewhere? Maybe a little bit of that, and we can toss it to people's questions about how better to engage.

>> RITU SRIVASTAVA: So I think what we have seen, Raman, this is not just India. I think it's a sample in terms of what is happening across the region. I think the frequency has grown in terms of Internet shutdowns across the region, and every country, when you talk to them, particularly national governments in terms of causations of imposing Internet shutdowns, there is a kind of exceptionalism that everybody will argue, that we are in a very unique situation and often unicultural diversity and cultural differences is used as a reason to argue exceptionalism and create some kind of an immunity to justify shutdowns. That is something -- I won't single out any particular country, but I've seen this across the

region, and and if you look at central Asia, the problem there is even more severe.

So I just say that's a point which I wanted to put out there, which is this is something happening across. The frequency is growing. The kind of measures which different governments are taking is also kind of there is -- there are two -- there are three key trends. One is that it's started off with the blanket network shutdown. Over a period of time, it got sophisticated in terms of governments or law enforcement agencies having the ability to reach out to ISPs or the network operators directly, and then do domain level blocking. So there are those capabilities which operators now have built where they are asking -- where they are being asked to block out specific domains. And that is problematic, because there's no way that you would come to know of it. Like, Internet platform, a platform like Facebook will not come to know that it has been blocked and such, because these notices are not served on us. These notices are served on the operators because they are the licensed entities and we have to comply because they're written into the license obligations, as you and I and everybody else in this room knows.

So that's the second trend which we've seen. The third element which is very interesting is that -- and, again, I go back to the causation point, that it's a combination and a conflation of national security and fake news, hoaxes, rumors, which is being used as a reason to shut down in the Internet or engage in the selective blocking of domains, which is a different discussion altogether, and there are countermeasures available to deal with both concerns of national security and as you know, that there are measures in terms of accessing of data access as well as content takedowns. Those options are available under the national security augmentation, which we see often, and also in terms of fighting hoaxes and rumors. There are other countermeasures, which are available in terms of both the takedown process as well as in terms of working and civic action level to make sure that there is an integrity in the news feed in order to fight fake news and hoaxes.

So I think these are the three main trends which I am seeing. In terms of moving to the solutions, of course what Lorenzo talked about and what Apar talked about, there's a lot of merit in there and we have to think about the coalition work which advances both of the technical countermeasures which needs to be done, because first of all, many times one does not even come to know. So efforts such as SFLCs, and the kind of the docketing, which Apar talked about is very important in terms of just making sure that there is the database which is created. Not just to talk about (?) but also to talk about the economic consequences. The economic harm as a consequence of this kind of shutdowns is something which needs to be documented.

The other point I would argue for is in different

countries, there is this discussion in our region on the trending of the rule of law system, and therefore we really need to look at the rule of law sort of framework to try and see how can you get judicial involvement and intervention in terms of reviewing this entire phenomena of Internet shutdowns, which as you know the levels of harms of the shutdowns have created a multi-level socioeconomic, political, and therefore there's a need to review that versus our fundamental freedoms as well.

So I think those are the kind of things which I would love for our community here at the IGFs to do. I think as an industry, we are very committed to the GNI process, and various local campaigns, which we are part of, in terms of our own individual advocacy work with policymakers, governments, parliamentarians, et cetera. This is by itself a bad act, and therefore, as we're looking at more growth of economic and network societies, you have looked at countermeasures to address concerns of national security and hoaxes and exceptionalism, cultural exceptionalism cannot be a reason for Internet shutdowns of the type that we have seen.

>> RAMAN JIT SINGH CHIMA: Thank you so much for that. That's a good setup I think to take open questions now. We have around ten minutes, we could potentially go into lunch with those who are still here, and we will be available outside.

I'll just note that many people here have specific projects that they are working on. I see many people in this room doing research on the economic effect of shutdowns as well as technical materials. Questions about how to collaborate. While this is an open session, and there may be sensitive discussions, feel free to ask questions. We'll take maybe a couple of questions.

I see one. Anyone else? If we can get you a mic. There's one there. If you could just queue up there, that would be great.

>> Hi. I'm wondering if we should find distinctions between the shutdowns. And I find that when I interview the people, they were not unhappy about the shutdown in the sense that they sacrifice some of their freedoms and so on, because they felt that they were getting some things back in exchange. It was like security, less of the rioting, less of the Kay yacht. It's not too dissatisfied. So I think some of these shutdowns may be acceptable to the community, if there are good reasons, and for a short period. So I think this one distinct ought to be made.

And the second is some of the claims about economic damage is overstated, because some things people do compensate. So I think we need to be frank and be brutal and say that these are overstatements, and I think that's not really fair.

And the third thing is that we are seeing that the security concerns are not being addressed at all. I mean, I hear no shutdown and so forth, but what about security concerns? Can we

come up with something that we can address some of the security concerns?

And my final point, I am proposing a conference to discuss the issue -- the best place -- because the shutdowns appear to be concentrated in south Asia. Perhaps in Nepal we can meet. So please drop me a note, I would like to get in touch with you.

>> RAMAN JIT SINGH CHIMA: One quick question. You said economic harms might be overstated. Could you explain that briefly?

>> I see one report talking about how they take -- the way to do it is what is the economy of the country. The valuable number of days. And then every day that it is shut down, it's one day off. And you look at the percentage of the Internet, on penetration in the country, and compute it that way. So if the economy is 20% of the economy, shutting off for one whole day, 20% off one day of the GDP. I think that's an overstatement because people work around that.

>> RAMAN JIT SINGH CHIMA: We will take another question as well and have some responses and try to take more questions.

>> Thank you. Hi there, from Bangladesh. My question is -- the shutdown, those kind -- it's like, is there any kind of international grounds, any possible actions to make that are giving the authority of the governments not to shut down certain times or certain websites or social network, because even from my country, governments can't deal with anything. Just completely shut down everything. Why like more than -- nowadays, there's like more than two million they are getting. Like the people getting from the outsource of working. Definitely, like quickly (?) to the economy.

So is there any kind of background, do you guys have anything, or is it not -- how could the policy be met or the framework that could lead these kind of situations right now?

>> RAMAN JIT SINGH CHIMA: I can try and answer the two questions. In the meantime, one suggestion and three questions. We noted that -- would anyone like to first address that? I think the first question, are some type of shutdowns okay? Can we categorize? Would anyone like to take it? Ritu?

>> RITU SRIVASTAVA: The definition of a shutdown is not being transparent about the state itself. They are stating to just to stop the spreading the rumor of fake news as well as national security. But the definition of national security is not being defined by the state. In one other case, what we have seen as well, why the shutdown is being there. In one case, when we are asking, they said that if the government wants to track down the terrorist, they can do it. They have CTV cameras, but how they have blanketed down the network itself. It causes panic and emotional distress. Instead of giving them relief from such kind of a situation, especially when it is for a longer duration. It's being blocked from the three months or four months, and 41 days. So the life of common people disrupts

when they are unable to access certain kind of services and those kind of things.

So, in fact, my colleagues also have asked that definition of national security needs to be transparent by the state. It is not okay to shut down the blanket services as well.

>> RAMAN JIT SINGH CHIMA: And this one commented, I think one challenge is that sometimes there may be shutdowns that people might be okay with. I think the question is on a rights-based framework, is that a good idea. I like the prerogative question. People might be okay with lynchings. 70% of the population may say, yes, that person should be hung by a tree. That doesn't make it right. There is a difficulty in mapping perceptions. You need to find the people who are most affected and excluded. So that's a social research question, how do we do that.

I think the economic -- we don't have -- Kay, would you like to answer the economic?

>> KAYYEN WONG: I think respectfully, I would like to disagree with the notion that there is no economic harm. I have not looked at a whole lot of studies in the region, but the study that was put out was pretty thorough. It was done by sort of through a very intense methodology, which I think is extremely well defensible externally in any forum. So I would encourage people to really look at the methodology also.

This is something that cannot be set aside, because it is very important, particularly for countries which are pivoting a lot in terms of building national initiative plans. A whole lot of trade is happening because of the integration with Internet, and even if you're to set aside the rights discussion for a moment, just looking at the economic harm, it's pretty enormous. There is no such way that you can work around. It has become a factor of production. Like, there are N number of SMBs, small and medium businesses, and if you shut it down, you basically have shut that out. You've shut out jobs. So I disagree with that sort of notion. And now there is data. Luckily now there is data.

And also, you know, in my generation, when we were growing up, there was this trend which would happen a lot because there was a lot of agitation at that point of time, where railways used to be stopped in their tracks. Right? Because people would agitate and they will not allow movement of railways from one point to the other. That stopped, and the reason that stopped is because people realized the economic cost of stopping railways from moving from one place, trains from moving from one point to the other, is they were carrying services, and disrupting the economy of a particular state. That notion led governments and other political parties and other civic agitators to pull back from that as a tactic. So it's my hope that the economic cost over a period of time will become so apparent to everybody that people and governments particularly

will stop using this as a measure to account for whatever issues they are confronted with.

>> RAMAN JIT SINGH CHIMA: I mentioned at the beginning that I think the work -- it will come in his report, as well as even previously general comment in the civil rights, from the human rights committee. Basically, there are norms on this space. And by lodging, blocking the entire Internet might be something even more nuclear. I think David has made comments clearly on that, but we can take that offline and talk about that.

>> RITU SRIVASTAVA: So there there was a human rights council last year in July. Specifically condemning (?) and they said that the rights in the online sphere, they also required the same standard of protection as the rights in offline spheres. For example, the right of free speech, freedom of expression. So the U.N. has also kind of endorsed that should not take place. But there are no specific -- no cases as such.

>> RAMAN JIT SINGH CHIMA: We have two more questions, so we'll take those. Introduce yourself briefly.

>> Hi. I am Jaden from the Philippines. Michael told us about the use of national security. I totally agree. I agree that we should not use national security. I share your passion, I share your idea that we should run upon the idea that we are using national security as a blanket tool to justify the blocking of any website.

But my problem, my personal issue is that we cannot just say that, no, you can't use national security, but what are we -- but we should also recommend what terms do we use if it's possible, because there's also legitimate reasons why the government want to sanction or to block this website. But what are we recommending so that we can come up with ideal setup that we can prevent -- I am not really -- I do not really want to use the term national security, but we should prevent some forms of terrorisms, but within our justifiable bounds. Thank you.

>> RAMAN JIT SINGH CHIMA: Thank you. We'll take the other question as well and then try and answer.

>> Hello. I am Saku from Bangladesh. Actually, I have a question. So I can ask Kay. She is the technical person here. My question is about OONI. The question was that when we are actually -- we are doing a look-up or something, so far that user's IP address, we are also getting the user's IP address. So when you are giving them freedom of speech, as you are saying as you were against this block-up, but at the same time, you are not also doing like some kind of privacy reading or something like that. And if users are giving you this kind of their personal data, this is the main portion. What is that policy that you will also secure. This might be some problem.

>> RAMAN JIT SINGH CHIMA: Maybe we can answer them backwards. In fact, Lorenzo mentioned that they have a privacy policy, and do you want to answer that?

>> KAYYEN WONG: I believe you can choose to opt out sharing your IP address.

>> RAMAN JIT SINGH CHIMA: So it's not just a privacy policy. Go ahead, Lorenzo.

>> LORENZO PRIMITERRA: Actually, opt out by default. So you want -- you really want to share it. Just share it with us. Otherwise, it's disabled by default. We will only collect your country name and your (?) that's all, and really generic data about you. We will know nothing about you. We just know that you opt in and you want to run tests.

>> RAMAN JIT SINGH CHIMA: Thank you so much, Lorenzo. I think that's a fairly clear answer. You can catch Lorenzo online. OONI is open to ideas. OONI collaborates with many groups on how they can make it better, including legal tests on how the policies can be made better. So if you have a concern, don't hold back. Share it. And we can pass on questions to OONI.

There was one other question -- it was a positive agenda, but can you have specific recommendations about when shutdowns can occur, what actions law enforcements and states can take. That's a provocative one, so I want to ask who might answer? Maybe that's the one we can end with and take questions offline. But does anyone want to try and answer that, the tough question about when can people do stuff, what is acceptable, what's not in this? There's a reason also for that, because if you start saying there's a middle ground, it's easy to say shutdown is perfectly legitimate, but it is a good question, right?

>> When we talk about shutdowns, we talk about blanket bans on shutdowns. That is for the reason of -- other reasons, security reasons, national interest. You cannot shut down the entire Internet, thereby blocking access to all the (?) as well. So maybe we can have a little bit of discussion as to whether selective blocking of sites in such conditions might be a solution, or whether they're also not justified. But, however, we do disagree that -- we do agree that a blanket ban on shutdowns in which even the basic utility services are also blocked, they should not be done, because they deny you basic access to services.

>> The one point which we also need to think about, when we are in a crisis, we need more voices from the government instead of blanking it down. City police has used Twitter just to mention that there are arrangements by the city transportation for providing the services. So it can be used as a flip side to use social media websites and other tools to bring the calm and bring quiet and calm place and peace in the society itself, or the community itself. Instead of shutting it down in the blanket notion, it won't help it that much. So we do agree that a blanket shutdown should not -- there can be some level of transparency and accountability by the state as well as by the -- I don't know about the telecoms, but there some sort of

accountability on the ground as well.

>> RAMAN JIT SINGH CHIMA: One, firstly, is that the sort of thing that Ritu just mentioned is that actually the massive use of social media by government to dispel rumors and provide information, even fake news. Sometimes the best answer to fake news is that when officials are online. That's when officials say horrible things also, public figures. They can. They're human beings. But the example is great, because three years ago in Banglo city, the discussion was let's shut down the Internet, and now you have police and chief ministerial officials saying they would rather use the web. You remember the first actual discussion of a shutdown in the London riots a couple of years ago under David Cameron, where there was a discussion they want to shut down social media.

No shutdown occurred. B, they studied the London riots. There's a fantastic report which I recommend everyone reads. It's very brief and very clear. And they interviewed the metropolitan commission of police, the head of the UK police force, and he said if you shut down social media, at least that would be illegal, and he said it would have been illegal. Secondly, it would have been counterproductive because we're dispelling rumors online. And he said, we're attracting people. We were just seeing someone tweeting out pictures. Look, I smashed a glass window and they deploy officials to that area.

So you can see the dynamic responses that were taking place. So that's an interesting thing to take. I wanted to say, the only institution I am ever tempted to say a shutdown of the entire Internet is actually the technical one, massive malware attacks, where, in order, sometimes you have to set off a switch. You have to be able to purge your network logs. That's perhaps the only occurrence. But, again, there could be debate on whether that's acceptable. In this region, we have heard cyber security agencies. We are also doing cyber security. At least in my home state of India, and I know you've heard too much of India in this session.

Perhaps that's the only model there. It's provocative. We'll take these comments. All is open to comments and criticism. They are also engaged in this and I believe there will be a consultation in a couple of months where many of them may be in this region and take parts and you should feel free to share that.

Many of us are available here, and we have ideas about criticism, thoughts, recent methods, legal ideas, please come and catch us, and we're available. But with that, I thank the panel and thank all the participants who have been patient, and thank you for your patience.

[Applause]

[Concluded at 12:29]

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.
