Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

Courts at the Crossroads: Defending Digital Rights Against Encryption Crackdowns in South Asia

Raquel Kroich - Internet Society: Hello, welcome everyone to Encrypt a Date to Safeguard Tomorrow. We're kicking off with the first session of the day, Courts at the Crossroads, Defending Digital Rights Against Encryption Crackdowns in South Asia.

Let me just pass it to Karthika, just so she can start the session today.

Karthika Rajmohan - Internet Freedom Foundation: Thank you, Raquel. Hi, everyone. welcome to the Global Encryption Day Summit 2024. I'm Karthika Rajmohan. I'm an Associate Policy Counsel with the Internet Freedom Foundation. We are a New Delhi based civil liberties organization working on digital rights issues, and I'll be moderating the session today.

IFF is thrilled to be organizing a panel as part of the GED Summit. The discussion today, like Raquel mentioned, would be on Codes at the Crossroads: Defending Digital Rights Against Encryption Crackdowns in South Asia. The inspiration behind this panel and the context that we're relying on is the increasing amount of governmental efforts to curtail end-to-end encryption under the guise of national security and crime prevention.

We're very glad we have a panel of extremely qualified, esteemed speakers who are digital rights experts from various South Asian countries. I'll briefly introduce all of the speakers. firstly, we have Dr. Sanjana Hattotuwa. He is a disinformation expert at ICT for

Peace Foundation, wherein he studies information disorders and its impact on democracy and society.

Next, we have Ms. Vrinda Bhandari. she's an independent advocate who litigates free speech and digital rights issues in India. And she's also an off counsel with Internet Freedom Foundation. next we have Mr. Shahzeb Mahmood. He's a senior researcher at the Tech Global Institute where his work primarily, examines online content regulations, AI, and deepfakes.

Then we have Ms. Farieha Aziz. She's a co founder of Bolo Bhi, a civil society organization geared towards advocacy, policy, and research in areas of digital rights and civic responsibility. And lastly, we have Mr. Santosh Sigdel, the Executive Director of Digital Rights Nepal, a non profit initiative directed to protection and promotion of digital rights in Nepal.

So now that we have, introduced our panelists, we could perhaps move on to some opening statements. maybe the panelists could start by giving us some context on what is the situation in their respective countries, what are the kinds of crackdowns that governments have been doing, against end-to-end encryption, and the kind of justifications that are being used the same.

I think for opening statements, perhaps we could start with Dr. Sanjana. If you'd like to begin.

Sanjana Hattotuwa - ICT4Peace Foundation: Yeah, thanks and glad to be here. I'll keep it short. For those from the region, Sri Lanka is a known story. We've just had a consequential presidential election, so we don't know whether what we have seen in the past will continue into the future. One hopes not. But the general context of the country has been a familiar story for other South Asian countries as well, where state authority, executive authority, and impunity have impeded, the freedom of expression and fundamental rights in the country for decades, well before social media, but it has been exacerbated as a consequence of, increasing interest in private privileged communications by the state and the securitized state in particular in the guise as was introduced, to curtail and combat terrorism, but also in Sri Lanka, with a view to this, protection of women and children argument, where there has been a lot of regulation and laws passed or, contemplated to be passed to ostensibly protect women and children, but is quite damning with regards to first principles.

I'll just, speak to two. One is an absolutely draconian law, unprecedented in the country's legislative history, called the Online Safety Act, which came into play in January this year. it's a longer story as to how it came about, but now it's in our statute books, and it's, I can't use, because of the Code of Conduct, expletives on this call, but it is horrible.

it is antithetical to, every imaginable, human rights in the Constitution. it's extraterritorial, it applies to everybody. On Earth, as incredible as that may sound, it goes back in time to the first time that you would have used the Internet, and it's, incredibly privacy encroaching, it is under the executive.

Which is a big problem because of the constitutional nature of the country and how powerful the executive is. It allows the law to get into any device, anywhere, at any time, over anything, over a category of content called prohibited content. And that's not me making it up, that's in the law. that may mean anything.

So it's not very defined. In fact, there are clauses in the law that have said read love like a romance novel, because in the law, it's said that if you say something that upsets the feelings of a community, that's It a possible intervention point. And I've said that I have no feelings when I've written love letters or whether I've received love letters, but it's very strange to find that language in law.

So the OSA can force disclosure and it's actually really quite bad. It impacts E2EE obliquely. In a context where you must understand in Sri Lanka, at least, where we are a very violent country and the Ministry of Defence regularly and over decades has, without any kind of due process, twisted the arm of telcos to get the information that they want.

Just to make it very clear, you don't need in Sri Lanka to undermine E2EE when you can actually arm twist the telcos to get metadata or some of the data that you might want around targeted individuals or institutions which are generally human rights activists. I'll end by saying that there is a second law which is in the draft stage and we don't know whether it's going to go ahead with the new executive president and the government, the parliamentary elections in a couple of weeks.

We don't know what the timeline of it is but under the This is a form of government. It was going to be introduced quite soon, which is called the Anti Terrorism Act. So we have a Prevention of Terrorism Act, which is draconian, but now we have an Anti Terrorism Act, which is ostensibly trying to fix the PTA, but it's actually quite worse.

And here we take a branch, a page of India, Where, the WhatsApp, the Indians on this call can speak to the High Court, Delhi High Court case with Facebook and Meta and WhatsApp and, the whole conundrum about them moving out of the biggest market if they were compelled to undermine their own E2E with WhatsApp But section 65 of the proposed draft of Sri Lanka's ATA is the exact same thing.

It will compel all Internet intermediaries and anybody, really, to give up their keys, give up their information. So it goes to the intermediary level, it goes to the platform level, but it also goes to the individual level. And it's, I won't read out the clause, but there's nothing like it again in our statute books.

And my point has been, if WhatsApp and Meta wanted to get out of India on account of what they were possibly being compelled to do, we as a country are less than the market of Mumbai. So I've alerted folks that, what do you think Meta is going to do in Sri Lanka if this law comes about. So I'll end by saying that it's, not the case that we are as bad as India or Bangladesh or Pakistan or some of the other countries, but the proclivity, the political preference and the bias is to undermine.

encrypted privileged communications. And this is now something of a bit of a central focus of those in the MOD and those in government, with a view to getting into civil society activism and, getting into privileged communications that they think is inconvenient because it's inconvenient for them.

So the argument is made around ostensibly, Curtailing terrorism, protecting men and children. But we all know, I hope, on this call and in the audience, that the end result of that is absolutely detrimental to first principles. So that's the general broad context of Sri Lanka as it stands today.

Karthika Rajmohan - Internet Freedom Foundation: Thank you for that. That was very useful. A lot of points I would love to double click on, but we'll come to that later. now if, Vrinda Bhandari ma'am, if you could Start your opening statement.

Vrinda Bhandari - Internet Freedom Foundation: Hi. I think it's perfect to go next in terms of we've already seen the context of Sri Lanka, so I think India follows suit, and I'll start maybe by actually talking about the challenge, that has been issued by WhatsApp.

So what happened was in 2021, the government amended, basically introduced rules called the intermediary, they have a very long name, but for our purpose, I'm going to call them the IT rules of 2021. Now, interestingly, this was not done through legislation. It was done through the government issuing a notification.

So under the rulemaking power of the government, and what happens there is you avoid parliamentary scrutiny, you avoid legislative debate, so it's easier to pass things through. So it was in the exercise of its rulemaking powers. that the government introduced these IT rules, which, were in two parts, the first part dealt with intermediaries and codified and added additional new due diligence obligations.

And the second part dealt with, news publishers online, so digital news publishers. and online content providers. so the controversial portion was rule 4 subclause 2 of these IT rules, which effectively requires these significant social media intermediaries, which is every intermediary, WhatsApp, was easily included.

So if you have more than 50 lakh users, you would be classified as a socially, significant social media intermediary. and what this did, so there were two parts that came in the rule. First, I'll talk about. the part that, in a way, has been challenged but has been

completely complied with. So this goes to your question, Karthika, where we think, what is the government's argument?

So the government's argument, to some extent, was all these social media platforms, none of them have offices in India, right? All their offices are in the US. So every time we have any law enforcement request, it's very difficult to get the data for us. because, they'll say, we don't have the data is not stored in India, the data is subject to US law.

So what these rules did, they mandated everybody, which is, which is a significant social media intermediary to have a resident grievance officer. Who was based in India. And what that does is when any company has to have an officer who, has to be based in India and then is subject to the jurisdiction of Indian laws very directly and Indian court, it encourages compliance.

So that was the government's, argument. They said we need to have better compliance. We need to have data, access to data which are used in crimes, and hence we need all these companies to have a separate grievance request. So if you actually go. To, Facebook, Instagram, WhatsApp, all of these pages, they'll have Twitter, they all have a separate, grievance redressal officer who's designated for the purpose of Indian law.

So that the government did because they said it's very difficult for us to get data under the MLAT process, which is the Mutual Legal Assistance Treaty process. so that was the first part. The more controversial part, and what we've touched upon a bit, is that Rule 4. 2 effectively requires these companies, that were providing messaging services to disclose the sender of the message on any order, right?

Now this disclosure has to be done for cases of national security, public order, any offenses, child sexual abuse material, etc. And the main challenge that WhatsApp did is that they said, look, this is going to break encryption. we cannot disclose the originator of the message. Unless we know who's the originator of the message.

and what I also want to point out is that it is actually very rare for tech platforms in India, and I'd be interested to hear other countries experiences, but it is fairly rare for tech platforms in India to take a proactive challenge to the law. Usually they're respondents or, they're, pleaded as respondents against, some other petitioner challenging or the government order.

But it is very rare for a social media platform to actually actively, challenge the law. And so this was an interesting example because it was one of the first cases. Twitter then followed up later with a blocking, challenge. But this was, this was interesting because it's the first time WhatsApp said, We cannot identify the originator of information.

Doing that will break and do an encryption. That is not how we work. Once we create a backdoor for one person, we have to create a backdoor for everybody. so the rule

actually was very clear. The government was trying to say, look, we've made lots of safeguards, so you don't have to break encryption. Any other less intrusive means are possible.

The rules also provide, according to the government, they say that if you have to comply with the identification of the first originator, you are not required to disclose the contents of any message, or any other information related to the first information, originator related to its users.

And then the rules also provide that when the first originator of the information is located outside the government of India is only interested in the first originator within India. So you see, it's not just that you're breaking encryption, you also then have to break it geographically. So you have to see who is the originator, who is first in India.

so I think this is it in terms of background for this Rule 4. 2 challenge. What I will say is, Although this came in 2021, finally, three years later, the government, the court, the Delhi High Court now is hearing petitions, challenging these rules, and they finally set it down for hearing. And so we are hoping that maybe in November, December, or early next year, actually hearings in this will conclude.

so we're actually After many years, on this point, we are actually going to be able to see some hearings. So we are in port on that. And then just very quickly, I just want to also mention, apart from these rules, there will also be cert in rules. So this is the security Centralization, the centralized security agency rules, and that deals with VPN providers.

And I just wanted to touch on that because that basically said that all VPN providers have to mandatorily enable logs of all information systems, all the users, the names, addresses, you Contact details, email addresses, et cetera, which was also challenged by a separate VPN provider, IFF provider systems in both these petitions.

And so that's another thing that if people are interested, we can talk about more, because that, deals with encryption in a different sort of way or deals with privacy in a different sort of scenario. So I think that's all for right now for India.

Karthika Rajmohan - Internet Freedom Foundation: Thank you. That was super useful. A lot of interesting context.

This is something that I think has... so I said jurisprudence across, multiple other jurisdictions as well. now if we could, hear from Mr. Shahzeb Mahmood, would you like to start with your opening statement?

Shahzeb Mahmood - Tech Global Institute: Thank you, Karthika. so I'd like to start by addressing some of the issues raised by my previous, Previous panelists speaking on the matter.

So Dr. Sanjana Patatua, I think he highlighted quite correctly that the legacy of the colonial laws, the languages that are used in this school, some of the colonial laws that we share, that permeated into the current legal landscape governing the Internet, which very much characterized how policies are developed in South Asia.

Ms. Vrinda Bhandari also mentioned. that cases, tech companies proactively pursuing cases is an exception. And my research has also shown, and I concur that it isn't an exception, and these are based predominantly on the internal policies of the companies. We'll talk about it more. As far as Bangladesh is concerned, the courts have had limited engagement with previously jurisprudence.

There's this one case from a few years ago where the high court division recognized that routine collection of call details and audio records without due process, without following due process and their unauthorized disclosure as leaked audio. it constitutes breach of fundamental rights, granted under.

Article 43 of the Constitution. Yet, robust judicial intervention against state encroachment in the areas of encryption, surveillance, and digital privacy remains quite minimal. So I'd like to point out three issues that characterize this lack of intervention. The first is face surveillance and interception, which are routinely carried out by, covertly, under, my apologies, by the recently ousted regime, and it was often done in collaboration with the telecom operator, including a lot of multinational subsidiaries.

This was enabled by broad provisions in the Bangladesh Telecommunication Regulation Act, and the licensing, the telecom licensing regime. And justified by an expensive, an expensive interpretation of Article 43's exception, which permits restrictions on privacy, on national security, and public order grounds.

And these terms problematically remain inadequately defined in Bangladesh. I know that it's fairly well defined in India, but in Bangladesh it's Still relatively undefined. The Supreme Court of Bangladesh have the mandate to assess constitutionality of laws and administrative actions. and over the years, historically, they have been quite proactive in legal reforms through suamutu rulings, through exercising extraordinary jurisdiction, issuing guidelines, passing seminal decisions.

But the relative inertness of the judiciary against their actions. Systemic state surveillance, over the last one decade is something I believe that has not gone unnoticed. The second issue I would like to touch upon is the issue of encryption, which is a simmering issue in Bangladesh, and an excellent case study for regional contagion.

India's enacted the information technology rules in 2020 2021. Introducing the traceability provision, which is essentially a requirement to identify the first originator of message shared on services or messaging other intermediary services. Now Ms. Vrinda Bhandari has, covered it quite well, so I'm not going to get into the details of it.

But it's quite, it's, quite interesting how this came about in Bangladesh. It came through a constitutional challenge, by, two way of repetition and, it, involving content regulation. And traceability requirement was introduced in the first draft of the proposed regulation submitted to the High Court by the Bangladesh Telecommunication Regulation, Regulatory Commission.

Unlike India, however, there are no threshold requirements, and the provision was meant to have extraterritorial reach. So technically, all service providers, and Even non residents were caught under the regulation. Now we, along with Internet Society and Access Now, raised awareness on how this would harm journalists, rights advocates, and opposition, because at the time there was limited to no understanding and awareness of how these provisions operated.

And we did a lot of myth busting around this in, how this is an ineffective solution to a genuine problem. Now, there are two arguments at the time that I heard from the proponents of traceability provisions. The first argument is that traceability is essential in a country like Bangladesh, to identify perpetrators of communal violence.

And within the constitutional architecture, it is both reasonable. And, warranted under national security and public order grounds, with counterbalance against previous consideration. And given that intermediaries, in most cases anyway, comply only when they want to, so naturally pushback against overreaching requests is expected.

So that was the first argument. The second argument, an argument that I found more interesting, is that traceability is being reframed as a privacy violating provision when in fact it is not, was the argument. Intermediaries do not necessarily have to break into an encryption. And that they can easily develop rights respecting technological backdoors to assist state authorities to address on the ground, real world problems that are being faced in Bangladesh.

the argument was that you do not necessarily have to break into an encryption in order to enforce the traceability provision to get to the first originator of the message. There are other ways of doing it, just like how Google, for example, developed Content ID to get copyright content. You just have to invest in technology to get to a point where you can do it without breaking into an encryption.

Now, ultimately what happened was, because there was no policy or technological solution forthcoming from the proponents of traceability provision, It was eventually dropped, from the revised draft of the regulation that was submitted to the court. Again, however, in, the silence of the court in addressing the issue head on has not gone unnoticed.

And finally, and very quickly, the third issue, is, how over the years, many services have, that enable end-to-end encryption have been restricted in Bangladesh, especially over the last, decade, and a half. Again, judicial intervention has been lacking here as well.

I've documented these restrictions, in an Internet shutdown report published by Internews and Optima, as well as article published in National Dailies.

in the interest of time, with that, I would like to thank the moderator. For the time, I'm happy to take any questions.

Karthika Rajmohan - Internet Freedom Foundation: Thank you so much. Again, interesting point raised that we would love to get back to. But next, if we could have Ms. Farieha Aziz to give her opening statement.

Farieha Aziz - Bolo Bhi: Thanks, Karthika. So many similarities and parallels that I'm hearing from previous speakers. Let me try and walk you through just this year in Pakistan with respect to what has been in place.

So this was election year, very controversial elections, and the question of legitimacy and mandates still continues, and our courts are literally at the crossroads right now. just early this morning, which is at 4 a. m. passage of a constitutional amendment, stream rolled through both houses of parliament, without any debate.

The judicial appointment process has been amended, and this is a controversial amendment again, where the handpicking of a Chief Justice is going to happen, the, the commission who is going to appoint judges is now tilted heavily in favor of the current political setup, So we're going to see how all of this pans out and now constitutional benches have been formed within the Supreme Court and the High Court and how that bifurcation is going to happen.

We're going to see, because litigation was one avenue, even though sometimes you don't get very far. but still courts were a venue for, and a site for contesting some of the violations that occur. And all of that now is up in the air, and we'll see how all of this settles. But February we had the elections, Internet disruptions, were happening, and on, and then we see that X is blocked.

First there was no official, acknowledgement from the government, and then it transpired that there was a notification, and the, information minister. And then finally, there were basically cases before various high courts of the country. At the moment, all high courts of the country, there are petitions pending regarding the ban on X.

And what they ultimately submitted in court was that X has been banned on account of national security. And obviously, relating it to, firstly, election related disinformation. but then also it became about, terrorism, as Dr. Sanjana also said, so for example, and not just, terrorism in the context of what the government refers to as separatist movements in the different provinces, but the military chiefs has also come on television to coin the phrase digital terrorism in relation to political parties and their workers using social media. So there's that aspect of it as well.

And then the second thing that, the government said in its submission to court, and this is something, that Ms. Rinder also spoke about rules. So we have the social media rules under the Prevention of Electronic Crimes Act, which was enacted in 2016, the first cybercrime law.

And in it, what was done was, And we have, I'm sure, shared frameworks. Article 19 freedom of expression from our constitution was literally copy pasted into this piece of criminal legislation and the Telecommunications Authority was given, in my view, our judicial and legislative powers to essentially interpret and apply the exceptions that exist, and we have a long list of exceptions in Article 19. You have the right to freedom of expression, but subject to glory of Islam, and national security and friendly relations, and the list goes on and on, for the exceptions. And we've seen arbitrarily how the Telecommunications Authority has blocked different websites and then came the social media rules, and again, borrowing from India and other jurisdictions, and the intent always was we want these companies to form offices and appoint staff.

And and again, the grouse with the, with X particularly is that they don't comply with our requests and they haven't opened offices as per our requirement. And in Pakistan, none of these companies have a presence unlike other regions. so that's the difference. And again, the same argument that, we send them requests and they don't comply with these requests.

And so it becomes this carrot and stick tactic where they'll keep them blocked, till they come to the table and start complying to some degree. And this has happened with other platforms in the past. So that happens. And then. We also hear that, Internet has been excessively slow, we hear that it's submarine cable faults, but also that there's a so called national firewall being installed and interchangeably being used with a web monitoring system or a management system, and previously there had been procurement from Sandvine, Deep Packet Inspection Technology, So then that part as well added on and you know what was mentioned I think in the Indian context as well is that those who are locally incorporated so the telcos and the ISPs and there's very little they feel they can do because their licenses can be cancelled at any time and so For them, it's like the path of least resistance, and they go on and comply.

One very significant court case recently was about this surveillance system, the Lawful Intercept Management System, as it was called. And it's been in place since 2013, but it wasn't until in a political case where audios had been leaked, of the former First Lady and also the son of a former Chief Justice, they went to court, and the hearings and orders ensued.

Turns out 4 million subscribers at a time, their data is being passed through a centralized system, just being handed over. and there's no scrutiny. And when the court inquired under what authority, are you doing this, turns out that nobody, no agency was authorized. And so what happens is post facto, an executive notification is issued authorizing the inter services agency, which is the ISI. to conduct this surveillance. Now,

that was challenged as well, but what ended up happening is that the High Court order got challenged before the Supreme Court, and the Supreme Court essentially stayed and restored the surveillance regime, which was stayed previously by the High Court. So here we're also seeing how different courts, different judges are responding to things.

The ex BAN petitions have been pending for months now, and High Court orders are being violated. as well. We're also against the backdrop of the so called firewall. they've been able to disrupt certain functionalities. A signal was blocked. WhatsApp media dysfunction. so on mobile data, we're not able to transmit WhatsApp media unless there's a VPN on.

so what has enhanced capability do they have to be able to do this? VPN registration and blocking, on the other hand, is going on, whitelisting of IPs, which the businesses are asked, to go through and they are complying with because they've also faced issues. So that also is ongoing at the moment.

And of course we have regulations. So in terms of, even if it's not content data that they may have access to, metadata, as was mentioned, And it's willingly handed over, and then you have centralized systems where they're able to get all of that. So they want to know. where are messages originating, who is communicating with whom, even if it's not the data.

And on the other hand, in terms of getting to the data, we've had widespread raids, arrests, illegal detentions, search and seizures, despite the fact that the law requires a warrant, is not sought. People are then forced to provide passwords or access to their phones, and that's how the information has access and the content has access, so chats, who you're communicating with, drawing those links, building those cases, sometimes even anti terrorism laws are used in combination with, the cybercrime laws, and then all of this still gets admitted into evidence.

in the trials, and usually these trials are not necessarily always to get to a conviction, but as I keep saying, it's processed as punishment. Once you've been able to obtain access and coerce and do what you need to, then that's, essentially the objective is achieved. So this is essentially where we are at right now, where all of this is still, it continues to play out.

And now we feel that even the courts, we don't know what this new structure under the amendment, is going to hold for us.

Karthika Rajmohan - Internet Freedom Foundation: Thank you for that, Farieha a lot of very interesting points that I'd love to take forward. lastly, if we could have, Santosh Sigdel to please, give his opening statement.

Santosh Sigdel - Digital Rights Nepal: Thanks, Karthika. After listening to Dr. Sanjana, Vrinda, Shahzab, and Farieha, I can conclude that we have the similar trend across South Asia regarding regulating digital space, digital rights, the tactics of the government is similar also.

In Nepal, there are two fold of regulation. One is through the executive orders and executive actions and another is through the laws and policies. since last few years, the government has started proposing a number of policies that, they want to regulate the digital space. And in a bigger picture, it was also because of the, in the last election, there were new political parties and young, independent candidates.

They took over the old guards and in many of the, including the capital city, a metropolitan density of, capital. there was an, young guy who was able to got elected as a mayor. he was a rapper. so these people thought that social, it was all due to the social media. we cannot get hold of, we cannot be in the race.

We, if we cannot control social media. There was a kind of, a sentiment among the old, parties, old guards, and, in the executive front, there has been a number of instances where the government is trying to. Surveil, the communication, at the same time, keeping tab on the people. They have proposed this Media Device Management Service, MDMS, through the tail codes.

And at the same time, there is telecommunication, Traffic Monitoring and Fraud Control Mechanism, TeraMox. There was also procurement, this corruption charges during the procurement processes and there was a writ petition filed against this proposal in the court. And ultimately the issue went to the Parliamentary Committee and Parliamentary Committee has they have pulled the process for now, so that has been, the Teramox has not been, implemented.

And last year, the government, adopted National Cyber Security Policy. There are a number of, problematic provisions in the National Cyber Security Policy, including, then, provision of National Internet Gateway. So they want to establish a National Internet Gateway just like the, that proposed in Cambodia with where the, all the incoming traffic to the country has to go through the dedicated checkpoint of the government, dedicated network of the government and all the traffic going out of the country has also through there and they have access.

Over all the Internet traffic. that is in the policy. We don't know how they are going to implement it, but, after the push from the civil society and media, now they have renamed it as a kind of broadband management policy. now they are. The last government, they had a study which we filed.

Digital Rights Nepal had filed a right to information request to get a copy of that report, but that report was, has not been released. So they have constituted a study on this

broadband management policy where they want to, they do not want to talk it as a national interrogative any longer, but they want to disguise it in another technical name.

as you might know that, they want to, that the same, argument as Brinda and others have provided that social media companies, they are not registered in Nepal, so they adopted last year, they adopted social media guideline, which required the one. Social media company to get registered in Nepal within three months, and immediately after one week, the TikTok was banned in last November, and more than a dozen read applications were filed in the Supreme Court.

And eventually TikTok was also approaching the government. And the trend is similar. As I said earlier, TikTok was doing the diplomacy, this negotiation through the back door rather than challenging the decision. And it was civil society organizations and others who were challenging the decision.

Challenging that decision and eventually they agreed, they negotiated. And, civil society organization is still, because the details of the negotiation between the TikTok and the government is not very clear. So earlier TikTok had said that, they will provide a system to flag the content the government finds inappropriate and they will review those content.

So it, now we don't know what. Are the other kind of, the civil society, suspicious of other possible negotiation between the t TikTok, but it has been resumed in August, 2024. And, now the TikTok has started the process of registering in Nepal. So it is characteristic. And after that, they, after they blocked it for one year, now, they are back in the country and they have started this registration process.

the government has also proposed two new bills which have very problematic provisions. One is a social media use and regulation bill, which we, Digital Rights Nepal, had analyzed and last year we provided the input to the government, to the minister. And that is now in the, this legislative committee of the cabinet, and which is going to be presented in the parliament in the coming session, upcoming session.

And only there is cyber, this information technology and, cyber security bill. And we believe that made, many of the provision of the national cyber security policy will come through this. this, cybersecurity bill, there are many problematic provisions, regarding content takedown and providing many institutions the power to direct the social media companies to take down the content.

it, the power has been given to at least five agencies, so any of the agencies they find any content problematic, they have to, they can issue the order and if within 24 hours content is not taken down, they will be fined with, 10, 000. Up to 10 lakhs rupees, that is around 70, 000, I believe. So that is the, there are other many problematic provisions.

One major provision is intermediary accountability. So we have also analyzed that. So we are coordinating with other organizations to make some amendments, propose some amendments in this proposed bill, and we have been also working with a member of the parliament. Talking about the courts, as, shared by Sajab or others, the courts has minimal role, however, there has been some cases where it has played a very important role.

Earlier, in a few years back, a sitting justice of the Supreme Court was sordid, and at that time, the investigation agencies, they have collected more than half a million record of the court detail and, thousands of, social media. content, text, SMS text, and at that time, we had applied to the court, challenged the decision of the investigation agencies, and at that time, the Supreme Court, issued the direct, directive orders, to make laws to regulate that, process, and at the same time, required the judicial sanction.

the approval of the district court to collect any call detail from the, telcos. So that was how the court was, how the court was able to implement the right to privacy, a right to privacy enshrined in the constitution. And there are, a number of other cases also that is currently sub judice in the Supreme Court.

Which may, for example, there has been a case regarding this Teramox, its implication on the right to privacy. we are looking forward to the, this, outcome of this subjudice case is how the court will, uphold the right to privacy. these are the, some of the general scenario, last concluding point is, the government is also trying to, because now, in comparison to traditional legacy media, online media has been very robust and critical, so they have come up with this, online media guidelines.

And now the government has proposed a media council bill, which is, which will also, regulate the online media. So many of the issues that we have been discussing now that will also impact because, the social media platform of the media, mainstream media or the online media, that will also be subject to this social media bill, information technology bill.

And The impact will be on the press freedom also in the coming days. okay, that's it for now, as a general context.

Karthika Rajmohan - Internet Freedom Foundation: Thank you so much. A lot of very insightful points we've received from all of our speakers. Just to bring it all together, I think a sort of common And the other thread that we've noticed across all the speakers is that there are certain, a list of reasons that governments seem to be using to justify crackdowns on end-to-end encryption.

They're firstly, national security. Then secondly, maintaining public order, regulating hate speech and fake news. And lastly, it's facilitating sort of criminal investigations and combating child sexual abuse. firstly, I'd like to direct a question to Vrinda ma'am and Dr. Sanjana, just to tell us what are courts in your country doing when it comes to

balancing the need to have a safe space for women and children versus the right to privacy and the freedom of expression?

What are the sort of arguments that courts have been taking, what are the kind of balancing acts that debates have been surrounding? if you want to start, Vrinda, ma'am.

Vrinda Bhandari - Internet Freedom Foundation: Yeah. apologies, Dr. Sanjana. I just had to leave earlier, which is why, I've asked, to be able to speak first. so what actually, it's interesting that in many cases, what happens is when the court is concerned, and I think maybe this experience will be shared, I'd be interested to know that, For instance, when we talk about child rights, what often happens is it doesn't come up in a specific case, but it gets filed as what in India we call public interest litigation.

So it will be filed by, say, some child rights organization saying, look, we need, this is a serious problem, we need to do something. And what happens is because it gets filed as a PIL, a lot of the intermediaries don't get involved, right? So it's the court and the PIL petitioner. And so they, the court then doesn't really understand what the technical aspects are, what, what does it mean when you say, oh, all of you must give your data to the government at all times. So while they are well intentioned, I think what we see often, and like this has happened even recently, with the Supreme Court and another judgment, where they will issue guidelines to various intermediaries.

Which then become difficult to operationally comply with, right? But because they've never heard those concerns, that's one, issue. I've also just sent a link to a paper that I had the privilege of writing with Anya Kovacs, and we actually looked at how has the, how have courts in India, when they're looking at questions of gender, and sexuality.

Has it expanded digital rights or have they actually contracted digital rights? So we, I've shared this, on the chat and I think you can share it with the wider panel as well, with the wider, audience as well, but what we found is many times while well intentioned But to protect women or, to protect the morality of women especially when we deal with anything that's obscene, courts actually end up restricting digital rights.

And we view digital rights very broadly in terms of freedom of speech and expression, privacy, all of these things. so that's one thing. When it comes to national security, Unfortunately, in most cases, the government has, the court has a hands off approach. they may, on specific facts, it's very difficult, so there was a blocking case that came about in the Delhi High Court, where there was a software, that, they had challenged it, and it had been temporarily blocked in Jammu and Kashmir.

And the court said, oh, look, this is a very temporary blocking, it's for national security concerns, it's in Kashmir. And then almost it's untouchable, right? no court is going to go ahead and then actually challenge that. We saw that with Internet shutdowns as well, when it happened in Kashmir and we had challenged that in court and while we got a judgment, there was actually no specific implemented, like there was no judgment on

the orders as such, like on the actual facts of the case, it was more a judgment on how should Internet shutdowns be treated, so what we often unfortunately find is when it comes specifically to national security, it becomes very difficult. For the courts, to really exercise their powers of judicial review. They tend to have a more hands off approach. And what we have tried to argue all the time is just saying something is a national security issue should not be enough.

There has to be some basis, because otherwise it's impossible for you as a petitioner to, to show support. or to rebut that presumption or to say why it's disproportionate. so there have been, that's I think where we are facing a challenge. Having said that, I would like to recommend everybody to see, read the recent decision of the Bombay High Court, on another aspect of these IT rules, and maybe Karthika, you could share the link to the judgment, but where the court struck down on a two is to one.

it was, there was a first split verdict, went to a third judge and he ruled in favor of the petitioners. IFF had also assisted in that. And where they struck down the establishment of a fact check unit, which would look at fake, false, disparaging, information, vis a vis the government.

And so this was a government notified fact check unit and the court struck it down. so that was a really positive development, but I think by and large, this is how we dealt with it. I am really sorry I need to leave. I will just leave my contact details in case anybody, wants to get in touch with me.

I would love to do that.

Karthika Rajmohan - Internet Freedom Foundation: Thank you so much. A pleasure having you here. Dr. Sanjana, if you'd like to add.

Sanjana Hattotuwa - ICT4Peace Foundation: Yeah, so the only thing that I can add to that is that we aren't, as a country, as developed in our PIL and our courts have been under the jackboot of the executive just in the way that the constitutionally, the office of the executive president is constructed since 1977, which is when the current constitution was, was given birth.

The EP is untouchable. And whoever has occupied that office has gone on to encroach on rights in every manageable form and way. And the courts have been subject to that authority. That is almost godlike. when we talk about South Asian discourse today, and we talk about, for example, the, the Fiat of Modi.

We've had executive presidents like Raj Paksa since 2005 onwards completely trampling on the So PIL has been quite effective, but it has come at significant cost. Activists have been arrested, harmed, hurt, murdered, and extrajudicially killed. And so even to embark on PIL, particularly on NATSEC issues, is hugely, it's a big hurdle.

So it's not easy. And we have this kind of Kafkaesque scenario, which kind of is, alludes to what the former speaker said, where In order to find out what the NATSEC issue is, they don't reveal what the NATSEC issue is. So it becomes a bit of an absurd scenario where you don't know what you're supposed to be fighting against, but you're told to accept it on authority that it is a NATSEC issue.

The other thing that I wanted to point out, and I again, when I hear, India's examples, I feel quite sad. One of the things that the AG's department and the Supreme Court judged on with regards to the Online Safety Act that was passed in Parliament in a very unconstitutional manner as well, so even that's contested.

But the judgment itself was extraordinarily bad. And one of the, to put it simply, I think it's very clear when you read the judgment that the bench doesn't know, isn't aware of, and hasn't been told around what online harms constitute. So they're going with a very dated, outmoded, outdated understanding and notion of regulation, harms, media, and the information landscape.

And there doesn't seem to be any badness at the. Supreme Court, and the legal fraternity writ large around some of the, issues that we are talking about on this call, which is a Gordian Knot. they don't have, jurisprudence that's particularly clear, but even on that score, Sri Lanka's judiciary and the legal fraternity are not tied.

Up to date. And that's very clear in the judgment. So we have a lot to catch up in that regard, and that affords autocratic fear. So the net result of that is that our government and our executive presidents have a proclivity and a propensity and a culture of impunity, given that even PIL, pushback is so weak to do as they see fit in line with what others have spoken about in, in, in other countries, arbitrary regulation, arbitrary laws, extra constitutional or contra constitutional orders given to telcos, metadata at scale. And I'll end by saying that one of the things that we take as a frontier issue is the advent of generative AI. And what that will mean for state authorities in the harvesting at scale of what they do and then the subsequent targeting on an individual or institutional or issue specific way.

in ways that there is no legal jurisprudence, jurisprudence or regulatory framework currently contemplated in the country. So that's just not a frontier issue, that's actually a fundamental issue. I think that's a front door issue, given what we have seen in the country, but that's perhaps a different discussion, but in the simplest way I can say is that with respect to the answer that was given from India, we are at a far more embryonic stage, and I would argue as a consequence, we are more fragile and open to autocratic fear and abuse, as a consequence of, the, fragility, and the outbounded nature of our courts.

Karthika Rajmohan - Internet Freedom Foundation: Thank you so much for that, Dr. Sanjana. I know we are running out of time, but I would just love to quickly get Fareeha's take on this as well. Especially because we have been talking about national security,

that being a justification for erosion of end-to-end encryption. Brinda also mentioned, that it is tricky for courts to balance these interests.

Dr. Sanjana also mentioned that especially in times of fragility that these issues become even more heightened. And given that you had mentioned that Pakistan, given an election year, judicial appointments are happening in the way. How is Pakistan dealing with this debate between national security and any other possible challenges surrounding concern, concerns of privacy, freedom of speech and expression?

Farieha Aziz - Bolo Bhi: The problem is, as Dr. Farieha pointed out, unqualified claims of national security. And we expect that the courts assert themselves a little more and ask the executive to qualify what exactly is threatening national security in the context of the X ban. and they've blocked it. The ministers are using X via VPNs, which they are also blocking and registering.

Just see the hypocrisy of it all. And at least question why and for what purpose and what is it serving? so there's that aspect. And again, in terms of authorizing an intelligence agency post facto to then conduct mass surveillance, that also, what is the requirement? And on the flip side, because a lot of habeas corpus petitions for abductions of citizens are filed before high courts.

In those cases, the CDR is never provided. Somehow the safe city cameras never work. They can never trace the people who actually abducted. None of the existing system ever gets used, to actually trace the culprits. But on the flip side, and what, in addition to what is happening, is we also have. courts who have an antagonistic view of social media.

And so we had the present Chief Justice, saying that all of these vloggers who make dollars and are on payrolls, etc. And because there's been critique of, obviously, the Supreme Court and the judges and others as well. And on the other hand, we've gone through this judicial crisis where High Court judges actually wrote a letter to And came out and said that, the establishment is controlling, there were cameras found in judges bedrooms.

there was a lot that happened, and the Supreme Court and the Chief Justice basically looked the other way. And so within the courts, you also have some leaning in one direction and some in the other. But contempt proceedings, because then you have these proxy wars where those judges were slandered.

because they were taking on the institution and but then they went the contempt route as well saying oh now there has to be data scraping and who's trending these hashtags and where is this data personal data of judges being leaked and campaigns being run against them and including the mainstream media so there's a lot of friction within the judiciary as well and now with Dr.

Farieha mentioned the jackboots and that's all. We've had a checkered judicial history, but at the same time, here at the Executive, there's more entrenchment happening in terms of, you, you want a judiciary that is independent and that challenges the Executive when citizens go to court against the Executive.

You want, the courts to be able to deliver. However, when, where that happens, the judges are sidelined or, for example, the Islamabad High Court order, which was then stayed by the Supreme Court, and now they want to just reshuffle the judges and also the whole, within the judiciary. So at the moment, we don't know.

Also, the whole practice of devices just being, taken. People are abducted, arrested, their devices are taken. So there is no protection. Even a data protection bill, which is in the works, provides more access to government, facilitates more government access to data rather than protecting.

And so for me, always, the intent is in question. The narratives are the same. We have to protect citizens and protect women and children as well. Those protectionist, paternalistic narratives, but none of that actually happens. And under the garb of all of that and national security, the encroachment of the state is entrenched.

And that's essentially what we've seen through law, rulemaking within the judiciary, attitudinal issues. and at this point, honestly, even the gains somewhat that we have made, I, they stand, they may be reversed, given how now the courts are going to be restructured, whether the jurisprudence will still apply, are we going to start with a fresh, clean slate, and then who's going to head those constitutional benches.

which obviously we seem to think are going to be handpicked appointees who will block any kind of rights based, advocacy and litigation. And there are various, cases pending, but they're not getting anywhere. yeah.

Karthika Rajmohan - Internet Freedom Foundation: Wonderful. That was really interesting. wish we could go on for longer, but if we could now move on to the Q& A. Okay, I believe we are over time. we will have to close the panel there. I'm so sorry, Santosh and Shazeb. I did specifically want to ask you a couple of questions. I had noted down, but we are, running out of time. So I think we will have to close the session here. I want to take an opportunity to thank all of our wonderful panelists.

This was a great, very enriching, insightful discussion that we've had, and, it's been a pleasure to be on this discussion with you all. Thank you so much.