GLOBAL PARTNERS DIGITAL

WHAT WOULD ENCRYPTION-FRIENDLY PLATFORM REGULATION LOOK?

CROSS-REGIONAL PERSPECTIVES ON ONLINE PLATFORM REGULATION AND ENCRYPTION

MONDAY, OCTOBER 21ST 12:30 UTC

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

What would an encryption-friendly platform regulation look like? Cross-regional perspectives on online platform regulation and encryption

Maria Paz Canales - Global Partners Digital: Good Afternoon I am Maria Paz Canales. I am the Head of Legal Policy and Research and Global Partner Digital. And I have the pleasure, as my organization, as a member of the Global Encryption Coalition, to be your moderator today in this very relevant conversation that we have. Entitled as 'What will encryption friendly platform regulation look like? Cross-regional perspectives on online platform regulation and encryption'.

Setting a little bit the scene of this conversation that I was introducing with the title of the session, and that will be shared substantively by our wonderful speaker, but I want to share a few words on it. We live in an age where many more people have access to encryption than ever before.

Yet, we are also seeing a stark number of new proposals that will undermine it, threatening the privacy and security of digital communication, imputing the rights and welfare of particular individuals and groups at risk. At the same time, there are well recognized needs to better protect children from harm and to ensure accountability for abuses of companies.

However, in this complex context, a regulatory response Our responses to these issues must be nuanced and consultative respecting, and comply with principles of legality, necessity, proportionality, legitimacy, and non discrimination in our perspective as advocates for protection of encryption. This panel discussion intend to bring together this wonderful advocate that I'm going to introduce in a few minutes from the UK, Nigeria, Brazil, that have been working on the intersection of human rights and technology to share their experience and expertise in this engagement in national platform regulation discussion.

Through this discussion, what we hope is to change tactics and strategies for engaging in this discussion. And four regulatory responses which are proportionate and protective of encryption. Our aim with this session is to produce learnings and takeaways which can be useful to the community at large in what they need to advocate in different moments, in different geographies, in different jurisdictions.

I will move now to introduce my distinguished speaker. So we have today with us Adeboye Adegoke, who is Senior Manager for Paradigm Initiative from Nigeria. We have also with us Heloisa Massaro, who is Director of Internet Lab Brazil. And last but not least, we have Mark Johnson, who is Advocacy Manager at Big Brother Watch from the United Kingdom.

And we will start the first part of this discussion particularly with a deep dive of the advocacy in national online platform regulatory process. Each of these distinguished speakers will have around four minutes. We have four minutes to share a little bit of their introduction. And with no further ado, I will start with you, Mark, and asking you to share a little bit of your experience considering that the UK was one of the first countries to develop a dedicated online safety system, as opposed to utilizing existing laws for addressing some of the platform regulation concerns. Can you tell us about your engagement in the process to elaborate the Online Safety Act, which we are referring, and the The struggle defending their strong protection of encryption, how was the discussion framed and how did Big Brother Watch, and other Civil Society groups that coordinated for confronting this proposal respond to this criticism, particularly of the role of encryption.

Thank you very much for being here, Mark. The floor is yours.

Mark Johnson - Big Brother Watch: Thank you very much, Maria, and good afternoon if it is afternoon where you are.

Yeah, if you don't know Big Brother Watch, we are a civil liberties organization based in the UK. We have a particular interest in the intersection between human rights and technology and the title, obviously, of the discussion is what would encryption friendly platform regulation look like.

I don't want to be negative in my perspective, but unfortunately from my experience, I have a good example of what bad non encryption friendly platform regulation could look like with the UK's Online Safety Act. For those people who are not familiar with this Act it was a piece of legislation passed by our Parliament last year, and was a number of years in the making.

The idea of a UK Online Safety Act was first mooted in the kind of early 2010s, but basically the way that this form of regulation works is that it creates or appoints an independent regulator to set up codes of practice predominantly for large open social media sites. And these codes of practice dictate rules as to how they should moderate content on their sites.

The early iterations of the kind of blueprint of the bill did not talk about private messaging services. For the most part, private messaging services were exempt, and the idea of this regulation was to create a way of regulating content on the major platforms Meta, like X, and so on.

Of course, there were a number of freedom of expression considerations there, and we worked on the bill predominantly at the start from a free expression perspective, thinking about how content moderation and And rules around that could impact users right to free speech online. But while the bill was being developed, there was a simultaneous push from our Home Office Department here in the UK to insert provisions in the legislation regarding private messaging services and regarding, in particular, encrypted messaging services.

And ultimately, the final iteration of the bill included provisions which became colloquially known as technology notices. And in essence, these technology notices were a very subtle, very underscrutinized and quiet way of essentially mandating that platforms have to use technologies like client side scanning when it comes to tackling child abuse material on their sites.

This was despite the fact that in the UK, law enforcement bodies and other agencies have a raft of powers already to tackle That issue, which of course is a rights issue and should be taken extremely seriously, but there were a range of powers already available to many of our law enforcement bodies and agencies to tackle that.

And these powers were inserted notwithstanding as well the privacy, accuracy, and even compatibility of the technologies at hand or the lack of compatibility with users devices. And so this was, these provisions were added into the legislation without a great deal of scrutiny from a civil society perspective, we engaged with the process, but of course this was a vast bill that spoke about the regulation of various different parts of the Internet, predominantly open social media platforms, but also it took into consideration not just content moderation, but also age verification also other, various other provisions, including some new criminal offenses.

From a civil society perspective, we're incredibly stretched, given we were already focusing on for expression considerations and other issues with regard to the legislation. We did engage with the government at the time the government were not particularly willing to listen to us, unfortunately, and we put forward the arguments, both the rights arguments.

the problems of accuracy when it comes to technologies like client side scanning and also the basic kind of issues around how the processes would work. Unfortunately, despite our best efforts working with opposition parliamentarians we ultimately were not able to remove these powers from the bill, so they did come into law last year.

The good news from our side, I think, is that is that so far the regulator that the government have appointed Ofcom have taken quite a cautious approach, so the powers have not yet been used. And I think we, it's welcome that Ofcom have been very cautious. They are very alive to the to the rights considerations, the impact on privacy, and many of the issues at hand.

The difficulty is that we are very much at the mercy of Ofcom to take that approach. They can change their approach any time. They could become significantly more hands on. And the regulatory framework of the UK Online Safety Act is A framework that is open to political influence by the way that it is written.

So there is a chance that the government could apply pressure on Ofcom to use these powers to mandate an encrypted messaging platform like WhatsApp, like Signal, to scan all of the messages of all of the users on the site. And there are very few ways in which we could stop that. Of course, there is always the chance, and in fact, I think it's quite possible that these powers could be challenged in a court of law in the United Kingdom, and the Human Rights Organization, the Free Expression Organization, Index on Censorship, commissioned a legal opinion to say that it was likely that the powers would be unlawful.

In fact, the the opinion was written by Matthew Ryder, who actually said that Ofcom now have greater powers than GCHQ, our digital spying agency here in the UK as a result of the bill. It's welcome at the moment that Ofcom are cautious, the powers haven't been enacted. But there is a chance that there will be a legal challenge if they are ever used in the future.

From our side, it's a difficult picture because it's a bad precedent that we've set. It will have an impact on users around the world because if these powers are used, and if WhatsApp or Signal were forced to compromise the safety of their users By undermining N10 encryption, it would have an impact on people around the world too.

So there is a rights impact in other parts of the world, not just the United Kingdom. And it is unfortunately a bad example of regulation. But there are still opportunities for us to fight it. We're scrutinizing it as much as we can. And if the government ever do think about pressuring Ofcom, or if Ofcom ever think about using the powers then we'll be the first people to push back and try and stop them from ever being used.

Maria Paz Canales - Global Partners Digital: Thank you so much, Mark, for those perspectives, although, yeah, are less positive. positive that what we will want for this conversation but I think that there are relevant learnings there that feel positive in terms of a strategy and an opportunity for also collaborating with a organization working in other jurisdictions for showing what could be like the larger consequences of this type of a legislative approach in other places of the world and moving to that conversation and I would like to ask Boye to come in with some perspective about what has been your experience and Paradigm Initiative experience in engaging with the drafting process of the online health arms protection bill in Nigeria, how you have been participating in the consultative stage of this bill to shape this development and how the so much for joining us today, and we hope that this topic of encryption have come up and how also maybe you could connect with some of the experience shared by Mark and those, how those could be useful or not or different in the unfolding of the discussion in Nigeria.

To you, the floor is yours.

Adeboye Adegoke - Paradigm Initiative: All right. Thank you, Maria. I think a lot of what Mark said resonated with me as well. But I think the major difference is that online, the the, the online, the UK online safety bill and the online harms bill in Nigeria the online harms bill in Nigeria is still an ongoing process.

We don't have a law yet. As a matter of fact, we don't have a bill yet. All we have is. A whitepaper that kind of defines the direction that we go. Now, in terms of our experience engaging this, I think it builds on our years of work advocating for digital rights protection in Nigeria. So when the Nigerian government talked about we were just setting up a committee to advise it on what an online harms protection should look like for Nigeria.

They decided to invite us into the room, but they didn't just invite us. It was also because we're also trying to create a balance in the engagement by saying to us that you guys have been advocating for digital rights protection. You have all. Also proposed a law on digital rights and freedom in Nigeria.

So what they had proposed at the beginning was that they want to have a piece of legislation that addresses digital rights and online health. So the proposal at that time was to have a digital rights and online health protection, legislation. But we thought that was tricky for us, given that we, we know how this process has happened.

We didn't want. The two issues to be muddled up. We want Nigeria to have a legislation that speaks to digital rights and freedom, while it can also address the issue of online homes. in a separate legislation. So we, so we cancel that. It's okay. We are on this committee to ensure that there's digital protection in your effort to regulate online harms, but don't give it that name because once they give you that name, then it's going to be difficult for us.

So the way regulation, for example, when Mark was giving the UK experience, he did say something about how, the final product, they couldn't change certain things they would love to change. So we also know that our power. was limited in terms of being able to determine what's going to, what the final document is going to look like.

So we do want to create an end to our advocacy for a digital rights legislation in Nigeria by modeling a topic seeks to protect online hands, given that we already know certain challenges that might come up in that context. So We started to work as a member of the steering committee part of the initiative alongside many other organizations who are part of that committee.

Many of them are think tanks, many of them also, they also work in the tech and policy, spaces. Of course, The issues were clear in terms of what is of utmost importance to each of the stakeholders. For us, what we were keen on is to ensure that this does not become another excuse to violate rights.

As we have seen many times in this part of the world, whereby whether law addressing cybercrime became a tool of oppression, became a tool of suppressing the civic space or of targeting human rights defenders. So that has always been a priority. So that process This led to the release of a white paper on online hands protection in Nigeria.

And if you look at that white paper today, it doesn't look really bad when it comes to the question of encryption specifically. But that is because we started from, we started the conversation from digital rights protection. But like I said, It is still early in the game to, to celebrate because what we have is a white paper, the white paper, from the white paper we are going to have a bill, and also the bill will go through many processes, the politicians will have their look at it, the different government agencies will have their say on all of that, and a lot of things can still happen.

But one thing that we have been very consistent in doing is to monitor the process. Not just because we are a member of the steering committee, but also because we have always monitored the digital rights landscape in Nigeria generally, and we'll be the first to blow the whistle when something goes wrong.

So one of the things we have also done is that we have held what we like to call the Digital Policy Engagement Series with Broadcasting Society Group to let them know what is going on with that process, because this is not public yet. Not many people know that this process is ongoing.

I'm sure that people on this call will be wondering what something like this is going on in Nigeria. Of course, it wasn't in the public. But what we did was we had that digital policy engagement series where We let stakeholders know this is what's going on, especially from the civil society space, to say this is what's going on with the Nigerian government.

This is what we have been asked to do. This is how we have supported them so far. Also, the concerning provision of the draft white paper right now, we have also, raised some issues. Also, working with our partner, Global Partners Digital, look at that white paper together. We identified some issues and we communicated them and said that these are issues we would love to be addressed.

So far, so good. That process is still ongoing, as I said, but it's too early to celebrate and say, oh this white paper is good for encryption or it allows for encryption. Anything can always happen because there are competing interests. And just as Mark said the point about being left to the mercy of Ofcom is also a potential for holes in this part of the world as well.

There are, we have seen many laws around here where on the letter of the law doesn't even look concerning. But from experience, we know that in terms of implementation, what happens then depends on who implements the law. So we are very conscious of that perspective as well. And we are also trying to guide against that in what will be the final outcome of this process.

Thank you very much.

Maria Paz Canales - Global Partners Digital: Thank you, Boye. Definitely, I think that there are different challenges to overcoming this. Some of them are during the drafting process of this legislation, but for sure, as your remarks from Mark's remarks highlight, there is another stage of the process. concern in terms of the implementation and the interpretation of the authority powers for implementing these laws.

Going to a different flavor in the challenges of this discussion we will hear from Heloisa, and I will ask you to particularly tell us about Internet Lab experience engaging with the process of to develop Brazil Draft Bill 2630 what is the context of the deal and key concerns related to it particularly on encryption issues, and how did civil society mobilize to avert threats to freedom of expression and privacy that were coming in this discussion.

Thank you for being here, Heloisa, for your talk.

Heloisa Massaro - InternetLab: Thank you, Maria Paz. Hello, everyone. It's really a pleasure to be here speaking today. I think that in order to speak about specifically the issues that popped up during the discussions of the 2630 bill, it's important, I think, to highlight two different contexts.

That kind of shaped a little bit how messaging apps were approached by the bill on its first drafts. So the first one is that between 2015 2017, Brazil had a couple of cases involving the blockage of messaging apps specifically WhatsApp. And back then, the blockers were, the blocking orders came from proceedings, from criminal proceedings that we don't have a lot of details on it, but like the main issue involved with.

Judges wanting access or persecutors wanting access to the communications that were encrypted and WhatsApp would not be able to give the content of these communications and the judge would block the application, the app, until the order was fulfilled. So there was These key episodes involving encryption and a lot of this misconception about how messaging apps would work back then.

We need to remember that in 2015, we were, we could say, in the first years of using mass encrypted messaging apps back then, like spread the news. And this is the first thing. We have had already had this couple of issues with messaging apps. And it's important to highlight that Brazil, it's a have user of messaging apps.

We have around 99 percent of the Internet users use messaging apps on their daily lives. They use messaging apps every day. WhatsApp We have research that shows that 99 percent will use that WhatsApp every day in their life. So it's it's a really heavy use of the application and considering that we have around 85 percent of the population connected, it's really a lot of people using it.

So when we get, in 2018, in elections in Brazil, what happened is that we had some reports of bulk messaging on WhatsApp violating electoral law and 2018 was the year when Bolsonaro was elected and it was an election that was heavily characterized by disinformation spread and attacks in a really polarized context.

That was the scenario, and there was this huge concern that the key channel for disinformation, for polarization, was messaging apps, and was especially WhatsApp. So when we get in 2020 after a lot of issues regarding this information and discussions on fake news, etc, and then we are on the pandemic the, there is this bill, the 2630, that is proposed on the Congress under the name Fake News Bill.

And the first drafts were really worrisome. There was a lot of pressure from civil society. And then in the middle of 2020, One of the first drafts were approved on the CNA. Back then, the draft was mainly about transparency and some procedural issues, but there was a really controversial point on traceability.

What the rule was would basically say that every message that was I don't remember exactly the details, but it was something like every message that was forward for more than five groups and reached more than 1, 000 people in a certain period of time. The platform would need to keep the metadata of this forwarding action.

So the idea behind. was that if you could identify a violating message, you would be able, through this metadata, to go back to the first person who sent it. What were the goals? The main goal was to identify from where this information was coming from. And, but what were the issues with this?

This traceability rule is that, first of all, is that platforms, the apps would not be able to identify once one message is sent, what, on whether it will go viral or not. So in practice, They would need to keep the metadata of every message until this time period, at least until this time period was reached.

So to make sure that if this message went viral, they would have the metadata and it was a mandate for massive data retention, and there was a possibility of accessing this data on criminal procedure procedures. There was not a lot of. requirements for this access, so it was quite vague how you could access this data.

And in practice, you had a lot of risks, But the rule in itself was not really effective for its goal, because completely disconsidered the fact that sometimes people just download the content. Sometimes people, content travels through platforms. So maybe the content was on Telegram and someone copped and passed it there.

So you could not really access who was the first person. person who sent it and it created the risk of criminalizing the user at the end of the day. And there was, a great challenge within this rule that civil society in itself was Quite off split it, it was not unanimous that the opposition to the rule and to the bill in itself.

And back then, there was a lot of pressure from a group, a coalition of digital rights organizations from which we are part, on acting together to counter this, problematic rules within the bill. And we, together with a lot of organizations that are part of this digital rights coalition, we worked producing both knowledge and policy analysis and trying to dialogue with the rapporteur of the bill.

And this was a really important thing back then because the rapporteur back then was someone that is really open to dialogue with civil society. And we had produced back in 2021, 2020, 2021, a policy analysis on the issues involved in this type of rule. And at the end of the day, the, there was a lot of back and forth discussions with this bill, and it ended up not being approved, because mostly, not because of the, Privacy issues in itself, but mostly because of political tensions within the Congress.

And then in 2023, it came back as a platform regular regulation bill. So the same bill, the text was completely reformulated and it came like a platform regulation bill that was more GSA and this provision on traceability was taken off. The bill, but again, the bill was not approved one more time, also because of political issues.

And now we are under a scenario that we will probably have the Supreme Court deciding on the constitutionality of the intermediary liability rule in Brazil. And this We'll change a little bit how the liability is in Brazil and try to add some points for regulation of platforms. So this is our current scenario.

Thank you.

Maria Paz Canales - Global Partners Digital: Thank you so much, Heloisa. And I think that this is a perfect moment of transition maybe for a more hands on dialogue in the following section of this conversation in terms of thinking in the big picture that is provided by these three different examples of engagement in, in, in dealing with the encryption threats that happen in the context of platform regulation.

But also thinking about how this space provided by the work together in the Global Encryption Coalition and the opportunity of expanding the community also in this event today, around the Global Encryption Day, can be helpful in continuing this exchange of tactics for national engagement and engagement.

Thank you. Strategies for defending encryption and I want to make a couple of additional questions to speakers in this round, in this section, but also I encourage the audience to share their comments, their questions, their reaction, but really with this more strategic approach in mind so we can make the most of the outcome of this session in terms of takeaway.

And going to Mark first You already started to share a little bit as the, how, as the Online Safety Act turns to implementation and enforcement, there is all this expectation and possible tension in how authorities and particularly Ofcom will interpret the bill and how we interpret its own key responsibilities provided in the bill and what are the key messages that you will have for policy makers designing or implementing online safety regulation, considering this tension that you are you already started to highlight in the previous blog, and maybe you want to expand a little bit more, but thinking also in the intervention that have come after you from the other colleagues in other regions, how, what other things you consider that could be useful in terms of the Tactics and point, focal points of attention in dealing with this issue of the setting of the responsibilities of authorities and the things that can be done during the implementation period that you already are starting to experience by yourself in the Online Safety Act implementation.

Thank you, Mark.

Mark Johnson - Big Brother Watch: Yeah, so in terms of the next phases of the implementation of the Online Safety Act, we actually have had very good communication with Ofcom, the independent regulator, who have been quite good, I would say, in terms of speaking to civil society and listening to the concerns. I think that when the online safety bill, as it was before it became an act, was going through Parliament.

There the debates around it were not thorough because there was almost bipartisan consensus that we needed some kind of legislation. We disagreed with the model of the Online Safety Act because of all of the different rights considerations, whether it was free expression or privacy or other different ramifications of the legislation.

But there was quite a lot of support across both Houses of Parliament. So the debate was never as full as it should have been in Parliament. And there's some lessons that we can learn from that experience and how we can be better as advocates and try to, push for more of a debate. But I think Ofcom have taken an approach after the legislation has been passed, which is that they know that we raise concerns throughout the process, even if this debate was not as full and thorough as it should have been in Parliament.

And they have had an open ear and they have listened to us and consulted with us, which I think is very welcome. And also that they have had a cautionary approach because they know that some of the changes that the laws will bring in will be quite radical and really like reformulate how our relationship with social media platforms or messaging services could work in the future.

So they have been, they have engaged our. Plan from our organization, organizational perspective is to continue to monitor how the process works as vigilantly as we can and to continue to engage. Ofcom have run some open consultations. We have engaged in terms of what we could do collectively.

I found that having external voices as part of the debate is massively helpful because when we were engaging with the government and when we were engaging with. politicians, even opposition politicians, because the opposition in the Labour Party, obviously they are now in government, but all of this happened when it was the Conservatives in our government in the United Kingdom the opposition were not very strong on digital rights, the Labour Party were not strong on digital rights, and the difficult, the challenge that we had was that we had, with this legislation, All of the different issues in front of us, whether it was to do with free expression, whether it was to do with age verification, privacy implications, whether it was encryption.

And so we were spread very thinly. And there was also the challenge of the fact that both parties wanted something to happen in this space. So it was very difficult. And often we would approach the same politicians over and over again, and they would say, Oh, this is Big Brother, Watch back again. They always make the same arguments.

But if we did have external voices and we did towards the end of, towards the end of the bill, we managed to get more external voices into the room. It creates a broader picture. It creates kind of color to the arguments because we can say this is, we'll violate our rights of privacy and we can say this will have an impact on, journalists or human rights defenders in other jurisdictions around the world as well.

It doesn't really, it would be the same arguments that we're making, whereas if we could bring other voices from other jurisdictions, from other backgrounds we had one roundtable with other, another rights organization organized where we had amnesty were there. We had an LGBT organization various different groups and organizations that represented people to talk about, journalists or human rights defenders in different parts of the world.

Having other voices in the room was really helpful, so although the outcome of the legislation was not as positive as we would like, there, that what is helpful is that we can look back with reflection and say this is what we could have done more of in the future. This is what other people can do in the future if they have similar threats.

Obviously as I said, the good news is that Ofcom have not used these powers and they are being very cautious. So it's not a terrible story, but there is certainly plenty to be learned from a kind of like legislative experience, which was definitely less than, should be desired.

Maria Paz Canales - Global Partners Digital: Thank you, Mark.

I think that also we shouldn't be so hard in ourself. I think that at the end also, the final bottom line of the outcome maybe was not the one that you wish was, but definitely could be worse. You were not conducting all those efforts. So I think that also you and others working in this disturb, good credit because.

Possibly also the restraint in the implementation phase that you are seeing, it's also a result of that the authority is aware of that, how this creates tension and criticism during the discussion of the bill. So I think that, let's take that also that positive side in the outcome. And moving to Boye, back to Boye again, I think that you also were mentioning already in your previous intervention, this concept that Mark brought to us in terms of expanding the participation of having not the regular suspect, but additional groups of civil society coming in, but I am curious if you can say so much for joining us and I hope that you understand a little bit more, Boye, in terms of the things that you have seen in in, in how, for example, the context coming from other jurisdictions from previous experience has been useful or not in the discussion that you are having in Nigeria around the online, on the Internet.

And what can be learned from the experience of the advocates in Nigeria beyond this element that you already brought about the expanding the participation that also has commonality with what Mark was bringing on. So the floor is yours, Boye.

Adeboye Adegoke - Paradigm Initiative: All right. Thank you very much, Maria. It's interesting because I don't even think we'll be having this conversation in Nigeria if the UK Online Safety Act does not exist.

Not because the contemplation did not exist or would not always be there, but it's also about the reputation of using legislations. that seeks to address arms, whether in the digital spaces or in offline spaces, as a tool to suppress civic spaces. There has been very significant pushbacks from the civic, civil society, or even from citizens against government whenever it tries to introduce any legislation of that nature.

So it takes government being able to point to examples from countries that would typically be referred to as good examples for the Nigerian government to be able to comfortably say you can see this is what is going on elsewhere in the world. And that's also what is going on in places you would call fair or democratic society.

So it gives some sort of more validation for, even contemplating to do this in the first place. So that tells you that it's of very huge influence looking at what has happened in Australia and what happened in the United Kingdom. It influenced the government's decision to even be bold enough to come out without having too much pushback from the citizen, because the trust deficit is very low around here between the government and the people.

And so every time government contemplates certain types of legislation, the citizens tend to see from the negative perspective and all of that. But then when government is able to then point to examples of what is happening in the UK and Australia, which, An average person around here considers, sane society, so if it's happening in those jurisdictions, why can't we then have that conversation here?

So that is the extent to which it influenced the decision to go on this journey in Nigeria. However, beyond that, it also influences even the test, the content of the proposed legislation as well. Because what usually happens is that. The countries that come out with some of this legislation first becomes a template for others to use.

As we speak, you can, if you look at it, even with the white paper, references were made to the UK Online Safety Act. References were made to the Australian version as well, because this then stands as a template that we are using. And we're then trying to contextualize whatever we see on those templates into our reality as Nigerians and as Africans.

We, we are very aware and very conscious of the impact or the, how much what happens elsewhere impacts what happens in our part of the world. And, it would even interest you, I would even argue that even global processes but UN frameworks.

Like the GDC or UNESCO framework, for example, or platform regulation, they don't have as much impact as national frameworks from certain countries. On a lot of African countries, including Nigeria. These national laws that have been enacted, whether it's in the UK or in the eu or in the US or in the United States or wherever they have significance.

Influence the shape the approach. And as a matter of fact, let me also give you a very interesting narrative in Nigeria when we introduced the Digitalist and Freedom bill. And when we took the bill to the Parliament, one of the things we were asked is that the parliament will love to see warehouse.

This has been done, they would even love to probably go on a working study to, to see what is going on in that tradition. And at the time we drafted the dictator on Freedom Bill. There was no country that was having a similar conversation at the time. The closest thing to it at that time was the Marco Civil in Brazil which then creates a conversation around where our African governments approach legislation, especially digital regulation and legislation.

That is an assumption that you have to wait for the big brothers to, show the direction before you then make a decision. That is that reluctance to take a leadership role when it comes to defining the direction for regulation of digital platforms or technology in general. Thank you.

Maria Paz Canales - Global Partners Digital: Thank you, Boye. Yeah, definitely, that's a challenge. I think that everyone can relate, particularly in the global majority countries, of looking to good and bad models and continuing in that vein. Brazil has been a leader in a lot of things related to digital, as you just mentioned, the Marcos Civil.

So that is why it's so interesting having you here, Heloisa, talking about the experience. What are your takeaways in terms of the learnings about the pitfalls and opportunities of regulating online platforms, particularly linked to encryption discussion? And maybe I can do a provocation for a final round of comments a little later for each one of you as panelists, so not only for Heloisa, but for the three of you in your final remarks, I would like you to cover.

What will an encryption friendly approach look like in the context of online platform regulation according to this experience that you have had already in, in engaging with this issue. So a little bit about the lesson learned in the Brazilian process. And then if you want to go to cover this more overarching question that also will be great and I will give the floor later also to Mark and Voya for giving their take.

To you Heloisa, thank you.

Heloisa Massaro - InternetLab: Thank you Maria Paz. First I would say that we are, we have been learning things since 2020, so four years of learning with this deal that goes and comes back and takes a lot of different forms and approach. But, I would say that, first of all, one thing that has been really central to our work is to offer better and more nuanced diagnosis.

And I know this has limited impact at somehow, but it's really important to have this to bring to the conversation. And why I'm saying this, I'm saying this because when we're speaking about messaging apps, for instance we started to develop quantitative and qualitative research on how messaging apps use it in Brazil for political communication.

And one of our key takeaways is how message, WhatsApp mainly it's a really important platform and it connects other platforms, but it's not the only protagonist. Thank you very much. And also, we were able to show the variety of use that WhatsApp has, so when you implement a measure that you are looking to, I don't know, address some issue with this information that might be No specific question on a messaging app, you are really impacting small business.

You are really impacting the daily lives of people. And we have been trying to bring this to the dialogue for the past years. And this is one of the things that we have found really important and useful because it helps with policy analysis and we develop better approaches as well. The other thing, and it's that working in coalition during this process was really important.

The digital rights organizations have really worked together during the process of platform regulation, and this has really been important to create, this kind of, to try to address the disagreements between ourselves in this safe space before really going to advocate for another approach.

And this has been really important for this process. I would say that a lot of victories that civil society has had during this process was through this coalition work. And we could also take the best of each organization in this. We would have organizations like Internet Lab, who would be producing fact oriented research.

You would have organizations that would be more on the ground doing advocacy in the Congress. So this was really important. And a final You know, lesson that I would say from these positive things is dialogue with stakeholders. And when I say dialogue with stakeholders, it's like really listening and really taking into consideration what are the issues.

that stakeholders are trying to address or what are the challenges they are facing. And this goes both to private sector to really understand in deep what they are, what are the issues that have been appearing, but also working with legal professionals, for instance. So like really dialoguing with prosecutors, with judges, and developing like this type of.

listening capacity that really helps in this process as well. And as for challenges, I would add two things and then close. I would say that despite all these wins that we have had, we don't have a bill that was approved. So at the end of the day, you have the political disputes that overshadow everything and kind of supersedes all the work that has been done.

And the power of legacy media, especially in Brazil, it cannot be underrated. Legacy media was really important in this negotiation process and it was really one of the elements that blocked the bill. This is my I would say my final considerations, and as for Maria Paz's question on encryption friendly platform regulation, I don't have the answer, but I would add one thing that I think it's really important to bring into consideration, that it's, I think we need, it's really important to go deep on the distinction between social media and private messaging apps.

and understand that the regulation is different. And when I say this, I'm also including under conversation the issue that sometimes messaging apps become social media platforms and this also needs to be taken into consideration. Otherwise, we will have regulation that are aiming to attacking the social media features of the messaging apps and undermining privacy and freedom of speech.

That's it. Thank you, everyone.

Maria Paz Canales - Global Partners Digital: Thank you, Heloisa. So I think we are, as usual, we're running out of time with this very interesting discussion, but I am interested in hearing your take, Mark, and your take, Boye, in this question, how a good approach look like for you. Also, I am mindful there is an additional question that was posted in the chat that I also maybe I can try to stretch our time and ask you, include you in your answer, which is related of like more specific opportunities that you see in coming in the pipeline in terms of working together in any legislative proposals or related in terms of Implementation channels or challenges in the implementation of some of the pieces of legislation that you have been following or any other opportunities that you see in the horizon in which this more like global coalition work can be useful in terms of service of others that are starting to have this discussion.

So in the two questions, maybe. Very quickly, you can distribute your time as you wish. Mark, and then Boye, thank you.

Mark Johnson - Big Brother Watch: Yeah I'll try to be brief. Yeah, on the question about what goods regulation could look like, it's a very difficult question. We, when we approach the online safety bill we're very clear, we're not friends, not close friends or allies of social media platforms, that we recognize that there was a lot to do to hold these companies to account, but we didn't think that the Online Safety Act was necessarily the right approach.

We would prefer to see regulation that tackles the company's business models, that ends the kind of like mass data trade and thinks about, privacy and free expression as core to, central to any kind of regulation. I think. In terms of the specific challenges that, different jurisdictions try to tackle when they're thinking about, circumventing or undermining end-to-end encryption, it's normally something along the lines of terrorism content, child sexual abuse material, and perhaps disinformation as well as, we heard in kind of case of Brazil the principle has to remain that, that end-to-end encryption cannot be compromised and that any surveillance has to be based on reasonable suspicion, and should be targeted, and that entire platform should not be compromised.

I know that the, that many of the major Private messaging companies do collaborate very closely with law enforcement in jurisdictions around the world. There could be ways of formalizing some of those relationships without compromising entire channels and the privacy of those people who use those channels.

So that's a bit of a vague answer, but I think the most important thing, obviously, as everyone in the school knows, that there should be certain red lines that we should never be prepared to cross. In terms of opportunities for collaboration, it is possible that WhatsApp or Signal or other major end-to-end encrypted messaging services could easily turn around to UK regulators or the UK government and say we are happy to not comply with what you're doing. And in fact, both major platforms spoke about the possibility of either pulling out the market or certainly resisting the threats, the end-to-end encryption that were posed by the online safety legislation.

But there are bigger markets or bigger jurisdictions for those platforms that are considering regulation at the moment, like the kind of chat control consideration in the EU, and where you have 400 million or plus users there, it's much more difficult for those individual platforms to resist or to threaten to walk away.

So the likelihood that they would have to change their product or service in that case is significantly higher as opposed to a smaller example like the UK. So obviously we're, for colleagues in the EU obviously we're not in the EU anymore, but for colleagues who are in the EU, if it's useful and we can help, and I know that the conversations are still ongoing at the moment, I think we're in quite a good place, but but if there's anything that we can do and for colleagues around the world, then I imagine that would be quite important jurisdiction to to speak out and to help on.

Yeah.

Maria Paz Canales - Global Partners Digital: Thank you, Mark. Boye, your take in this encryption friendly approach to platform regulation, how would it look like?

Adeboye Adegoke - Paradigm Initiative: Yeah, I think that the debate for us within the the age long debate around privacy and security in terms of what an encryption friendly platform regulation can look like.

I do think that what's important is that we need to recognize the conflicting issues in terms of how, for example, compromising encryption can have significant impacts on privacy, users privacy rights, and you can also expose certain users to risk. But also we must also not, overlook the aspect of how encryption can also be misused by or can be a tool by bad actors.

I do think that what is important is the provision of safeguards that also ensure that authorities do not weaponize encryption to achieve political end. To use to use, weakening encryption to, to achieve political and weak encryption, to target certain individuals, probably because of their political beliefs religious beliefs or of or way of life, or whatever other distinguishing characteristics that they possess.

I do think that we are guided by the National Human Rights Instruments in terms of how we approach limitation to rights, such as human rights to be able to communicate, to have encrypted communications. I do think that limiting those rights has to follow very clear guidelines. The 3 Test Procedure, for example.

I don't believe that there should be a blanket power for authorities to be able to have backdoor access to encrypted communications, for example, which is In practical terms and in terms of the real life experiences of many people, which is usually the case, whereby, especially in countries where there are weak institutions, and I think that's going to be very relatable for most countries in the global south.

The lack of strong institutions has created a system whereby the authorities, Typically take advantage of this weak institution to go behind sometimes harassing social media companies or companies providing communication services, demanding access to, demanding backdoor access to communication without following procedure, without following the rule of law, without, any legitimate pieces and all of that.

So I think balancing would, what balancing will look like to me is creating a system that respects procedure, that respects the rule of law, that only accommodates legitimate concerns, either by security agencies or authorities, but not blanket access or blanket ban on encrypted communication. We have to limit how much power law enforcement have, how much power authorities have to to get to the back door of heavy conversation and heavy communication.

It has to be exceptional cases where this is required. It doesn't have to, it shouldn't be the norm. It shouldn't be the norm. That's basically what I'm saying. And in our work in Nigeria as well around the online exploitation, our argument has been around Creating strong safeguards, protection in terms of the principle contained in international human rights laws to guide government efforts in that regard.

I'm very conscious of time, so I'm going to put a stop to it there.

Maria Paz Canales - Global Partners Digital: Thank you so much, Boye, and you give me the perfect key way for the final takeaways Thank you very much to all of you for your perspective. I hope this can be useful in terms of action points for people following today's conversation.

And I will summarize that some of the key elements to take into consideration from your experience are this idea of enlarging the group. And I think it's important to have this kind of participation in order to have a broader community to taking care of this and understanding the nuances for different communities of the implication of impacting negatively the use of encryption, the idea of working in coalition for kind of shaping this discussion in a more safe space before going into other battles with the authority, the diversity of context and different uses and different actors here, not only thinking about the big tech, but also the diversity of implementation that this different app and the role that they play in society. The focus in the challenge, coming back to the last point of Boye, his closing remark, challenges, and I'm trying to focus on those challenges and government approach from a human rights perspective.

With this, I thank you very much, all of you, and I will be closing this session and inviting you to the next one in this very interesting Global Encryption Day Coalition Conference. Thank you.