



THE IGF IS A GLOBAL MULTISTAKEHOLDER PLATFORM THAT FACILITATES THE DISCUSSION OF PUBLIC POLICY ISSUES PERTAINING TO THE INTERNET

[ABOUT](#) ▾

[IGF 2018](#) ▾

[INTERSESSIONAL](#) ▾

[IGF INITIATIVES](#) ▾

[PUBLICATIONS & REPORTS](#) ▾

[CALENDAR](#)

[Home](#)

IGF 2017 - Day 2 - Room IX - WS178 Assessing Implications of Internet Shutdowns According to Internet Governance Principles

Engage with us:

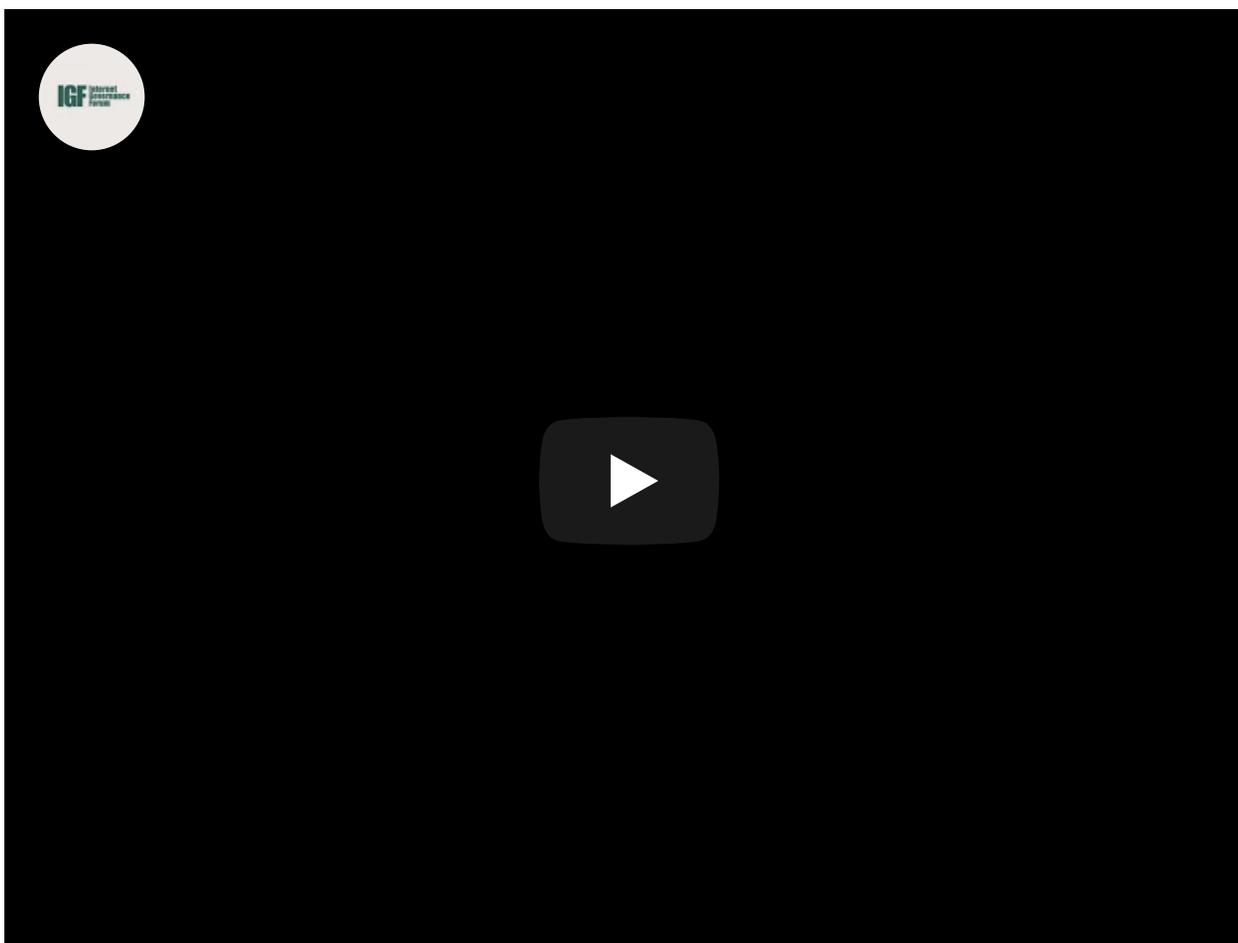


[My User Profile](#)

[Find/Become a Resource
Person](#)

[Subscribe to Our Mailing
Lists](#)

[Participate in Our
Meetings](#)



[· Get the Report of the Session HERE](#)

The following are the outputs of the real-time captioning taken during the Twelfth Annual Meeting of the Internet Governance Forum ([IGF](#)) in Geneva, Switzerland, from 17 to 21 December 2017. Although it is largely accurate, in some cases it may be incomplete or inaccurate due to inaudible

passages or transcription errors. It is posted as an aid to understanding the proceedings at the event, but should not be treated as an authoritative record.

>> THIAGO TAVARES: Ladies and gentlemen, welcome to the session, Assessing Implications of Internet Shutdowns According to Internet Governance Principles. This is the workshop number 178.

Our roundtable session, it is featured around three segments of 30 minutes each, and the discussion will be around three policy questions regarding Internet shutdown, website blocking, jurisdiction, international law and the multistakeholder community in coping with challenges in the next 10 years. I'm a board member of the Brazil Internet Steering Committee, CGI.br. Today I have the honor to comoderate this with my friend Paul Fehlinger, Director of the Civil Society, Internet and Jurisdiction Policy Network.

We have invited seven speakers and I'll invite you to them, Carlos Affonso on my right-side is the Director of Institute for Technology and Society of Rio De Janeiro, Brazil. He's a professor of private law at the Rio De Janeiro State University and affiliate Fellow of the Information Society Project.

Kyung-Sin Park is a professor at Korea University Law School. He's one of the founders and director of Open Net Korea, formerly one of the nine Commissioners of Korean Communication Status Commission and active director of the PSPT Law Center.

Also on my right side, I have Monica Rosina. She's a public policy manager at Facebook, Brazil. She holds a PhD in international law and is also a professor of law.

On my left, I have Neide Oliveira. She's a federal prosecutor in Brazil. She coordinated a task force on cybercrime at the Office of Federal Prosecutors in Rio De Janeiro and a project called Digital Location in schools. They are pieces of the same branch from the federal prosecutor's office in Brazil.

I have Peter Micek. He is a graduate from Vienna University, focused on shortcome in democracy and analyzing, and after studying

international relations for a year and since June, 2014 -- sorry -- he also taught Internet policy and progress.

I have Stephanie Felsberger. She has been working as a researcher focused on censorship.

And on my right I have Susan Chalmers, an Internet Policy Specialist at the Office of Human affairs in FTIA and focuses on Internet related Intellectual Property, trade and liability issues, tracking the Working Group on Cooperation and engages in the Internet Governance Forum.

To introduce the first round, I would give you a brief introduction and some food for thoughts, and afterwards invite our distinguished speakers on that.

First of all, an Internet shutdown is a disruption of Internet hindering unaccessible or effectively unusable for a reason or location, often to exert control over the flow of information. Internet shutdowns are interventions on the infrastructure level, and have been increasing in frequency in 2016 and 2017. The disruptions vary and include network of States and government blockers, usually motivated by national security or public safety concerns. It also leads to stability and to stop protesters and control elections.

Depending on the cause of the disruption, it may prevent the vast majority of people in a region from accessing a product, like YouTube in China as of March of 2009, or restrict access for certain segments of the population, like Google products in Kenya in February of 2012. The impact alone was estimated in 1.9 billion pounds. The huge impact on Human Rights and Freedom of Speech cannot be appreciated or accepted.

In application, website blocking is distinct from shutdown. This is used usually by governments to allow access to material, including International Security. However, a part of the issues related to child safety, there is a real international consensus on what constitutes appropriate content from a public policy perspective. Even in the case of child online protection, there is a better approach instead of blocking, directly remove the content or origin, the hosting content provider, and assist law enforcements with the metadata needed for prosecution of defenders, and support a national hotline which offers the public a way to report this in each country.

The multistakeholder international community convened a conference in 2014 in San Pablo reached consensus on a set of principles that should be considered as a baseline for our discussion today. Rights that people have offline must also be protected online. Those Rights include, and are not limited to, Freedom of Expression, of association, privacy, accessibility, Freedom of Information in access of information, developments diversity. People have right to keep the Internet as a unified and infragment spaces that should continue to be a globally interconnected, stable, fragmented, scalable and accessible networks based on a common set of unique identifiers and that allows data packets, information to flow freely end-to-end regardless of the lawful content.

I also would like to recall the Manila Principles as an example of Best Practice guidelines for meeting the liability for content to promote Freedom of Expression and innovation. And at the national level, the Brazil Internet Steering Committee has approved it by consensus in 2009 a set of it 10 principles for governance in use of Internets in Brazil. Those principles inspired the discussions and shaped the view of our Internet work. Four are directly related to our session today, and I would like to highlight them as an additional suggestion for our discussion.

Freedom, privacy, Human Rights, the use of Internet must be driven by the principles of Freedom of Expression, individual privacy and respect for Human Rights, recognize them as essential to preservation of fair and a democratic society.

Number two, neutrality of the network, filtering or trafficking must meet ethical criteria only, excluding any chrome factors or any other forms of discrimination or preferential treatment.

Number three, no liability of the network. All action taken against the activity on the network must be aimed to those directly responsible for such activities, and not at the means of access, this upholds the fundamental principles of freedom, privacy and the respect for Human Rights.

Number four, functionality, security, stability. The stability security and overall functionality of the network must be actively preserved to the adoption of technical measures that are consistent with international standards

and the adoption of Best Practice.

Having said that, I would like to invite our distinguished colleagues to address the first question proposed to this session:

With your experience in different countries, what are the impacts of international shutdowns and application blocking in local and global terms? Based on your experience, what would be some local issues important for this debate?

Perhaps we should start with Monica Rosina.

>> MONICA ROSINA: Thank you.

Thank you so much for having me on this panel. It is an honor to represent Facebook Brazil, and a pleasure to be among so many familiar faces. Thank you.

There have been several panels at [IGF](#) this year on Internet disruptions. If there is one consistent message across them, it is that Internet disruptions isolate people and communities, and because the Internet is one of the most powerful engines for economic growth, disruptions also affect the economy. Facebook's mission is to give people the power to build community, that's our new mission, and bring the world closer together. Over 2 billion people around the world are using Facebook on a regular basis across the globe, and that includes 122 million monthly active users in Brazil alone. At Facebook we strongly oppose shutdowns and any other disruptions of the Internet as a whole or of a subset of websites, apps and/or services.

Blocking specific apps and services risks fragmenting the free, open and global Internet and we're deeply concerned by the trend towards this approach in some countries around the globe. Disrupting access to the Internet or to apps and services like Facebook and WhatsApp separates people from their family and friends, chills free expression, harms stability because it interrupts normal economic and social activity, and it undermines economic activity and growth because it harms small and medium enterprises and disrupts the ecosystem. Even temporary disruptions of Internet services have tremendous negative economic and social consequences.

On a final note -- I know this is a larger panel than it was intended originally, and I'll just stick to my 2 minutes -- I would just like

to highlight a few numbers were mentioned on the economic impacts of blockings and shutdown. I would like to highlight that several studies recently looked at this issue and, you know, according to strict methodologies did the maths of the cost and the economic impacts of Internet disruptions and one of them is a study conducted by the Brookings Institution and it estimated that Internet disruptions costs countries at least 2.4 billion in one year alone and the estimated -- it was between July, 2015 and June, 2016. In this study, they identified 81 disruptions across 19 countries, and in Brazil alone the estimated cost of the WhatsApp blockings were as high as 320 million-dollars.

In addition to the Brookings Institute study, they have been looking at the cost of Internet disruptions. And in 2016 the Light Study released via the Global Internet Initiative says that disruptions cost countries 23 million per 10 million people per day in an illustrative high connectivity country. If you move to less connectivity countries that would follow 6 of.6 million per 10 million people per day. In some, we do not believe that the blocking of an entire platform is a proportion response, and it has an effect of imposing a collective punishment on all of the users of that platform and is not directly relevant to the harm that authorities are seeking to address.

Thank you.

>> THIAGO TAVARES: I'll go over to another Brazilian from the federal prosecutor's office.

>> NEIDE OLIVEIRA: Good afternoon. Thank you.

I will speak as prosecutor, as a prosecutor.

Rights to communication and Freedom of Expression, like all guarantees, guarantee that in the Constitution of the Brazilian Republic are not absolute and can be modified for the protection of other equally important rights and that are protected in investigations of serious crimes such as right to life and right to public security.

The WhatsApp application, for instance, the most used app in Brazil, which has been affected by judicial decisions to show the services in Brazil has brought contributions to the discussion regarding the fundamental Rights of freedom and communication. No doubt WhatsApp is available when applied to lawful activities, but

no one can use censorship when it is taken to prevent messages and used for a legal proposed such as pedophile activity, for example.

In Brazil, the six decisions that resulted in the suspension of WhatsApp do it to not deliver the encrypted content, but they do it due to the companies lack of explanation to the judge after the proper explanations were provided for. The decisions were reversed in an appeal. This clarification about the technical and possibility of complying with the legal determinations were given by the Internets of service provider after the Brazilian law by the application. In many cases, even the metadata which is not included in any other application was not delivered, making it impossible to start the investigation of serious crimes such as the planned murder of a public agent and other actions of criminal organizations. The measure is not disproportional either as it aims precisely to protect the other Rights. It must be measured in concrete terms on a case-by-case basis.

In Brazil, there was an exception period and due to the lack of clarifications by the application itself with its operation, however, after the federal prosecution servers gathered, the Brazilian public service published in 2016 a technical note distributed to all members of the prosecution services in the country clarifying that this was not the best measure. There has been no request for suspension of the application, and consequently, no legal decisions.

The Freedom of Expression cannot be an excuse for the practice of crime as stated by our Supreme Court. The Freedom of Expression and communication is limited by the Constitution along with other rights that must be respected such as right against child abuse, security, only to name a few. The violation of the social right of security, the violation of the principle of the dignity of the human person who is one of the foundations of the public of Brazil in accordance with our Constitution. We felt such a security, other fundamental rights would be in danger. Right to Freedom of Expression and communication does not prevail in face of other Constitutional Rights, among them, Right to freedom, to life, child protection among others.

The federal prosecution service does not deny that Freedom of Expression, it is a fundamental Right. On the contrary, it seeks to enforce the Article 13 of the American convention on Human Rights which recognized the need to

protect public safety. If on the one hand, rights of Freedom of Expression and communication is essential, they can and should be restricted when other rights need to be protected, precisely for this reason, the Internet framework in Brazil ensures the privacy of that to protect it being assessed by authorities without a court order. The legislation also established punishments for those who grant unauthorized access. In at least two situations in 2017 WhatsApp application was down. We found major incidents to look at the deprivation of rights of Freedom of Expression, people continuing to exchange information, news continues to be published and business continued to be performed normally. In this context, we have the following situation, WhatsApp is Indies, a good service, but it violates the Brazilian law, the suspension by its own failure despite its claim does not deprive anyone of any rights but their inability to comply to legal decisions puts at risk the safety of children and adolescents and the exercises of other rights despite this, the company says it can't be punished for the violations and therefore Articles 2 and 3 which had been inspired by the principles of Internet Governance published by the managing Committee of Internet in Brazil imposes the respect of all Human Rights for the users, citizenship as well as plurality and universally. The devices of the Internet certain framework form a coherent system ensuring the protection and also the means of appropriate sanctions in case of violation.

The sanctions abstractly in the norm understood within the framework are needed this disproportionate or unconstitutional as explainable, they are addressed to providers that while ensuring certain rights cannot violate others equally important and protected by the Constitution. The system of guarantees and penalties provided for in the Brazilian Civil Rights framework is not unconstitutional on its face because it must be tested as a balancing test. The framework preserves rights and issues legal means for compliance with its roles.

>> THIAGO TAVARES: Thank you for the statement.

We're strict on time.

I invite Professor Carlos Affonso who will present the Internet Society Technology Institute of Rio De Janeiro, one of the coorganizers of this session.

Please, Professor.

>> CARLOS DESOUZA: Thank you.

It is a pleasure for us to organize this workshop together with CGI.br. We have to say all of the heavy lifting of bringing everybody together is due to CGI.br. Thank you for the invitation.

A couple of quick points, and I'll focus on blocking.

A thing that's important for us to understand, that sometimes when we have application blocking, it is due to the behavior detecting of a third party of a user such to say and the platform and to tackle and to fight against illicit activities, they're done in the platform. It is important for us to differentiate between the work done by the person in the platform and the legal statutes of the platform on itself. Sometimes we end up mixing the two things, and it is important to understand that one thing is the user conduct in the platform, and the other thing, it is to portray the platform as a whole of being illegal, illicit and that will lead to blocking.

I will mention three quick documents that mention the issue of blocking. It is just to say that the discussion on app blocking or website blocking is definitely not new. If we go back to 2011 during the discussion around SOPA and others in the U.S. there was a whole discussion about blocking done through DNS. This is just one document for you to take a look on if you are interested in this discussion. There was this document called Security and Other Technical Concerns raised by DNS Requirements in the protected -- Protected IP View. It is a document that's altered by Steve Crocker and other researchers. They are very explicit against using DNS to block websites, saying DNS futures would not be vetted easily and would likely prove ineffective at reducing online infringements, further widespread would threaten the security and stability of the global DNS. This is one example from 2011, the discussion around SOPA and PIPA.

If we bring the discussion more recently to 2015 you have an interesting document from the Swiss Institute of Comparative Law saying -- I'm doing a quick translation here -- after the decision for the European Court of Justice in 2014 that allow the blocking of websites, there has been a lot of objections to this development at the European court. If you look especially on German law courts deciding against this type of

decision, claiming Human Rights, proportionately and doubts on the transfer of judicial power to third parties.

And in 2010 -- this is the third document I'll mention -- the U.K. had released a document called site blocking to reduce online copyright infringements and they play around with different types of blocking that could be made and they end up saying that DNS blocking would perhaps offer a simpler, less expensive option, but it is likely to be fully effective only until DNS is implemented, perhaps not a long-term solution, IP address blocking simply not regular enough, and the easy way it can be circumvented would suggest that it is not a suitable candidate.

This is just to say that the debate goes on from a long time, and if we look at the Brazilian perspective it is important for us to make sure that this discussion right now in Brazil, it is being brought to our Supreme Court because the Brazil Internet Bill of Rights that's been mentioned a lot here, in one of its Articles, it has the one provision that says it is possible for application provider to be sanctioned by the suspension, but it is not the suspension of the whole application provider, but only of the activities that are mentioned in Article 11 of the Brazilian Internet Bill of Rights deals with the collection of data.

When you hear about this situation saying the Brazilian Internet Bill of Rights allows for blocking of websites, our personal opinion is that that is not the case. It allows only the suspension of the collection of data that's the interpretation of Article 12. This issue is under dispute right now at the Brazilian Supreme Court. We expect a decision on that by next year. This is a subject that's now in our Supreme Court.

I would just finish by saying, of course, we had our situations of WhatsApp blocking in Brazil, the four times that the suspension ended up trying to be achieved, and maybe one simple fact that shows how complicated this discussion is, is that one of the WhatsApp blockings that we had in Brazil ended up taking WhatsApp out from some parts of Argentina and Chile as well. You can say oh, that was a mistake that it was done when the blocking was implemented, but mistake or not, I think it is important to understand how we're dealing with the infrastructure of the Internet and once we do this, we open up for situations like this one to happen. That's super complicated and those are the topics I would like

to raise here in the beginning.

I'll stop here.

Thank you.

>> THIAGO TAVARES: Thank you.

Now we have a frame of the Brazilian situation and we would like to invite Susan Chalmers to give you a more international perspective on that issue.

>> SUSAN CHALMERS: Thank you, kindly, Thiago.

Good afternoon. It is a pleasure to be here with you at the 12th IGF.

Today I would like to share some insights from a session at this year's IGF U.S.A. that NTIA helped to coorganize. The session was titled Healing Internet Fragmentation. For the purposes of the panel during this session our speakers stipulated to a three-part classification of fragmentation, that is technical fragmentation, commercial fragmentation, governmental fragmentation. So we had an excellent mix of speakers, one of whom shared his technical perspective. His remarks focused on and this is very relevant to what Carlos and Neide Oliveira was speaking too, his remark is focused on the impact of high-level political decisions on the Internet's infrastructure. For example, when governments will restrict the free flow of data across borders or forcing localization of data. What made sense from a geopolitical point of view to some, making sure that data stays in a country, for example, from a technical point of view often has big consequences. So these decisions can actually jeopardize the Internet's ability to self-heal and contribute to a loss of -- they contribute to the loss of the national resilience that exists in the physical, transport layers underneath.

So network operators really face a tough challenge because in practice, the implementation of these policies, they take place further down the stack at the packing forwarding level where simplicity is a key design, key design principle. What's the solution here? What we discussed during that panel was that we need to build capacity and understanding between the political level or the judicial level and the technical level. We need to develop translators so to speak to be able to convey very simply and

very practically the very real consequences of some of these decisions that are made. As we heard from our colleague from the federal prosecution service, it was the technical explanations that assisted in finding the best measure to effectively address the very real needs of law enforcement and also ensure that the application of any such measures, technical measures are not over broad and disproportionately impinge on the Human Rights of users.

Also as Carlos mentioned, the DNS paper came out -- that came out in the SOPA, PIPA discussion really illustrated the practical impact of the legal solutions that were proposed. As we go from policy, and as the policy is expressed through legislation, all of these need to be able to contemplate the technical impacts which ultimately can have Human Rights implications.

Thank you.

>> THIAGO TAVARES: Thank you very much, Susan.

Moving from U.S. to the Asia-Pacific region, we would like to invite Professor Park.

>> KYUNG-SIN PARK: I didn't know this session would start off with a showdown between Facebook and the prosecutor's office. I think I mentioned a bit about the current situation and give the Asia-Pacific perspective.

I think what happened with the WhatsApp in Brazil, it is not just a free speech issue but a privacy issue. It raises very important issues of whether the court can punish someone served with warrant for not carrying out production of certain confidential data. There had been discussion about what a warrant is, whether warrant is a permission for the prosecutor to access the information, or whether it is an affirmative order for private party to do something like production of confidential information. The theory is that warrant should not be an affirmative order. For instance, in the United States the court order could not force Apple to write a new software that allowed decrypting iPhone of a known terrorist. That terrorist was made possible because of the prevailing interpretation that a warrant is only a permission to the prosecutor, not an affirmative order on private parties. Coming back to Brazil, by shutting down the whole app for failure to produce information, the court was attempting to enforce an affirmative order on

Facebook which cut against the prevailing interpretation of the legal nature of a warrant.

I will use my last minute on the Asia-Pacific, more on Korea, and then I'll talk about other parts.

Korea has an initiative censorship party, the standard commission, which does comprehensive censorship of the Internet, some of which has affected, shutdown the entire website. For instance, NorthKoreatech.org, which is an information website ran by a British journalist on -- I must be saying something right, thank you -- on the information on the Information Technology used by North Koreans. Korea has national security law that punishes any speech condoning or praising North Korea and government position and using the law, using that law, the police requested shutting down of that website, and it is usually done through DNS blocking and the whole website was shutdown, although the website only mutually presented information about how much North Koreans used the Internet, how much mobile phone they used, we filed an initiative lawsuit against the decision, we canceled it, the cancellation was affirmed just a month ago. This was I think in surveying the world, this was the second time probably after a Turkish activist undid the blocking order on YouTube three, four years ago was the first time that people's right to access a full website was recognized and given back by judiciary.

>> THIAGO TAVARES: Thank you very much, Professor Parker.

The time is strict. I come back to Europe and give the floor to Stephanie, please, if you could speak in 3 minutes, we would appreciate it.

>> STEPHANIE FELSBERGER: I want to say thank you. I'm happy to be here.

I will talk a bit more about politics and not so much about laws, because I'm -- my background is in politics, not legal studies. I will speak about Egypt. I will talk about two major incidents of Internet shutdowns, one during the Egyptian revolution and another started in May 24th this year and is underway as we speak at the moment, analyzing the impact, both, and also seeing how they contribute to the general debate.

I'll try to be short. If you have any follow-up questions, just come up to me afterwards and I'll tell you the details.

So in 2011 in the middle of the protests against the regime and the president the Internet was shutdown. On the 25th, Twitter was blocked; 26th Facebook was blocked, SMS was shutdown; and on the 27th the Internet was blocked up completely. We have done research, our center, on how exactly this happened. There are different theories because access to this type of information is difficult to come by.

In 2017, now what's happening, it is that there is a number -- a large number of websites that's been blocked as of today, and the number is 465 websites which is a staggering amount of websites blocked. They're international news media, local news media, most critical voices of Egypt on websites were shutdown, ISBs, things like the way back machine, IP services like Skype have been blocked and this is an unprecedented move from the side of the government. Before what happened, it is a bit in line with the principles that were discussed before, but very -- applied very wrongly because before what happened was they wouldn't prosecute or put responsibility on the platforms or the news media themselves but on individuals where individual journalists or activists would be arrested.

Now there is a shift where entire platforms and news medias and websites are being completely blocked. When we look at the implications of basically the type of censorship that happened, it is interesting to see that somehow the effects of the -- the intended effects may have been a bit different.

In 2011 the block didn't necessarily stop the wave of protests happening, unfolding. On the opposite -- people had to go down on the streets and find out what was happening. In the end, the opposite of what was intended happened. I want to follow-up a bit on what was said about the economic cost of the shutdown, because there was a quite large economic loss that happened in Egypt because the Internet was shutdown four, five days and there are different numbers that are out there. There is an estimate of an economic loss of around 18 million U.S. dollars, totaling a minimum of 90 million during the five days of the outage. Other estimates are around 110 million overall. I think this is one point that I think might be an interesting aspect to add to the current debate.

To move -- aside from the focus on Rights and on the legal aspect of things, also look at the economic costs. Because from our perspective, that might also be a way to argue

and show that the impact is not just Freedom of Speech because some governments don't seem to be as receptive to those rights-based arguments, but economic arguments in our experience carry a different weight sadly.

A quick note on the 2017 blocking, the economic cost is not the same as 2011 obviously because only individual websites are effected, but the effect is an information blackout because all independent websites are blocked and the existing are very much in line with the official story of what's happening and it is very interesting to see that this is happening now because in Egypt people are used to a plurality of media available throughout 2000 because there were liberal economic policies, and the Internet was a rather open space but there is a shift that happened and it is interesting that people are aware of the censorship and the blocking going on and it is important to note when we think about Internet censorship and blocking that this type of blocking is very different from copyright take down notices that are not as obvious so that's something that's like this, so that at least this is easier to counter.

Thank you.

>> THIAGO TAVARES: Thank you very much.

I will give the floor to Peter from Access Now please.

>> PETER MICEK: I'm Peter Micek, general counsel from Access Now and I teach a class at Columbia University.

At Access Now, we have tracked the trend of Internet shutdowns across the world where we have a shutdown tracker finding the incidents rising according to our definitions and our coalition called #keepiton, a coalition of more than 150 organizations internationally. According to our research, shutdowns have increased from 56 incidents in 2016 to more than 77 this year and we do have Brazil's blocking of WhatsApp in the definition.

I wanted to take it back to the principles of Internet Governance, we started the session with -- I think it is clear that a multistakeholder processes and the idea that all those effected by a decision ought to have a voice in making that decision are key to building the Internet as we know it and the horizontal organizations that we currently depend on to organize it. These decisions to shutdown the

Internet are clearly unilateral decisions that do not consult with affected stakeholders and are not made through transparent or democratic and inclusive processes. We actually know very little about how the decisions are made, who makes them, we see the impacts and we can guess at attribution, but there have been -- it has been rare that courts or legislators have honestly and openly robustly debated who should have the power to deny us access to the Internet, when and under what circumstances.

These shutdowns are a form of discrimination likewise, they violate its principles of neutrality and are targeted at specific applications, services and communities. As far as stability, we heard a bit about how Internet shutdowns and other types of blocking can damage the infrastructure itself, leaving lasting damage in addition to the acute harm to networks. I would add that if we're talking about stability on the Internet as a principle of Internet Governance we should ask what is the purpose? Stability for peace and stability sake? I think it is for dependence on a network that can build trust and ultimately growth and all of these values are offended when the Internet is shut off at will.

Then finally, to Human Rights, I think we have heard a bit about the impacts of Freedom of Expression, as well as on the economy and the Economic, Social, Cultural Rights.

I would add that we have recorded at Access Now, shutdowns that directly impact right to life. We have two incidents where women were unable to contact their doctors and lost their unborn children during complications with their pregnancies. These are incidents that we have recorded. We have to assume that there are more that we know of and have to assume that other people were unable to access emergency medical services because the networks they depend on were suddenly and momentarily deprived.

I'm very hopeful, even though we have seen some trouble with the courts approaching this issue that more judges will see a more robust determination of what's proportional when it comes to blocking the Internet. I think the proportionately test is true, but I think the factors, the way that Internet impacts our daily lives are not well understood, they're not economically quantified in such a way that judges can make these determinations readily. And as I said, there are effects of shutting down services. I would call on just as the United

Nations in the safety of journalists' resolution at the General Assembly this month has done, I would call on more organizations to condemn disruptions unequivocally as violations of Human Rights in the digital age for telecom companies to continue to push back, being transparent about the orders they receive and for more Civil Society and more support for the keep it on network calling out the problem.

Thank you.

>> THIAGO TAVARES: Thank you very much, Peter.

This brings us to the second part of this discussion. I think those were interesting comments by the panelists addressing the plethora of issues we're addressing here. I would say that all of the different issues that you heard here can be perceived as systems of a broader illness, it is a challenge of all, everybody faces this alike, and it is how national laws are applied on the cross-border Internet. I don't need to explain to anyone in the room that most online interactions involve multiple jurisdictions at once and this brings a lot of new challenges. The questions especially if we talk about shutdowns, what level, with what tools and what procedures are national laws applied in the cross-border Internet. I want to take the opportunity now as I briefly have the microphone to provide some elements of clarification. I think that shutdowns are a fairly new phenomenon and it is very important that we all use the same vernacular and don't confuse the terms when we talk about shutdowns and how national laws are enforced on the Internet. When we talk about shutdowns, I believe we talk about what was said about infrastructure shutdowns, they can be just part of the Internet, entire Internet, fully national or in regions. This is certainly the most extreme way for a government to control the Internet by shutting it down so it is not accessibility more. As the panelists mentioned, there is severe consequences for Human Rights and the economy. However, shutdowns can also have cross-border affects, averse, unintended cross-border affects. I want to highlight Egypt. It was interesting to see that while the Internet was shutdown the cross-border transit traffic was not touched but you can have incidence in theory where the Internet is shutdown and the services with the data centers in the country are unaccessible for users worldwide.

The other issue that was mentioned, and this

is the case for instance for the WhatsApp case in Brazil, it is the ordering of ISPs to block certain websites or applications, again websites and applications, this is not the same thing, this can be done through DNS or IP blocking, the technicalities vary and the reason why things are blocked vary and it is important to keep this in mind, the case of WhatsApp in Brazil, this is an issue of cross-border access to user data. The reason why, WhatsApp was made unaccessible in the Brazilian jurisdiction is because WhatsApp did not comply with an order to produce data that was requested by Brazil. You can have other incidents where the issues is cross-border content removable or issues or instances where courts or other public authorities try to make content unavailable in a given country.

I think it is very important to keep this in mind when we discuss those issues and there is even a third area that no one touched upon here, that's part of the larger picture, it is domain suspensions to registrars or registries, it is a technical thing but applying national laws that can have severe cross-border affects but the challenge we have in this room today, it can advance on how to build a bigger common understanding of the challenges that we collectively face with regard to shutdowns. What is the way forward? We want to look at the next ten years, this is a new phenomenon and it is a great place to grasp this phenomenon, it is to see other emerging principles, procedures or standards with regards to Internet shutdowns and I would like to give the opportunity to the people here in the room which are all knowledgeable in this topic to open the floor and to ask you, looking at the different incidents of Internet shutdowns, do you see emerging patterns in terms of principles, procedures, standards? What is your view on this? Maybe we can collect 2, 3 comments from the floor in that regard.

Who would like to go first?

>> AUDIENCE: I'm from Brazil.

I have a question. I understand the need for public security and respect to jurisdiction and sovereignty, but I would like to know what are the criterias you use to evaluate the limits between what concerns public security and what is surveillance and who establishes the criteria?

>> THIAGO TAVARES: Maybe would you like to

--

>> If you don't mind, I'm a colleague of

Neide, I'm the federal prosecutor also, thank you for the explanation, I wanted to put out here some things about the panel.

First of all, what we need to understand, it is that the block -- I would like to say block instead of shutdown and suspension of services and when we have this, it is because someone or a company disobeyed some orders in Brazil. We work with very severe crimes. We're talking about crimes, investigation and procedures in criminalities. We're talking about child pornography, we're talking about rapists that endangers the Internet. When we talk about the panel, it is not just like very well mentioned by Carlos, it is not just in the Civil Internet, the Civil framework in Brazil. We have the procedure code that gives the power for the judge under circumstances under the law to give this panel.

Another thing, if I can just complete it very quick, it is because we are from the federal prosecution office, we enforce it that this can just be used or just has to be used with a lot of option and as a last resource. Why? When you do this, when you have a penalty, you want to penalize not the users, not the consumer, you want to penalize the company that's not contributing with the investigation. Really to finish, we're talking about as very well said about Monica about the economic impact. I want you to think a little bit, as we have seen in our daily work, how much you would pay, a mother would pay, to have some information that could give her -- succeed in an investigation to take out his son or daughter from a rape going on from the Internet. We can't start an investigation like this with metadata and things like that, we try to get it, when we don't get it, we try to solve with financial penalties, not blocks. We don't want to block anything. It comes as a response and it comes in the last resorts.

Thank you.

>> THIAGO TAVARES: There was another question.

>> AUDIENCE: I'm from Brazil. I'm a Fellow.

My question is to Monica. You are here as a face group representative, but when law enforcements go to Facebook offices to talk about WhatsApp, you say you're not related. How does the company separation work, you're here as public policy, you can speak on behalf of WhatsApp, but when it is law enforcement from our requests, you can't. How does it work?

>> MONICA ROSINA: That's a great question. I'm not here as a representative of WhatsApp, I'm a public policy manager for Facebook, Brazil and WhatsApp is part of the Facebook group of companies. Whenever there are requests from law enforcement, those requests are directed to the WhatsApp office in California and the WhatsApp application team, to my knowledge, responds to those requests.

>> THIAGO TAVARES: Thank you very much.

There is another question over there, please.

>> AUDIENCE: I had some comments on of the trends I'm seeing in India with respect to shutdowns. The last few days there was a shutdown and we have had about 72 shutdowns this year alone, more than double of what they were last year.

The other thing, we have had in one particular state, a small state, there was 100 days of shutdowns, a continuous 100 days and we have had incidents in a state where across 6 months there is repeated shutdowns, what it does to people, it makes them lose faith in having Internet access and we have heard that directly from people who faced shutdowns as well as from dealing with the shutdown that's happened.

The impact it has on people, for example, students who are going to study, all admission forms are online, they can't file for their admission. The states I mentioned, they're tourism-heavy states, and operators and tourism companies have lost money because they couldn't take bookings. Journalists who were reporting on the situation on the ground have had to file stories using SMS because of no Internet. There were people, businesses unable to file the taxes, all tax filings is online.

There is a disproportionate impact it has on people's lives. What we're seeing, which is even more worrying over the last year especially is that there is now preemptive shutdowns where there is an assumption that there is some situation that will spark, for example, the results of a court case earlier this year and the Internet is shutdown on a preemptive basis expecting social strife. What we're hearing from people is that the first step that they take is to shutdown the Internet because they're worried about rumors. That's administration. One thing we hear from the people on the ground, the one thing we keep hearing from them, the rumors

spread person to person and they're not able to validate any information because they don't have access to the Internet. I think my worry is that even though there was a rule passed in India earlier this year, and that seemed to have a stronger process for shutdown with checks and balances in place, we have seen the number of shutdowns increase given the checks and balances and given next year is an election year, nine states going into elections, we're seeing social strife as an outcome of hectic political activity leading up to elections, we're expecting shutdowns to increase next year. That's very worrying.

>> THIAGO TAVARES: Can you state your name and what organization?

>> I'm Nico Powel with the Internet freedom foundation in India.

>> THIAGO TAVARES: Are there other questions in the room?

>> AUDIENCE: Good afternoon, everybody. Very interesting insights coming through from the panel.

I would like to point out something else -- I'm Juliette. I work with a collaboration for international ICT policy.

Going back to what's discussed, we seem to focus a bit on the people who are already online. Some research that we have also done on Internet shutdowns has shown us that people that are not on the net, not actively using the Internet, also affected by shutdowns. When we look particularly at cases where mobile money is effected -- and we recently produced a report on the economic impact of shutdowns and previous reports -- we have not fully looked at that the aspect of Internet shutdowns but we found those offline were equally effected by the Internet disruptions. When we look at it from the services, service payments unable to be conducted, Peter mentioned the case of -- what was it -- right to life. In many instances, basic services rely on mobile money payments, but we're at a point where we have no idea what impacts some of the shutdowns have had on people who are very reliant on mobile money, what impact the Internet shutdowns have had on them in cases of rural communities where doctors cannot serve the patient if they don't have the capacity to make a payment, the child won't be allowed in the classroom without making the payments. We have to look at this with a wider lens with those that

are not directly using the Internet-based services and consider those that are relying on related applications that are also affected by the Internet shutdowns.

>> THIAGO TAVARES: Thank you for the comments.

Over there, please.

>> AUDIENCE: Thank you. First of all, thank you for your presentations. I'm Patricia from Yale Law School. I have a question.

When you present your definition of what an Internet shutdown is, you said that it is justified on the circumstances national security and public practice. I would like to ask you more or less, if it is your definition, how did you elaborate it? It came from the analysis of the specific cases like maybe Brazil or Egypt, but the practice and debate of shutting down the Internet has been for a while already and has been discussed in well consolidated democracies, the reasons why they want to do it cover a lot more than the public protest. I would like to ask you how much do you know about the cases and whether they will make you reconsider your definition of what an Internet shutdown is.

>> Thank you for the question. It is not quite mine, but I try to resume what the main reports in the areas are at, for example, international society has a fantastic report on that, they use that definition, some companies like Google has a shutdown on data transparency report, it they use it, some of the roles to define what shutdown it, so it is a well-accepted, I assume, definition by the broader multistakeholder in communities. That's why I included on my statement just for introduction to give you food for thoughts.

That's it.

>> THIAGO TAVARES: Thank you very much for the question and the answer.

Are there other comments or questions in the room? Yes, you would like to follow-up on the initial question that you asked?

>> AUDIENCE: So my question -- I'm Jiviana, I'm here with Youth.

My question is for everybody, but it is a follow-up from her question actually.

Okay. We have this -- we have to

investigate some crimes, that's something that we all agree here I think. I cannot see how the investigation that's a punctual thing can be a punishment for the whole society. However, we must investigate. So my question is, you mentioned our law, the certain code and everything, but blocking everything or shutting down everything violate the Human Rights conventions and Marco Civil, another law. By one way or another, we're violating laws and conventions.

My question is, what is the solution? Shutting down is bad for everybody. Not shutting down is bad for these cases.

As mentioned, there is the how much would a mother pay for removing the pictures of the son, how much the mother who lost the baby would pay to have the baby. I want to see something that would not prejudice one or another or some kind of a middle way. That's my question.

Thank you.

>> THIAGO TAVARES: I think this is a very good question. I imagine everybody on the panel has an answer on this.

Who would like to shoot first? Volunteers.

>> How much time we don't have!

>> THIAGO TAVARES: Maybe a few quick comments then. I imagine that everybody has -- Peter, would you like to start?

>> PETER MICEK: Sure. That's a great question.

We can talk about having a better society where people don't permit crimes, I don't think that's within the purview of this panel.

I think if we're talking about law enforcement, access to data, law enforcement, stopping, preventing crimes and finding those responsible, although the explosion of the information, there is data and information that's previously possible, and I think it is -- we center on the few cases where things may be dark, where an encryption may protect the content of communications, we do maintain that there are many, many other tools at the disposal of law enforcement and tools and tricks and training and legal powers to access the data to surveil lawfully and, yeah, I would love to hear more from the panelists.

Thank you.

>> THIAGO TAVARES: Thank you very much.
Monica, please.

>> MONICA ROSINA: Thank you.

I would like to highlight that Facebook has been working with law enforcement, providing metadata whenever it is requested and content whenever it relates to child exploitation or emergency requests through a very fast process and through the international Cooperation Treaties, when that content is required.

We have seen that metadata has a lot of value in criminal investigations and it is usually used around the world as access to content as a last resource so that criminal investigations. This year alone, we have had a lot of successful stories of working with law enforcement in which the data that we were able to provide was very helpful to the successful outcome of that specific investigation. We are eager to continue to work in partnership with the law enforcement and with other key stakeholders and issues.

>> THIAGO TAVARES: Please.

>> I would like to say that is the difference between Facebook and WhatsApp. The problem with WhatsApp was that they didn't answer the judge, minimum of answers to explain the kind of cryptation that they use and to give the answer of content from the judge. Sometimes, they didn't answer the metadata too. We have a lot of tools as Peter said, to work investigations, but sometimes to initiate the investigation, we need the metadata, it is essential.

We think the answer of this problem, it is that we need the providers to help us, work with us and to help us how to do best our work together. As Monica said to Facebook too.

>> PANELIST: Can I add something?

Very quick, I think my answer for your question is cooperation. Cooperation: We talk a lot about international cooperation. This cooperation must start inside our countries. We must cooperate. Multistakeholder -- it is an overused word, but we must really use it. We must go hand-in-hand, walking together, with this we don't need to reach the panels.

Thank you.

>> PAUL FEHLINGER: Thank you.

The essence of the question was concretely what can be done. The current situation is unsatisfactory for all categories of stakeholders right now, everybody is looking actively for solutions to how to make it work, how can we look at the cross-border of the Internet and international laws in a way that works.

I take this opportunity to shamelessly say that the Internet & Jurisdiction Policy Network is a global multistakeholder policy network working on the issues. They're the second global Internet & Jurisdiction conference that we organized in Ottawa in partnership with the Government of Canada at the end of February. I won't elaborate on the activities, but all of the issues that are discussed here, they're actively addressed in the ongoing policy process, and we have a session on Thursday at 9:00 in this room actually if you're interested.

We're entering the last 10 minutes. I would like to stay on the speed of what concretely can be done. Remember, the purpose of this session was to look ahead, to say in the next decade, what are things that need to be solved. I would maybe like to take the opportunity starting with you to ask a last question of the panelists. If there is one thing that you think the multistakeholder community should address with regard to shutdowns and maybe let's focus on the issue of shutdowns and not only on the issue of blocking that's been more discussed than the issue of shutdowns by the international community so far, but what is the main policy question that you would like to see addressed by the multistakeholder community staying on the speed of what can be done concretely?

>> There are two principles that multistakeholders can and should agree on.

Number one, executive branch itself, should not take down or shutdown the Internet or even individual posting. Freedom of Speech should not be by the administrative initiative because speech by definition is interactive because the consequence of the speech depends a lot on how it is received by the listeners, the hearers, the receivers of the information.

The second principle is the principle of personality. Some of the shutdown is issued by the independent judiciary of the country, but

Internet is not content. Internet is a place. Yes, some postings, some illegal posting may be up there on one day. Some other posting can come up on that same space. Now, the only way to shutdown the Internet or a part of the Internet or website is to risk preventing posting of all those other postings, lawful postings that could come up in the same place. Understanding that Internet as space, not content is something that we can try to agree on.

>> THIAGO TAVARES: Thank you very much.

What's your policy question?

>> STEPHANIE FELSBERGER: It is maybe not so much a policy question. I have an anecdote, and a follow-up from that.

In Iraq, for example, the Internet has been shutdown to prevent cheating on exams for 11-year-olds, and that's happened multiple times. I think the question on when -- I don't want to say that the Internet should be shutdown, but I think more research should be done on how and to what extent shutdowns are harmful to people. I think there is a more better understanding of the harms that do occur when the Internet is being shutdown. Maybe principles and standards in terms of if you shut it down, how can you mitigate certain things if you want to do a targeted prevention of certain things which I'm not sure I would -- yeah. I don't know -- to kind of mitigate the harms, not to say that you agree with the principle in the first place, yeah, maybe something like that.

>> THIAGO TAVARES: Basically if it is done, how should it be done.

>> STEPHANIE FELSBERGER: How can you mitigate the fallouts from -- if you have a specific goal you want to prevent with the shutdowns and maybe an Internet shutdown but it is kind of giving governments a toolbox to prevent Freedom of Speech which is also not a good place to start.

If we're in a place -- the problem, I come from a background of Egypt where politics is not a place where you can go and give policy advice and the government listens to you, it's a place where you kind of mitigate the harm. Yeah. That's my point.

>> THIAGO TAVARES: What's your policy question?

>> NEIDE OLIVEIRA: (Off microphone).

>> THIAGO TAVARES: On the microphone.

>> NEIDE OLIVEIRA: I would like to summarize our speech as said, that we -- law enforcement agents and providers, we must work together towards more appropriate solution for the protection of the users and of the investigations.

>> THIAGO TAVARES: Thank you very much. Susan, your policy question.

>> SUSAN CHALMERS: I think the question I would ask is what can the multistakeholder approach do to help solve this problem. So practically earlier I described the practical need of conveying technical ramifications of political decisions to decision makers. Supporting the very bright young minds that are entering the space with technical backgrounds to be able to convey those ramifications clearly and concisely. I wanted to mention the work of the Freedom Online Coalition, very, very briefly, because that's because we're working towards building solutions here. That's a coalition of 30-like-minded countries and the goal of the coalition is to serve as a coordinating body that advances across multistakeholder engagement to protect and promote Human Rights online.

While the Freedom Online Coalition is governments and it takes a multistakeholder approach and practically and there is a call for expression of interests to be a part of the advisory network that's open until January 11, if you're from Civil Society, Technical Community, private sector, please take a look at that call so you can be a part of developing the solution.

>> THIAGO TAVARES: Thank you very much.

Monica, what would be your policy question on those issues?

>> MONICA ROSINA: I'm going to take the liberty of going back to blockings, that's the Brazilian reality.

The last point I would like to make, there are currently several proposals on the table that would make the blocking of certain apps illegal in Brazil. My policy question to that sense is how can we as a multistakeholder group, what can we do to address that and make sure that doesn't happen.

>> THIAGO TAVARES: Thank you very much.

>> CARLOS AFFONSO: I'll be super brief, just mentioning that even though it is true that the Internet shutdown is not a reality in Brazil, since we're asking more broadly policy questions, I would just suggest everyone in the room that would like to see since we're mentioning multistakeholderism all the time, we focus on CGI when talking about multistakeholder in Brazil, there is a specific example of how multistakeholderism can act in practice which is the fact of closing of the 425 for sending out spam in Brazil which is a really good Example on how multistakeholder group can get together to take a decision concerning the management of 425CCP, that was a case in Brazil where it was one of the countries who used to send out most spams throughout the world, and by doing this after a multistakeholder procedure the situation was micromanaged. This is just one example and CGI prepared a document in Portuguese and English on that, that would be -- maybe in Spanish -- but that's useful if you want to take a look on how multistakeholderism can act in practice and I give out just that example. Thank you.

>> THIAGO TAVARES: Thank you very much.

What's your policy question on how to address the issues?

>> PETER MICEK: Thank you.

Well, I would ask -- first I would ask if we believe that there is such a thing as a redline, a floor below, we don't think it is accessible for any actor in the Internet sphere to fall below. If there is, that possibility, how do we go about defining it? The statement from the global commission on the stability of cyberspace about not impacting the public for the Internet is an interesting starting point.

I would ask, you know, then what every stakeholder group can do and personally, with Civil Society, we have organized and the #keepiton coalition, certainly inviting more to join. It is the most productive list serve I have ever seen in Civil Society for one thing.

You know, I think the telcos have a key role to play. They want to be welcomed into the Internet age, and I think it is incumbent upon them to put a little distance and transparency to the relationship with governments and many have and continue to.

States have spoken up at the international level and Freedom Online Coalition and at the United Nations bodies, and I would really love to see regional bodies, courts even, taking on this issue, and it is particularly variations, whether blocking, censorship, DNS management, that sort of thing.

Thank you.

>> THIAGO TAVARES: Thank you very much.

Thank you very much for this interesting discussion.

I think it highlights, nevertheless, the need that the starting point for multistakeholder cooperation is the framing of the problems to make the distinction between shutdowns and blocking issues that won't go away. Both are issues where the multistakeholder model can provide avenues for solutions through cooperation and I think it is very important to ensure that those issues are offered in a way that the different stakeholder groups can agree on what exactly are the problems that need to be addressed, to dissect the problems, they're very complex problems that touched the foundation of our international system, touched the questions of how the sovereignties have exercised in cyberspace and I hope that this session could clarify a few key points and show the plethora of issues that lay in front of us. The issues will not go away, and addressing them in a timeframe of 10 years as mentioned in the proposal, this is a long time for the Internet age. So the pressure to find solutions, to develop standards and norms and principles and decision-making procedures for issues of shutdowns and also of the issues of blocking, of cross-border access to user data, those are among the most pressing issues of our time. We all need to work together in the multistakeholder community to develop the necessary solutions so that we can also in the future continue to have global unfragmented Internet.

Thank you very much, everybody.

Archived Content

- [2017 IGF. Geneva](#)
- [2016 IGF. Jalisco](#)

Resources

[Documents](#)

Additional Information

[IGF Funding](#)

Contact Information

United Nations
Secretariat of the

- [2015 IGF: João Pessoa](#)
- [2014 IGF: Istanbul](#)
- [2013 IGF: Bali](#)
- [2012 IGF: Baku](#)
- [2011 IGF: Nairobi](#)
- [2010 IGF: Vilnius](#)
- [2009 IGF: Sharm El Sheikh](#)
- [2008 IGF: Hyderabad](#)
- [2007 IGF: Rio de Janeiro](#)
- [2006 IGF: Athens](#)

[Publications](#)

[Press](#)

[Glossary](#)

[IGF Donors](#)

[Participant Funding](#)

[Vacancies](#)

Internet Governance Forum ([IGF](#))

Villa Le Bocage
Palais des Nations,
CH-1211 Geneva 10
Switzerland

igf [at] un [dot] org
+41 (0) 229 173 678



UNITED NATIONS

[Contact](#) | [Copyright](#) | [Privacy Notice](#) | [Terms of Use](#)