IGF 2017 Reporting Template

Session Title

Local Interventions. Global Impacts How Can International, Multistakeholder Cooperation Address Internet Disruptions, Encryption, and Data Flows

Date: December 18th, 2017

Time: 10h - 13h

Session Organizers

Flavio Rech Wagner – Federal University of Rio Grande do Sul, Brazil
Ginger Paque – Diplo Foundation, USA
Wisdom Donkor – Africa Open Data and Internet Research Foundation, Ghana
Dominique Lazanski – GSMA, USA

Chair/Moderator

Tereza Horejsova, Geneva Internet Platform and Diplo Foundation, USA

Rapporteurs

Katherine Townsend, USAID and Africa Open Data Conference Movement
Diego Canabarro and Jamila Venturini, NIC.br

List of Speakers and their institutional affiliations

Riana Pfefferkorn, CIS Stanford, USA
Demi Getschko, NIC.br, Brazil
Raúl Echeberría, ISOC, Uruguay
Stefania Milan, Amsterdam University, Netherlands
Melody Patry, Access Now, UK
Bertrand de la Chapelle, Internet and Jurisdiction, France
Anriette Esterhuysen, APC, South Africa
Luis Fernando García, R3D, Mexico
Vint Cerf, Google, USA
Christoph Steck, Telefonica, Spain
Paul Nicholas, Microsoft, USA
Stefan Schnorr, BMWI, Germany
Farida Dwi Cahyarini, MCIT, Indonesia
Anne Carblanc, OECD, France
André Laperrière, Global open Data for Agriculture and Nutrition, UK
Moctar Yedaly, African Union, Ethiopia
Fiona Asonga, TESPOK, Kenya

Key Issues raised (1 sentence per issue)

Extending the call for a multistakeholder approach toward Internet governance to include keeping the Internet open and preventing or countering full or partial shutdowns, including with the Global Network Initiative (GNI).

Work with companies and Internet service providers ahead of any shutdown to know the law and ensure they do not shut down their services out of an illegal demand from the state.

If a partial or full shutdown does occur, and if safe to do so, alert global coalitions and communities to apply pressure and respond.

Target advocacy efforts at local governments and stakeholders, those most closely connected to individuals and communities directly affected by threats to the Internet.

As with any vital infrastructure, ensuring reliable access to Internet is not only a governance issue but is also beholden to basic geographic limitations including disaster-prone areas, large swaths of rural populations, varying terrain, and particularly island or atoll nations.

Government inability to protect special access on encryption.

If any government has the ability to break encryption, it may abuse that power and then lose control of the privilege toward unknown actors and motivations.

Encryption is vital to saving lives, and training for encryption is very necessary particularly for journalists in conflict zones.

The Internet was designed to be open. Attempting to restrict information flows according to political borders and whims fragments and changes the fundamental nature of the Internet.

Policies are fine but they aren't helpful without processes. It is necessary to have structure and frameworks for implementing them so policies can have any longevity and impact. To be effective they have to be developed and refined through multistakeholder partnerships.

Communities like IGF need to step beyond their current zone of action and extend their influence to counter the unprecedented power and in many cases overreach of government control on Internet.

Openness needs to be supported and invested in and this very much includes open source communities and technologies.

Technologists are needed in the government, or in close partnerships with governments, to help them make better, more informed and nuanced decisions.

We have to find a way to hold others accountable for promoting and protecting human rights.

If there were presentations during the session, please provide a 1-paragraph summary for each presentation

Shutdowns

Anriette Esterhuysen emphasised the increase of shutdowns over time and how the debate on the subject evolved from a human rights debate, to calculating the actual costs of shutdowns. She emphasized how shutdowns and disruptions have a profound effect on user's lives. Whenever there is a shutdown there has been immediate reaction but little recourse. Ms. Esterhuysen praise Access Now for its campaign of "Keep It On" led by human rights defenders and journalists. She also said that recently businesses have also started to provide data on the costs of shutdown, increasing awareness on the breadth of shutdowns and their impact, but considered that even with this added attention they still happen. Ms. Esterhuysen explained that shutdowns vary in complete shutdowns and partial blocks and recalled that the issue is not localized in developing countries but also across the global North. Ms. Esterhuysen closed her intervention by calling for a multistakeholder approach to the subject: this IGF community talks about multistakeholder approaches for Internet governance, but for so many it's still the power of the states to instruct an operator or instruct a regulator to shutdown the Internet.

Melody Patry introduced the #KeepItOn coalition, a global coalition of over 140 members, mostly from civil society, across sixty countries working to combat Internet disruptions through advocacy, norm building, detection, and mitigation. Ms. Patry explained the approach of the coalition saying that they try to find solutions for populations when they are affected. This includes working with authorities who are enforcing shutdowns orders from government and employing the UN Resolution on Promotion, Protection and Enjoyment of Human Rights on the Internet. She confirmed the alarming increase of Internet disruptions, citing 72,000 instances in 2017 up from just eighteen recorded in 2015 and fifty-six in 2016. She noted that the cause of these disruptions primarily lies with the states which directly order internet service providers or dedicated platforms (e.g. WhatsApp, Twitter, Facebook, and so on) to execute disruptions. She did caveat that in 2016 there was one instance of a shutdown by a non-state actor but stressed the main actor is the state. Ms. Patry issued a series of calls to action for civil society, faced with countering the state as the main actor: 1. When possible, alert the coalition and ask for solidarity- to not just let people know that the shutdown is happening but to alarm the authorities. She said they are also trying to protect the communities affected because something that has already been proved is that internet disruptions underline human rights, harm local economies, disrupt emergency services, impact local communities, and threaten all our work at IGF. 2. Review agreements and licenses with operators and telecommunications service providers so that they know what rights they have against a request from the government and ensure they don't shutdown the Internet outside of the rule of law. 3. Encourage states to implement legislation that protects the Internet and generally work as closely to the local level as possible.

Farida Dwi Cahyarini detailed the unique challenges for Internet reliability in her country, Indonesia. She explained that connectivity between eastern and western Indonesia is a persistent issue, that the country has 17,000 islands and geographic conditions vary, and that sitting on the Ring of Fire means Internet connectivity, and other vital infrastructure, are threatened by earthquakes. She said that taking the whole of the country into consideration, remote areas are higher in population than urban areas so providing universal access requires a whole-of-coverage approach. Ms. Dwi Cahyarini did note current initiatives already underway, that the Government of Indonesia is trying to provide solutions by rolling out broadband fiber optic currently underway in three regions with a projected finish by 2019. All totalled that project should cover 36,000 kilometers across 14,000 cities and is a collaboration with private sector. For next steps Ms. Dwi Cahyarini noted that the Government of Indonesia is reviewing current policy and regulation including EIT, the Indonesian Electronic Information and Transactions Law.

Demi Getschko introduced the Brazilian perspective explaining the role and history of the Brazilian Internet Steering Committee (CGI.br). Mr. Getschko noted Brazil's experience began as many countries did as an academic initiative and expanded to the whole community. By 1995 a newly created steering committee gave some structure to the academic networks and today this multi-sectoral, multi-stakeholder body that predates ICANN does still exist. In Brazil since 1995 Internet is not considered a telecommunications issue but an added value to telecommunications structure. The result is a country with very few regulations on the Internet, which Mr. Getschko concluded is a very good thing. Yet despite the overall positivity of low regulation, Mr. Getschko did cite problems such as the 2007 blockade of YouTube from a perceived undignified video. This motivated the development of some agreed Principles for the Internet, which the Steering Committee then presented at Vilnius IGF and which were very well received. After this decalogue of principles, Brazil approved a civil framework of the Internet on the Rights of Citizens, which was also well-received internationally. Mr Getschko concluded with empathy on the difficulties in preventing disruptions in Internet services. He said that there are no clear maps of the thousands of networks that make up the Internet and that could include those contained within and crossing political borders and country boundaries. Because of that, any attempts to shield the Internet, if done improperly- and he remarked that there is no clear right way to protect the Internet- will invariably cause disruptions for other parties and much worse effects than intended. He concluded with a call to action and a plea to the community to emphasize the protection of privacy, neutrality of network and the responsibility of intermediaries in the process.

Christoph Steck , who serves as the Chair of the IGF working group on ETNO & international chamber of commerce, pronounced that shutdowns are a lose-lose situation for all the participants since they prevent operationality and cause damage to the reputation of the providers. Mr. Steck considered that full network shutdowns are not sustainable for the future, but specific service disruptions are on the rise. Without delving into taxonomy, Mr. Steck did stress the difference between when access to Internet disappears entirely, which is off course the worst case, and service shutdowns, when governments want to drop specific sites and which are happening more frequently recently. Mr. Steck drew the distinction to draw attention to the difference in motivations: elections in some countries, in others bringing down certain sites prevent policy engagement. Even in the democratic country of Brazil a judge ordered shutting down access to WhatsApp, he said. Mr. Steck's solution is a call to action to raise awareness. He noted that Telefonica is working with many companies within the GNI (Global Network Initiative) to ensure governments understand that partial or full shutdowns are not a good idea. Mr. Steck built on Ms. Patry's call to increase transparency and information on the process for legal government shutdowns to ensure businesses and others can counter illegal calls by governments to disrupt Internet access.

Encryption

Riana Pfefferkorn started the second segment of the main session commenting on the stage of the discussions around encryption. She stressed the role of encryption as a security tool in the protection of human rights, the crossborder impacts of strong encryption and the lack of it, and the impacts of current rules on encryption for the future of cybersecurity. According to her, encryption saves lives in many parts of the world, and democracies that do not enforce encryption subject their own citizens to other countries' laws and unintended consequences.

Raúl Echeberría explained the importance of encryption for the protection of personal data, companies' data and government information. He eloquently noted that, "the issue with law enforcement agencies is that there is an illusion that breaking encryption is only available for the good guys. In this world it is very difficult to differentiate who are the good guys - it's not like the movies. There are plenty of examples of technologies that are available for law enforcement and for hackers and other people…" Mr. Echeberría also pointed out the need for encryption for a functioning government. Security of information is very important for stability of the economy and also for the confidentiality of government operations, like paying taxes. Governments need secure ways of collecting money from taxpayers. He concluded: "Our life is a digital life in this moment at least for half of the world, so we need tools for protecting our privacy, our interest, and our freedom in that digital world".

Moctar Yedaly stressed the need for a framework for the protection of personal data in order to develop digital policies related to encryption. He described the African Union's unique convention on private data as the only convention in the world that deals with data protection. While the Budapest convention relates to cybercrime, he noted that the African one relates to data protection and is made up of three mains parts: the first one regards financial transactions, and Africa is now a leader in online financial transactions worldwide. The second part is personal data protection, and the introduction of digital identifiers such as electronic passwords has led to a lot of questions about identification. Mr. Yedaly channeled the terrifying spectre of the Rwandan genocide and the perils of having an open database of ethnic identification, calling again for the need for policies to protect private data. The final aspect of the convention is cybersecurity and combating cybercrime. He concluded mentioning that the AU Convention defines cryptologies and crypto activities and identifies core terms including encryption, health data, authorized access, personal data, personal data file, how to process personal data, and the obligations and duties of a person who has received personal data.

Luis Fernando Garcíaa gave concrete examples on the importance of encryption for the personal security of journalists and the need for companies to adopt encryption in order to protect users' personal data. He mentioned that over the last 15 years over 100 journalists have been killed in Mexico. Violence is so great in countries like Mexico that traditional media won't report some issues or in some areas. For journalists, privacy and encryption are essential tools to protect their lives and the lives of their sources. Because of this, many civil society groups have invested lots of time in teaching journalists how to protect themselves and how to be secure in their work online.

Paul Nicholas brought in a corporate perspective on encryption and explained that the rapid developments in connectivity and cloud computing caused some governments to block or weaken encryption. He described that after Snowden's 2013 revelation of the NSA PRISM program, organizations redesigned and reassessed how they implement end-to-end encryption. Mr. Nicholas' perspective is that the private sector is "at the balance" of finding a structure that provides appropriate law enforcement access but also follows principles and protects human rights.

Data Flows

Vint Cerf opened the segment on data flows emphasising that the ability to interconnect as the core of the evolution of the Internet is based on technology. He described the need to secure information on the cloud across political borders. Mr. Cerf further stated that the inhibition of data flows would cause the fragmentation of the Internet, citing his own experience that the "thing that makes the Internet so valuable is its connectivity and its reliability for reaching some place [else], and so a fragmented Internet is not an Internet at all at least the way my colleagues and I have conceived it."

Andre Laperriere explained that free data is the key tool for innovation, food security, and safety for all. He gave an account on how free data flows are helping less developed countries to advance rapidly, citing two examples of WeedScount or PlantWise which allow farmers to identify diseases in their crop instantly and receive advise on how to deal with them. Laperriere touched on privacy and data, the curation of data, and the problem related to chasing data.

Stephania Milan tackled the role of digital platforms and their rise as economic and infrastructure models, as well as their role in data markets. She noted that in university settings social media is now the primary platform for connecting with professors, fellow students, and assignments. She emphasised the need for more transparency, literacy, and accountability. Professor Milan concluded with a question for the IGF about the current regulatory model: if you have privatization, data flows stay outside of the larger regulation model, then we really need to assess whether this is what we need going forward.

Fiona Asonga explained the need for the private sector, business, technical community, and government to cooperate in order to enable the use of data. As the government in Kenya had gone full throttle to ensure they are offering services online, business have changed their strategies to ensure they are also aligned to keep operations digital. In 2016 a multi stakeholder group developed the Kenyan "ICT Masterplan" so that data government had collected in analog form needed to translate to online space going forward. One solution was the Uduma services, in kiswahili uduma means help, so they put together centers across the country for citizens to access government services including birth registration details, to pay for your business licenses, and paying basic utility bills. The private sector has been very helpful in this process by ensuring that the government's requirements have an appropriate quality standard and that the guidance is in place for how data should be managed and handled. After two years of running, Uduma has demonstrated that it is possible to work together in a multistakeholder arrangement and that the data are still available for the respective government agencies which need access.

Stefan Schnorr stated that the need for free flow of data is essential for Germany and its democracy, economy, scientific development, humanitarian actions and environmental protection. Mr. Schnorr stressed the importance of balance between the data flows and data protection. To protect citizens and data he cited the example of the European General Data Protection Regulation (GDPR).

Final conclusions

Anne Carblanc elaborated on the openness of the Internet in the technical, economic, social and legal sense. She stated that the issue of Internet disruptions should be tackled on the local, national, and global levels. Openness is vital for the Internet to provide all of its benefits. The Internet was designed to be open and global, which has enabled it to be an engine of innovation. In conclusion she said that coordination is necessary in this field because a lot of policymakers are having the same problems, but there is also a need for frameworks of policy solutions and standards.

Bertrand de la Chapelle summarised the discussion and the necessity to reconcile competitive objectives by recognizing that, at the core, the discussion was addressing how to improve systems, and as such it is an involved and complex issue requiring a multitude of actors around the same table. Mr. Chapelle showed empathy that in any instance any given actor may be right, even regarding an Internet shutdown, and that adding to the particular complexity is that we are living in a world of extreme legal uncertainty. We don't know exactly how national laws apply to cross border Internet environment, and sometimes organizations have competing laws they are compelled to comply with. The only way to move beyond the current state is by stepping out of our silos, he defended. He also noted of the IGF community that we have a tendency to discuss symptoms and problems with actions taken in reaction but that the whole debate about disruptions and shutdowns, for example the blocking of WhatsApp or YouTube, are that these measures are often adopted in reaction or in frustration because other problems aren't solved e.g. how to handle cross-border access when data are not stored or available within your borders. Mr. Chapelle concluded by highlighting that even with this robust discussion so much was left unsaid, including mandatory data localization, which he regarded is a huge issue.

Please describe the discussions that took place during the workshop session (3 paragraphs)

In the first part of the session, the discussion touched upon normative guidelines for access to the Internet, accountability for disruptions by public and private sectors, and the necessity of net neutrality. Patterns in Internet shutdowns included disruptions during school exams. According to Access Now, in 2016 and 2017 thirty instances of government shutdowns occurred during exams. They highlighted that Middle Eastern and African countries in particular employ this technique widely. The discussion also highlighted that shutdowns happen during times that are sensitive to governments including elections and periods of social unrest.

The debate on encryption identified technologies supporting encryption tools and demanded multistakeholder discussion on policy options in this topic. It also touched on the issues of lawful hacking and cybersecurity, as well as the need for normative regulation. The general agreement from discussants is that governments are ill-equipped to provide any nuanced regulation of encryption, that there is no way to guarantee that breaking encryption will only be used for the purposes the government intends, that when they have the power to break encryption they will abuse it. The conclusion was that there should be no ability for governments to have special access on encryption technologies. A resounding call was made to invest in open source technologies and communities. Again a push for multistakeholder approach was made, and it was recognized by all that the digital world does not obey political boundaries, most of the population of the world live under non-democratic regimes, and even democratic regimes are not equally democratic. Democracy is not a universal value. But the Internet is ubiquitous, so it doesn't matter where we break the legitimacy of the information it has global repercussions. Just because one government is a legitimate representative of its citizens and therefore has the right to break privacy, then every government will do it. Once the technologies are available then they will be available for everybody. Encryption has no ambiguity - you either have it or you do not.

In the segment dedicated to data flows, questions and comments tackled the issues of compromised data, data protection and encryption, anonymity of metadata, and net neutrality. Vint Cerf stressed the importance of data integrity citing his conversation with the President of Ethiopia - "I'm not so sure about people seeing my medical information, I'm worried about something changing my blood type so that if I need a transfusion it could be lethal" - concluding that the integrity of the information is as important as the encryption. The conversation on data flows returned to net neutrality, and the talk has centered on government's responsibility on encryptions and backdoors, but not on the role of net neutrality in disrupting information flows and hierarchies of global impact on local information.

Please describe any participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs)

There was clear support from all discussants for a robust multistakeholder approach to preventing and responding to partial and full Internet shutdowns. Particularly emphasis was paid to ensuring transparency in the legal framework and steps for causing a legitimate shutdown and educating all stakeholders, particularly the private sector, to not follow an illegal order for a shutdown. Advocacy campaigns noting the financial burden of shutdowns were also emphasized. Specifically citing Africa, Fiona Asonga urged greater engagement with the technical community and the government so that the government better understands how to address targeted problems rather than a whole-of-internet block.

Regarding the discussion about encryption, there was a call for finding mechanisms for accountability in case of human rights violations. It was also said that a framework for the protection of personal data would help in the development of digital policies related to encryption. The conclusion was that there should be no ability for governments to have special access on encryption technologies. A resounding call was made to invest in open source technologies and communities.   There was a call for a Digital Geneva Convention. IGF was asked to step up, that, "if governments are acquiring unprecedented powers to surveil then they [IGF] have to accept unprecedented responsibility to protect."

There was a call for more transparency and accountability from online platforms once they can also impact free data flows. The way forward was noted as nothing new, but it is still important to have more transparency, more literacy, and better accountability mechanisms that go in various directions, and rethink the multistakeholder model. The representative from Germany was most convinced that joining the German-hosted IGF in 2019 would be the best way to achieve such progress.

Gender Reporting

- Estimate the overall number of the participants present at the session:
175

- Estimate the overall number of women present at the session:
75

- To what extent did the session discuss gender equality and/or women's empowerment?
Minimally. There were presentations on women as farmers but the core message of the session did not address gender.

- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion:
Any conversation on gender equity arose largely in discussion and in insights or response to questions, for example a participant noted that 28% of India is online and of that just 26% are women.