APrIGF: Human Rights Workshops

29 July 29, 2016

Fellows of Rapporteur Group:

- Sajina Karki, RayZnews, Nepal
- Monika Zalnieriute, University of Melbourne, Australia
- Nighat Dad, Digital Rights Foundation, Pakistan
- Nayanatara Ranganathan, Internet Democracy Project, India
- Jelen Paclarin, Women's Legal and Human Rights Bureau, Philippines
- Cheekay Cinco, Engage Media, Philippines

MSG Buddy : Chat Garcia Ramilo

Summary Report

Key issues raised across sessions

1. Human rights are indispensible to conversations about the internet. Beyond obviously relevant rights like freedom of expression and right to privacy, a whole range of other rights like the right to health, right to work are at stake, as illustrated by the global trend of network shutdowns.

2. The internet has also become a space that replicates and enables the same kinds of discriminations that were present before the internet came along. A gendered lens is useful therefore to examine how absence of rights disproportionately affects women and other marginalised groups. In the workshops, there was an emphasis that there continues to be a large gap in access of women to the internet, in relation to men. While we talk about meaningful access to the internet for women, it is imperative that online behaviours of users improve, but this must be supplemented with a broader conversation about discrimination against women more generally.

3. The balancing of competing rights was brought up- While the right to privacy, anonymity and public access to information require a complex balancing of rights, its importance to the Asia Pacific region is enormous, and progress on securing their implementation would enable healthy public debate and benefit several marginalised groups. In this context, there is a continuing lack of strong horizontal privacy protections in many jurisdictions, and overly expansive and disingenuous exemptions to the right to privacy. The responsibility for protection of some of these rights is increasingly being pushed to users.

4. In the conversation on radicalisation, it was stressed that ISIS is not the only source. Also that caution must be exercised to look at pure technical solutions to problems that are entrenched in disenfranchisement of young people. Efforts to censor or filter content online due to radicalisation result in a wipe out of content that is many times irrelevant. In Thailand and other countries, resistance is painted as radicalization, and doing so it becomes easier to discredit content that the authorities want to take down.

Commonalities or priorities

1. Many speakers spoke about how they continue to use the internet to organise creative actions/campaigns, for example: In Occupy Taiwan movement, they managed to employ open source, alternative tools and mesh networking to respond to network shut downs

2. One common priority was transparency- the lack of transparency is debilitating for useful conversations on information control- surveillance or censorship and filtering. If there is no information about the technologies used for surveillance, the data retention policies around that or budgets allocated for functioning of intelligence bodies, there can be no debate about reasonable restrictions to the several rights.

3. Privatisation of human rights- standards for several rights are being set by private intermediaries, who are not invested in protection of fundamental rights. This came out in conversations on sexual expression on the internet, where intermediaries like facebook set the norm for what is acceptable nudity. This also came out in the conversation on the Right to be Forgotten, where the delicate balancing of competing rights is being performed by Google.

Recommendations/suggestions in the sessions

- Push for requirements of transparency in governments, from ISPs. Suggestions in one workshop also emphasised that more attention and understanding is required to see how fundamental rights are complicated and affected by the architecture of the internet and its administration, beyond mere content and usage – as this has an enormous impact on fundamental rights and democracy, yet they are mostly invisible to us in our everyday life.

- The conversation around radicalization has to be extended to include the many forms it takes, and also has to be nuanced so as to ensure that groups/identities are not branded without the need to.

- There is a dire need for a counter narrative to find its space online. We need to engage the youth in the counter narrative to empower them to make their own choices, this requires that they also be givenawareness. Communitylevel initiatives are also needed. At times it has been seen that people join radicalized groups for a sense of belonging, that need to be sustained through something else.

- Adopt privacy by design as a default to strengthen protection of privacy and lessen the burdne of privacy to users. Compnies an dother entities that collect big data to set up ethics committees, build capacity of other civil society groups such as development aid agencies, resarech institutions that collect sensitive personal information about data privacy models based on their specific threats

- Meaningful and equal access for women has to address not only connectivity but also barriers to such as lack of capacity, discrimination and violence.

- Capacity building to understand different layers of blocking, and work on them separately with different groups- content platforms, telcos. More research into surveillance tools used in protests

Workshop Reports

Privacy, Anonymity and Public Access to Information (Monika Zalnieriute)

1. *Right to be forgotten* (RTBF) could be interpreted in several ways; and could be understood as overly expansive in certain contexts. Therefore, there are crucial questions still to be determined in Asia – Pacific (just like elsewhere) on what criteria should be used when balancing between public right to know and individual RTBF.

2. Increasingly, mediation and balancing of fundamental rights online, including free speech, privacy and the RTBF are left in the hands of private actors via their standards contractual clauses. Therefore, *de facto* free standards on, e.g., public nudity (e.g, banned female nipple) are set by Facebook; *de facto* delicate balancing between competing values are made by Google when dealing with RTBF requests. This *'privatization of human rights'* is convenient model for the governments and private multinationals; and therefore, regulatory – as opposed to judiciary (which we see plenty of) interventions are unlikely.

3. From the perspective of public access to information, public wants to know what's behind this 'convenience' – and what are governments demanding the corporations, and how our personal data is used.

4. From the perspective of library policy in the Asia-Pacific region, the role of RTBF is rather limited. In the context of digitization of public records and governmental archives, increasing progress is made in the region, where, in countries like, e.g, New Zealand, researchers now can browse digitized governmental records of the past 150 years. In this context, role of RTBF is limited – or rather irrelevant.

5. *Right to anonymity is* directly related to free speech and other fundamental rights; and it has particular value in the Asia-Pacific region, where discrimination is still prevalent (just like any other region), and various minorities, including queer and LGBT+ communities benefit enormously from the chance to come together online anonymously (especially, where LGBT+ might be criminalized). Right to anonymity, nonetheless, has not been debated equally across the region, e.g. in Pakistan it has hardly received any attention; and is especially acute in the context of the rising security concerns.

B. **What to Make of It: (my own synthesis):** whereas various aspects of privacy, anonymity and public access to information surely require complex delicate balancing act in many difficult situations (bullying, violence online, public records vs RTBF); the importance of these rights in the Asia – Pacific region is enormous, and the progress on securing their implementation would benefit many marginalized groups, such as LGBT communities, women, under-age children.

Internet Architecture and Human Rights (Monika Zalnieriute)

Internet Architecture and Human Rights: *Intro:* Internet Architecture concerns political and economic implications of design and administration of Internet; and various actors – such ICANN, IETF and Internet platforms, such as Google, Facebook, do in fact govern and mediate human rights on the Internet via their standard contractual clauses and Internet design (e.g, algorithms.)

***Data ownership questions regards Internet architecture**:* Who owns personal data- ISPs, bank, phone operator, eCommerce provider, government- complicated question. Which providers can be trusted?

***Value of privacy**:* why privacy is needed and is not something bad, as often interpreted by various interests? Demanding privacy doesn't mean you have something to hide. You wouldn't develop as a person if you are scared of the practical concerns of your searches and how it could be traced back to you. A lot of self-censorship. Nobody wants to have to use PGP, tor, etc. But it's needed, so they do.

***Practical questions**: Participation in policy making:* IANA transition is ongoing, and Accountability WS2 is working on enhancing HR in ICANN.

Framework of Interpretation for HR bylaw- so the dormant bylaw can become active

***Substantial Policy Questions**:* Privacy and WHOIS: Problematic aspects of the WHOIS policy, need for policy debate, not just technical improvements, as proposed in the RDAP. Critical questions of privacy, data protection and data retention, and participation and attention to legal details are crucial.

***Data Sharing Agreements among Governments**:* data is flowing from East to West, where the big companies are located. Asia-Pacific governments feel that they have a lack of access to data. Disconcerting to think that individual data treatment depends on international relations. Different compliance rates between India and US Government requests for data from corporations.

Data localization. Backdoors to encryption- ongoing debate. No US company can provide data directly to another government- it needs to be given to the US Government first, which then gives it to the country- An MLAT request takes about a year to be completed.

Synthesis and Recommendations*:* More attention and understanding is needed how fundamental rights are complicated and affected by Internet Architecture and infrastructure – as opposed to content and usage – as they have enormous impact on fundamental rights and democracy, yet they are mostly invisible to us in our everyday life.

Privacy, Protest and the Private Sector (Cheekay Cinco)

Highlights:
In the countries represented in the panel (Malaysia, India, Pakistan, Taiwan - Vietnam is an exception), the internet has become a space to exercise FoAA, and to organise creative actions / campaigns. Some examples covered were: #ClaimYourMosque (Pakistan), Bersih (Malaysia), Pink Chaddi (India), net neutrality campaign (India), and Occupy Taiwan.

On the other hand, many governments (with or without backing from the law) have implemented network shutdowns, especially during times of protests. India, to date, has had 40 network shutdowns with the last 6 months having around 9 network shutdowns. Most government have kill switches for network connectivity. Another tactic employed by governments has been to take down websites. For goverments like Vietnam, the goverment

has done both network-level shutdowns, site blocking (application blocking), and word censorshp over SMS.

In Occupy Taiwan movement, they managed to employ open source, alternative tools to respond to network shut downs.

Many of the goverment actions to curtail FoE and FoAA target already marginalised groups already (i.e., LGBT groups)

Recommendations:

- Advocating against network shutdowns on rhe principle that the cost of keeping the network up is cheaper than shutting the network down - Seek to judicial review to get repressive laws repealed or lowered - Counter speech is really important; using alternative tech
- Understanding layers of blocking >> work on them separately >> embed people in gov >> work with gov
- Capacity building for the public sector is just as important - Look into surveillance tools deployed during protests
- Strategies around publicity (depending on the level of non-violent mass movement). Secure when small, publicise when there´s a mass tipping point

Regional Transparency Report and Online Rights Protection measures (Jelen Paclarin)

1. Context: When Google released its transparency report in 2011, it encourages more organisations to release similar reports and present the various cases/issues where a company or agency became obligated to cooperate with the government.
2. Transparency remains a continuing challenge in varying aspects:

No clear data how many data request from the government through the service providers were sent through court order

No data from the police in terms of how many request from the government were acceded by the service providers

Content removal and surveillance are ongoing concerns in countries like South Korea, Taiwan and Hongkog

Continuing lacking of overall policies to require governments to protect right to privacy of citizens (e.g. vague law or lack of law)

Limited access to government data -- but there is huge imbalanced when it comes to privacy protection by government versus corporations, it seems that regulatory regimes are under pretty stringent preservations of real identity information

Recommendations:

- Set up an independent review of the government request.

- Develop a public internal guidelines
- Make regular the release of information of government and service provider
- Need to raise awareness of citizens on their rights and freedoms both offline and online
- Government must proactively investigate on cases which has potential risk to violate the right to privacy.
- Telcos must be encouraged to conduct their own transparency reports.

Online Women Violence and Awareness of Social Media (Sajina Kark)

Key points:

Different perspectives and scenarios were raised from the panelist representing Nepal, India, Taiwan and Philippines.

The research suggests that 73% of the women are already exposed to or have experiences some sort of online violence. Again, Online VAW mostly occurring at the age 18 -24, specially in and around their own proximity where there seems to be lack of awareness and regarding action and laws there seems to be a gap of understanding and another fact that came into notice is that several Online VAW goes unreported. The major reason might be the fear of social repercussion. Also, victimized women/girls have had unpleasant experiences while seeking legal assistance.

Some of the examples: #Quandeel Baloch (Pakistan), #Priyanka Karki (Nepal), #Iamtrolledhelp (India), #Sunflower Movement (Taiwan)

Though the cyber law is present but due to lack of proper monitoring and updates, it serves little use in protecting users online. Internet provides easy accessibility and other facilities but at the same time technology also threats the communities in lack of proper mechanism and policies which needs to be researched and worked on.

Many ideas and thought of schools have been poured in but an interesting aspect of the session was the ideology of women being against various aspect of the socio cultural practice. Likewise, it also highlights the contemporary practice of male dominated society which needs to settle down with effective women position strategy and leadership opportunities as well as the need of right knowledge of sex education in terms of gender equality.

Recommendations:

1. Further aggressive awareness campaigns are needed in terms of Online VAW
2. Counselling call centers must be opened
3. No tolerance in terms of policy and action mechanism is needed
4. Women are unaware of their basic rights in the developing countries so more focus needed in that segment
5. Effective policing and immediate action mechanism should be set-up
6. Social media intervention is highly recommended
7. Special awareness packages for Men is needed
8. Online research and surveys are required
9. Proper sex education with gender equality knowledge

Fostering Freedom Online: The Role of Intermediaries (Cheekay Cinco)

- a look at legal and practical challenges Highlights Conversation will be based here: http://responsible-tech.org/the-recommendations/

The first country to immunise the ISPS both civil and criminal law. Trends is towards balancing, and having immunity for intermediaries on civil cases

- India: 300 M subscribers, 2nd largest
- Korea: Law allows content regulation on two levels: content removal request of those that are in violation of ¨sound communication¨ ethics; defamatory content can be requested, as do the messages that break traditional. More powerful than the right to be forgotten.
- Expectation that reading an EULA automatically means that users understand the privacy policies
- ¨Informed consent¨ should be interrogated. Getting consent once because users value what they are getting over their privacy, but have no idea what it means to give their consent
- Inconsistency in providing notice to users about content takedowns. DMCA complaint - user is notified. Intermediary policy violation - user not notified https://www.manilaprinciples.org/template

Recommendations

From http://responsible-tech.org/the-recommendations/

- Guidelines on Privacy Should apply to civil society sector as well. HR, dev, aid worker organisations also collect data about health, personal information, sensitive data about other people. Build capacity in these groups to look at data privacy models based on their specific threats
- Instead of pushing the responsibility of privacy to the users, look how privacy is default in the design.
- Opt-out privacy clauses is not a great idea. Privacy is not a luxury.
- Have ethics committees, especially on big data

Threats to Free Expression and Challenges for Reform in South-East Asia (Nayanatara Ranganathan)

General threads

- Increasing domestic internet controls discussed in Malaysia, South Korea, Thailand, Phillipines, in the nature of censorship, filtering and surveillance

- Anti-government speech and debate criminalised in many jurisdictions in the name of libel, seditious speech, in public interest and penalties are disproportionate

Specific country cases

Thailand:

Information controls including relating to the internet among the first measures taken after martial law applied- banning speech, requiring ISPs to cooperate in censoring and monitoring social media

South Korea:

Defamation and hate speech laws being used to incarcerate speech critisicing the government and insulting police officers, creating a chilling effect; obligation of thinking about 'public interest' on individuals

Public interest obligation imposed on people trying to say something, thereby losing a lot of important debate

Many falsity defamation are seditious libel cases- KCSC gives 'correction requests' with 100% compliance rates

Phillipines:

58 journalists were killed in an election-related killing; becoming one of the most dangerous country for journalists

Many content types, widely interpreted subject to censorship, filtering or surveillance- cyber libel and other cyber crimes, child pornography, malicious disclosure of information, terrorism, treason, espionage etc

Emerging threats are the proposed national id system, proposed mandatory sim card registration system, proposed expansion of exemptions to anti-wiretapping law

Malaysia:

Sedition laws interpreted such that insult to ruler, govts is criminalised, affecting politicians, activists, lawyers, cartoonists

Multimedia and communication act- penalties include being banned from the internet forever, or having a tracking device after getting out of prison

Wide berth to interpret intermediary and where DNS blocking happens, nobody willing to show the list

Recommendations:

Well-known security measures like using https, DNSSEC stops many of the ways in which information is controlled (packet manipulation, DNS blocking)

UNHRC's general comment 34 (2011) useful
- no criminal punishment for statement not subject to verification
- truth must be sufficient defense
- try to stay away from criminal prosecution

The role of key stakeholders in disrupting the dissemination of child sexual abuse material online (Jelen Paclarin)

1. Use of child sexual abuse material (CSAM) over child pornography.

There is an increasing number of child sexual abuse materials uploaded in the internet nowadays. However, the facilitator emphasized that children's groups are using the term CSAM rather than child pornography because "many people find it difficult to imagine pornographic images of children, and therefore do not understand what is meant by child pornography".

2. Issues and Challenges in Online Child Sexual Abuse

- What is the responsibility of the internet platform?

- No clear definition of ISP liability in reporting child sexual abuse

- Varying cultures have varying contexts and define laws differently; because of varying cultures, they may be activities that are not defined by laws but are exploitative of children

- There are competing and varied issues on child rights and internet that needs further discussion. These are the following : child protection vs right to information access, child participation in internet governance, Multi stakeholder engagement to create a child friendly environment, Cross boundary cooperation and multi stakeholder collaboration

3. Varying efforts to combat online child sexual exploitation

a. Photo DNA Cloud Computing of Microsoft: Includes effort that advocate for online safety and foster digital citizenship – safer, responsible and appropriate use of technology.

b. Digital Crimes Unit of Microsoft: Aims to keep the internet safe from malware attacks, protect the vulnerable situation including children and older persons (e.g. internet scams).

c. Financial coalition against child pornography (e.g. Asia Pacific Financial Coalition): Collaborative efforts between financial industries such as Google and Microsft which aims to understand the business model of the merchants that are selling illegal content but using legitimate corporate platforms.

Gender and Access (Nighat Dad)

Key issues:

- Access is essential to realising the potential of the internet

- For the development of equality it is imperative that online behaviours improve, but must be supplemented by improvements in offline spaces as well.

- The issue of gender is linked closely with sustainable development goals - and to promote this we need to engage with civil society actors, private sector, government, activists and more.

- It is critical for women to be able to live freely - nothing is more detrimental than discrimination and inequality for women in what are so obviously assumed to be male spaces, sans any real discourse.

- Access issues persist in India overall and not just in terms of gender where 70% of the population is accessing it through cafes. Situation is even worse for women that have only a 17% penetration. Pakistan is in similar dire straits.

- Access efforts are often geared towards teaching women how to use the internet for 'productive' measures and never towards their own happiness or desires. It's not as simple as them using it for education, work or solving problems, they can use it to also fulfil themselves.

- Women often prioritise work and children over using the internet. They seem to believe that they have no need to use the internet, and women using it is often seen as a waste of time and resources

- Religious and patriarchal barriers are in strong play all over Asia. In some spaces people literally feel that women using technology is taboo; e.g. girls using internet to promote their folk music in Kashmir have found a fatwa stating that it's not right for them to be on the internet.

- Digital literacy is measured in vague terms. It's the same with computers and mobile phones. Mobile phones are becoming one of the major tools in India to access the internet. India is seen as an oral society and a missed call is taken as a form of communication. They don't want to waste the Rs. 1.50 and instead they give signals through missed calls

- Real problem with government services is because the lack of sex aggregated data.

- Access needs to be inclusive and we want ICT to include the concept of digital inclusion. The number one thing here is accessibility.

- It's not enough to build infrastructure, people have to learn the capacity.

Solutions:

- It is interested to take stock of innovative approaches undertaken at the community level. There are lessons here that can be learned and expanded onto other regions

- There is a lack of awareness about access, and basic right to access, an efforts need to be made to rectify this situation

- Women need to be sensitized as to not just what is their right to be productive online but also that it is their right to be happy online

- People outside the typical activists circles need to step up their game in defending women's rights. It's not enough for activists to do and say what they do, a dire need exists for an expansion into the mainstream

Radicalisation in the digital age - How to counter online extremism and build a counter narrative (Nighat Dad)

When we talk about radicalization our main focus almost always becomes ISIS. In the Asian region - and even globally - it feels like the most significant threat. Most recently, ISIS is on the fore front of news about radicalization again. The Dhaka attacks left more than 20 dead, and were conducted by young, somewhat privileged kids. But ISIS gets all the press, others are radicalizing minds online too. Just in South Asia, there is a problem of Hindu extremists, the Taliban are using social media to radicalize minds, and while ISIS hasn't been able to take roots in Pakistan, religious extremist parties continue to use social media to push fwd their agenda. South East Asia is no different, as our panelists from Indonesia, Malaysia and Thailand helped point out. The panel helped shed light on different aspects of the situation in Asia.

Main points

- Radicalisation can mean something for one person and another thing for another because there hasn't yet been set a specific definition of what it means in the global context.

- Efforts to censor or filter content online in Indonesia resulted in actually a wipe out of content that may not even have been relevant. When we opt for mass actions there is always collateral damage.

- Counter narratives being built through digital means have also been targeted with malware and their data has been taken down. Meanwhile it continues to be hard to report and remove content online.

- Radicalisation has to do with the youth having a need to belong to something and somewhere. While outsiders do not understand the appeal of something like Daesh, for the young girls that join it, it's more about finding equal footing with the men

- The issues can also stem from a twisted narrative. In the case of Thailand resistance is painted as radicalization, and by doing so it becomes easier to discredit. One person's radical could be another's freedom fighter.

- Radicalisation is being done to do two things basically: one to get recruits to promote hate, and two to target a certain set of people

- In most cases, the targets are minorities. Be it ISIS or a Hindu extremists, the targets are some form of minorities - could be the LGBT, could be women, could be religious minorities, etc.

- Women are also a target of radicalization, despite not classifying as a minority, the power dynamics put them at risk anytime they try to break away from the status quo

Recommendations:

- We need to see what kind of responses that are needed from allies and not just feminists, and also from the platforms and then fix them.

- The conversation around radicalization has to be extended to include the many forms it takes, it also needs to be nuanced so as to ensure that groups are not branded without the need to

- There is a dire need for a counter narrative to find its space online. We need to engage the youth in the counter narrative to empower them to make their own choices, this requires that they also be given awareness

- Community level initiatives are also needed. At times it has been seen that people join radicalized groups for a sense of belonging, that need to be sustained through something else.

- Companies like Facebook and Google need to further ask how they will deal with problematic legislations and government pressure