Multimedia Toolkit

Internet Rights are Human Rights:
Sexual Rights & the Internet

Developed by Rima Athar

CASE STUDIES

Case 1: Content Censorship & Lack of Transparent Process (Indonesia)[1]

Activists in Indonesia have been trying to raise awareness on internet regulation and censorship by the Indonesian government as a sexual rights issue. In addition to Indonesia's obligations under international law, activists highlight how free and open access to the internet is a constitutional right guaranteed to Indonesian citizens.

Article 28C paragraph 1 of the Constitution states that, "*Everyone shall have the right to develop him/herself through the fulfillment of his/her basic needs, the right to get education and to benefit from science and technology, arts and culture, for the purpose of improving the quality of his/her life and for the welfare of the human race.*"

Activists highlight the importance of this right particularly for marginalized communities. For example, for people living with HIV/AIDS who face social discrimination and stigmatization if they are open about their positive status, the internet provides a space through which they can join support groups, access information about living with HIV/AIDS, and participate in forums with relative anonymity.

In 2009, the Ministry of Information Communication (Menkominfo) formed a network with civil society organizations, academics and internet businesses to launch the 'Healthy and Safe Internet Program' (Program Internet Sehat dan Aman, INSAN). This initiative aims to regulate the internet in Indonesia through establishing 'decency' norms, and working through ISPs to block so-called 'pornographic' content.

On the positive side, INSAN attempts to provide information about internet safety and conducts activities that complement this focus. However, the worrying trend for activists is that the lack of clear definitions of what constitutes 'indecent' material, and what criteria are used to label sites 'pornographic' has resulted in the public Ministry and private internet service providers (ISPs) filtering and blocking online material and websites related to sexuality online.

A few examples of websites that were labelled 'pornographic' and blocked included:

---

[1] This case study is sourced from http://www.genderit.org/feminist-talk/sexual-rights-indonesia-creating-and-protecting-safe-spaces-women-minority-groups, and http://www.genderit.org/feminist-talk/controlling-indonesia-s-internet

- OurVoice Indonesia—an NGO whose website compiles news on tolerance, diversity and respect for LGBT rights, the rights of religious and ethnic minorities, and other populations who face discrimination Indonesia.
- The International Lesbian, Gay, Bisexual and Transgender Human Rights Commission (ILGHRC)
- Guerrilla Girls—a feminist group that campaigns against sexism, racism and corruption using art

When OurVoice Indonesia's director asked for an explanation from the ISP, they responded that they were following Menkominfo's orders. Yet when OurVoice Indonesia asked Menkominfo about the situation, Menkominfo responded that they had not ordered the block.

OurVoice Indonesia was left with no clear answer as to why their website had been labelled 'pornographic' and blocked by the ISP, and with contradictory responses from both the government ministry and the private service providers, there seemed to be no option for recourse.

For activists, when looking at these websites and their content, it appears that 'pornography' becomes a blanket term to filter and block content that either the state and/or private corporations simply do not agree with: i.e. information and political expressions that support gender-equality, sexual diversity and autonomy, and political power for marginalized communities.

Discussion Questions:

- In what ways have individuals' rights generally, and sexual rights specifically, been violated in this case?
- Who are the main actors in this case, and what are their responsibilities in regards to human rights?
- Is there a similar misrepresentation of political expression, sexual rights and/or 'sexuality online' as 'pornography' by actors in your context?
- What strategies would you take to find recourse in this instance? What demands would you make, to whom would these be directed?

Case 2: Privacy and Anonymity: Facebook's 'Real Name' Policy[2]

In September of 2014, Facebook suspended the accounts of a number of San Francisco based gay and transgender entertainers for not using their 'real names' on their profile pages. Facebook asked them to switch their profiles to their legally registered names, as per the company's 'real name' policy. Facebook claims asking people to use their 'real names' "helps prevent bad behaviour while creating a safer and more accountable environment"; specifically Facebook suggests that people are less likely to engage in abusive behaviour online when their real name is attached to their own account.

Yet as activists have pointed out, Facebook's policy has far-reaching implications for people's right to self-determination, privacy and freedom of expression online. There are a number of reasons why people may choose to not use their real names in online spaces, as a strategy of self-protection. For example, victims of abuse & stalking may choose to use an alternative name online, so as to still be able to access a supportive online social network, but not fear being threatened, harassed, or targeted offline. This is similarly true for LGBTIQ people who may not be 'out' to their families, friends or certain parts of their communities offline, but who still want to have an online social presence where they can be open about their orientation or gender identities, by using a different name.

The policy also has implications on professional relationships that revolve around confidentiality. As one health practitioner explained, "It is counterproductive for a client of mine seeking mental health services to be able to, especially at the beginning of our work together, know and see me as I appear on Facebook … Many of my colleagues also use a fake last name to prevent this exact type of access by our clients." Similarly, a sex educator explained how she has received many death threats for her work: "Divulging my real name publicly could very well put me and my family in danger. Anonymity is important not only to people in the public eye but to anyone who may feel threatened having their private info publicly available."

With millions of users, Facebook relies to a large extent on user-reporting to identify accounts that are not using 'real names'. If they suspend an account due to the 'real name' policy, Facebook requires those who wish to retain access to their email to provide official government IDs (e.g. credit card, drivers' licence, passport, or other government document) to confirm their identities. This raises acute challenges especially for trans* identified people, who may not be able to change their names on their official government IDs due to legal barriers; it also has far reaching implications on the power of Facebook to obtain, store and/or share the personal information of users beyond what is regularly requested by online service providers.

Questions for discussion:

- What implications does Facebook's 'real name' policy have on privacy rights and sexual rights of users?
- Do you agree with Facebook's claim that requiring users to use a real name helps "create a safer and more accountable environment"? In what ways could the policy contribute to a less safe environment?
- Should Facebook be allowed to ask for and store user's government issued IDs?

[2] This case study and all quoted material is sourced from http://www.cnn.com/2014/09/16/living/facebook-name-policy/

Case 3: Targeted Violence Online [3]

In 2013, APC conducted a global survey (Sivori and Zilli, 2013) on risks facing WHRDs working on sexual rights, including reproductive health and rights, LGBT rights, access to safe abortion, sexual violence and rape, and sex education. The report states that "99% of activists stated that the internet was a crucial tool for advancing their human rights work. And yet, 51% reported receiving violent or threatening messages online. About one third of the sample mentioned intimidation (34%); blocking and filtering (33%); or censorship (29%). This resulted in 27% of them discontinuing the work they were doing online."

In one example, In 2013, the website of the Latin America and Caribbean Women's Health Network's (LACWHN) was hacked and disabled and their Facebook page taken down twice. This happened after the Ecuador-based network had launched an advocacy campaign around safe access to abortions, using the hashtag #28SAbortoLegal. The Women Human Rights Defenders International Coalition noted in a statement released shortly after the attacks:

> The WHRD IC believes the digital attack is a deliberate attempt to silence legitimate feminist voices, suppress dissent and stifle women's political participation in the public sphere on these issues by stigmatization and sabotage. The spaces where we, as WHRDs working on sexual rights provide information and communicate from on the right to information on health and bodily integrity are being systematically attacked. (Women Human Rights Defenders International Coalition, 2013)

Concerns of digital security—especially for activists—are not only confined to the web. Another example is the 7 May 2012 police raid of the Ugandan Women's Organisation Network for Human Rights Advocacy (WONETHA)'s sex worker drop-in centre. As one of the five people arrested recounted, the organizations computers were targeted for confiscation:

> "They started searching our office in every corner including the dust bin. They connected the computer and asked me the password, and opened the emails we send to our office in Kampala. They asked me if we have a flash disk, which I said we didn't… but we have a modem for our Internet. They took it, along with papers, a printer, the cash book, a stapling machine, a puncher, a computer and a CPU" (FD, 2012).

The implications of the raid were serious:

> "Confiscating the computers enables the police to access private data on sex workers, their names, health status and their contact details. Demanding the passwords to their systems and opening emails puts many people at risk – not only the sex workers, but people who work with them. As activists, we are individuals and organisations connected to others in online spaces. This means that awareness and practice of our safety means securing our communities. As c5, an activist who trains and capacitates activists in digital security says in all her trainings, "We are as secure as the least secure members of our networks."'

Questions for Discussion:

- Who are the main actors responsible for the attacks in these two examples? Who are the main actors' who are affected? What avenues of recourse might there be?
- How do you/r organization implement digital security practices in your activism?

---

[3] This case study and all quoted material is sourced from http://agi.ac.za/sites/agi.ac.za/files/standpoints_digital_security_as_feminist_practice.pdf.