Feminist Principles of the Internet Training Module
Module Handout

Developed by: Rima Athar

Module Outline

The module centres around the 15 Feminist Principles of the Internet[1] that were developed by the Association for Progressive Communications (APC) and a group of international activists, researchers and scholars at a Global Meeting on Gender, Sexuality and the Internet (April 2014). The Feminist Principles are explored through a brief overview of the key themes of activism, access, economy, privacy, and agency as they relate to the internet as a public space.

Throughout this module, the following questions are posed:

- What is a feminist approach to the internet?
- What does activism, access, economy, agency and privacy on the internet look like as a feminist concern?
- Why is digital security a feminist concern? How can we increase our security by engaging with the politics behind the technology?

What is a feminist approach to the internet?

> "There is no such thing as a single-issue struggle because we do not live single-issue lives."[2] – Audre Lorde

As a political framework, a human rights based feminist lens is underlined by recognizing the intersectionality[3] of our struggles for rights and justice. The above quote is from a speech made by Audre Lorde, who self-identified as a black, lesbian, mother, warrior, poet in part to shed light on how all parts of our identities give rise to different struggles that shape our daily experiences. By being present within all of us, these struggles cannot be explored in isolation disconnected—for Audre Lorde, this meant that she stood at the intersection of numerous forms of discrimination and oppression, including homophobia, sexism and misogyny, a lack of socio-economic support for women raising children, a lack of accountability for violence against women in the domestic sphere and in daily life, economic poverty in her community, all of which were compounded by and embedded within a system of anti-black racism. She chose to politicize and publicize these parts of her identity, because they underscored for her the multiple fronts on which she stood, both as a warrior—struggling for justice and rights, and as a poet—imagining, creating and expressing the world she wanted to see.

Intersectionality is an important addition to understandings of rights as intimately connected. The key principles of universal human rights are that human rights are inalienable, indivisible, interdependent and interrelated. This means that rights exist within us from birth, that the rights we have cannot be divided up and compartmentalized, and that the

[1] http://www.genderit.org/articles/feminist-principles-internet

[2] This often-quoted sentence is part of a 1982 speech by Audre Lorde, entitled 'Learning from the 60s', which she gave to commemorate impact of Malcolm X on creating a generation of critical thought about race relations in the USA. The full text can be read in English here: http://www.blackpast.org/1982-audre-lorde-learning-60s.

[3] Intersectionality was first voiced as a critical sociological theory by legal scholar Kimberle Crenshaw in 1989, though as a political framework intersectionality has its roots in black women's resistance movements in the 19th and 20th centuries against violence, slavery, systemic racism and disenfranchisement in the United States.

realization of human rights requires balance. In practice this means that one persons' right to freedom of religion or belief, for example, cannot trump another persons' right to education, right to healthcare, or right to freedom of expression. Similarly, one person's right to freedom of expression cannot trump another persons' right to privacy, or right to life free from violence. A human rights framework implicitly recognizes the connection between individuals' rights.

By looking at the meeting points of our various identities and how that shapes our social experiences, intersectionality highlights how the enjoyment of rights in practice is dependent on who has access to and enjoyment of various forms of structural privilege and structural power. Intersectionality looks at how multiple forces work in tandem to reinforce conditions of privilege and inequality, social inclusion and exclusion, that shape day-to-day life.

Writing about women's critical participation in Internet governance, Dafne Sables Plou highlights, "The women's movement has always had the ability to make visible the invisible and grant it a political character." [4] Making visible and addressing the intersectionality of our movements and struggles as they relate to the internet is that political character which underlines and frames a feminist approach to engage with, to imagine, to define and to (re)create the internet as a public sphere for the realization of universal rights.

As Jac Sm Kee explains, "From falling in love to demanding accountability from our government, [the internet] is becoming part of the texture of our everyday social, political, economic, and cultural life. It's not just an inert tool that we wield when we have access to it, but a space where things happen, where identities are constructed, norms reified or disrupted, action and activities undertaken. As such, it cannot help but be a space of intersectionality where many things collide and connect."[5]

Developing the Feminist Principles of the Internet

When the 15 Feminist Principles of the Internet were formed, the main groups in the discussion were those concerned with 'internet rights', 'women's rights', 'sexual rights'—frameworks that, generally speaking, tend to prioritize specific foci within a broader set of human rights.

For example, some of the key concerns for 'internet rights' are the issues of access, freedom of knowledge and expression, and privacy as they relate to online and digital spheres.

Women's rights are concerned with the intersection of gender and sexuality as it relates to human, civil, social, economic and political rights—particularly focusing on the ways in which women continue to be marginalized from accessing rights in these spheres. Ending violence against women is also central to this framework.

Sexual rights centre the relationship of human rights in protecting and promoting sexual agency, sexual pleasure, sexual health, sexual education, with a focus on choice, consent and agency. Sexual rights frameworks implicitly centres women and LGBTIQ people's experiences—including experiences of gender-based violence—when exploring the intersections of gender and sexuality in human rights.

The aim of the Global Meeting on Gender, Sexuality and the Internet was to look at the intersections and overlaps between these frameworks, and to see how they could be strengthened by building solidarity around the internet as a public sphere where rights are

[4] ibid. p. 8

[5] http://ignite.globalfundforwomen.org/gallery/building-feminist-internet

realized. After three days of workshops, discussions, and collaborative action, the 15 Feminist Principles of the Internet emerged by consensus. Broadly speaking, the principles centred around five overlapping thematic areas that lie at the intersection of gender, sexuality and the internet: (a) activism (b) access (c) economy, (d) privacy and (e) agency. These themes and some of their intersections are discussed briefly below.

Activism

Central to the Feminist Principles of the Internet—which express the kind of public space we want to see that supports the growth of our social movements—is a recognition of the internet as a vital public sphere for our activism.

In the same way that feminists on the margins, of class, race, gender, sexual orientation were presenting the importance of intersectionality in the 1970s and 80s, today they are continuing to do so—and in some ways the internet is facilitating this resistance, by allowing for freedom of expression, amplifying our voices, and building bridges across global struggles.

One example is the move by Dalit women in India to raise awareness about and to dismantle the centuries old hierarchical system of caste in India, which excuses the continuous sexual violence, harassment, intimidation—as well as the economic, social and cultural exclusion—that Dalit women face daily. Using the hashtag #DalitWomenFight, the group has taken their campaign to the public sphere of the internet, promoting Dalit women's voices, authorship, interpretations, stories and resistance.[6]

In March 2015, the group held a 'Wikipedia Hackathon', where they combined learning and promoting their struggle, with a hands-on exercise in taking back the tech, and engaging the audience to write entries about the struggles of Dalit women. The aims were to create space for Dalit women's histories online, and to be present on the internet. The event was a success, but not without challenges. As one participant shared, as they were creating Wikipedia entries about Dalit women's histories, they were facing backlash of derogatory comments, attempts to delete the entries they wrote, and other forms of trolling by Hindu nationalists who wanted to silence discussion about Dalit women's rights in any public sphere.[7]

The act of trying to silence #DalitWomenFight online is an (perhaps inadvertent) admission and recognition on **the transformative power of the internet as a public and political space** to raise voices, to increase debate, to inform and educate, and to demand the realization of rights. The 'trolls' here were seeking to ensure that the internet generally—and Wikipedia specifically as people powered popular forum for information exchange—isn't being used to support Dalit women.

While Dalit women are taking to the streets and the internet to raise their voices and to resist systemic discrimination, they are facing aggression and silencing and the denial of rights in both public spaces. **This is a clear example of the ways in which gender-based violence and discrimination on the basis of numerous identity markers *online* are an extension of systems of gender-based violence and discrimination that exist *offline***. It is also a clear example of the power and need for connecting resistance movements in both spheres.

---

[6] See http://www.theguardian.com/world/2015/mar/12/thenmozhi-soundararajan-dalit-women-art-and-activism, as well as https://www.facebook.com/dalitwomenfight, and https://twitter.com/dalitwomenfight

[7] This was related through personal conversations with a participant at the hackathon.

Another example of **the potential for the internet to become an extension, reflection and continuum of our movements and resistance in offline spaces, public and private**, is the Kenyan campaign #MyDressMyChoice, which was launched in response to two women being stripped and beaten by a group of men in Nairobi. The men claimed they were justified in ripping off the women's clothing and beating them, because the women were "dressed indecently".

The incident gained widespread attention when a video of the attack was posted to YouTube, although the platform subsequently removed the video in accordance with its policy prohibiting content designed to "bully, harass, and threaten".[8] Women in Nairobi held a protest on 17 November 2014, many of whom came out in miniskirts, to raise awareness, demand justice, and call for an end to violence against women. The online Twitter campaign saw people from all over tweeting their support for the women's protest, demanding justice, denouncing the idea that dress codes are ever an excuse for violence against women.[9,10] As of 5 April 2015, a Nairobi court rejected a demand to drop the charges against the six men, instead ruling the case would be heard on 27 July 2015.[11]

Access

Underlying our ability to engage the internet as a public sphere to support individual rights and the growth of social movements, requires that we have universal, affordable, unfettered, unconditional, and equal access to the internet.

Yet if we look at **how gender intersects with internet governance** today, we see a (perhaps unsurprising) imbalance in terms of **access to and participation in decision-making spaces by women generally, and especially women on the margins of class, caste, ethnicity, gender identity (especially trans and intersex women), ability, sexual orientation, and other identity markers**.

A few examples:

- In 2012, there were only 2 women, out of a total 15 members, on the Board of Directors of the ICANN—the non-profit organization responsible for "helping preserve the operational stability of the Internet; to promote competition; to achieve broad representation of the global Internet community; and to develop policies appropriate to its mission through bottom-up, consensus-based processes"[12]. In 2015, that number has risen to 4 women, out of a total of 20 members.[13]

- APC mapped discussions on 'gender' at the Internet Governance Forum (IGF) in 2012 and 2013, and found that "Of the 71 sessions for which ratings were given for 2012, **gender was rated as the main theme for only 1 session** (1% of the total, as against 6% for 2013), and was seen as **not relevant or not related for 50 sessions** (70% of the total, as against 49% for 2013)." There was also a definite majority of male panellists, moderators and remote-moderators, from 2011 – 2013, and the women that were present in these roles tended to be representatives of civil society, rather than government or private sector.[14]

[8] https://www.youtube.com/watch?v=8AyrQKh9eWI

[9] https://twitter.com/hashtag/mydressmychoice?src=hash

[10] www.ibtimes.com/kenya-miniskirt-protest-my-dress-my-choice-supporters-show-support-woman-beaten-men-1724692

[11] http://allafrica.com/stories/201504020326.html

[12] http://www.icann.org/en/general/icann-mou-25nov98.htm

[13] https://www.icann.org/resources/pages/board-of-directors-2014-03-19-en

[14] http://www.genderit.org/es/node/3489, http://www.genderit.org/es/node/4123

- In a 2014 breakdown of international employees of the major social networking and technology giants (including Apple, Google, LinkedIn, Yahoo, Twitter and Facebook), women made up only 30-40% of all employees.[15,16] The majority of women were in non-technical positions however, making up only 10-20% of the technical workforce.[17] While the breakdowns did disaggregate according to 'race', showing how systemic racism further marginalizes Black and Latino women in the hiring process in the US, the breakdowns said nothing of how many women were in upper-level management and policy-setting positions.

When looking at **women's participation and use of the internet,** however, we get a different picture. Looking at statistics provided by the International Telecommunication Union (ITU) in 2012,[18] Dafne Sables Plou noted that "in several Latin American countries (Uruguay, Paraguay, Colombia. Honduras, El Salvador, Brazil) there is near parity in the number of women and men who regularly access the internet, while there are very few countries where a large majority of users are male (i.e. where there are 20-point differences between the sexes, as in Turkey, Morocco, Azerbaijan, Serbia and Croatia). In the United States, there is a slight majority of women in the number of internet users."[19] Additionally, gender-disaggregated statistics on the users of Facebook and Twitter showed that women were the majority of users on both platforms, and accounted for a majority of the traffic.[20] There is still less access by women, in terms of participation and usage of the internet, however the statistics are closer to parity.

Another concern around access includes being able to participate in public life online, without fear of violence, intimidation, silencing or censorship. Today it's well documented that women are disproportionately targeted for violence online—from threats of sexual violence and murder, to hacking private data and spreading it online or using it for blackmail, videos of sexual assault being passed in endless loops. These issues are now gaining more attention worldwide, but it has taken years of women's rights activism to hold governments, the judiciary and corporations to account for their inability to deal with this abuse. In 2015, small steps are being taken—for example Twitter recently announced a revamp of its Terms of Service specifically to deal with the issues of non-consensual distribution of private photos, threats of violence and verbal abuse[21,22]—there continues to be an overwhelming lack of political will to address gender-based discrimination online.

This is similarly true when we look at internet censorship around sexual rights—globally the rise of religious fundamentalisms and the accompanying backlash against sexual rights, has led to increased attempts to (a) censor access to information on sexual and reproductive health, sexuality education, and LGBTIQ rights online, and (b) to silence the individuals and activists committed to making this information and conversations accessible.[23] While everyday sexism and misogyny online has begun to get recognition as a problem, there has perhaps not yet been

---

[15] http://www.theguardian.com/news/datablog/ng-interactive/2014/nov/25/diversity-in-tech-gender-breakdown-of-key-companies

[16] http://www.techrepublic.com/article/diversity-stats-10-tech-companies-that-have-come-clean/

[17] http://www.geekwire.com/2014/chart-bad-gender-gap-tech-companies/

[18] http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[19] Dafne Sables Plou (2012). ' Introduction', in Critically Absent: Women's Rights in Internet Governance, p.5

[20] Op. Cit.

[21]See for example http://www.theguardian.com/technology/2015/apr/21/twitter-filter-notifications-for-all-accounts-abuse.

[22] For a critique of Twitter's revamped policies, see: http://time.com/3831595/twitter-free-speech-safety/.

[23] EROTICS (2013) Survey on Sexual Activism, Morality and the Internet, http://www.genderit.org/articles/survey-sexual-activism-morality-and-internet.

a concerted discussion on the heteronormative sexism, misogyny, homophobia and transphobia within the patriarchal religious rights' attempts to silence women and LGBTIQ people online.

The intersections of these threads of access paint an interesting picture: If women make up near equal, or in some cases more users of certain platforms and internet spaces, and are also disproportionately targeted for violence and harassment online with little recourse—but the pace of change regarding women's and LGBTIQ peoples' access to rights and safety online faces tides of resistance—then conversation about 'access' cannot be solely about access to the technological tools, platforms, and online spaces.

Access needs to also include *access to governance* and the decision-making spaces that define how people are enabled to use ICTs,[24] and therefore access to how conceptions of citizenship are shaped, both offline and online. The picture of 'gender' in these conversations needs to be expanded as well, accounting for women and trans* and third gender people in all their diversity (ethnicity, disability, orientation, caste, class, and more), as we recognize how various groups face more threats, violence and marginalization in certain contexts and spaces. An intersectional feminist analysis enables us to link with past and current experiences, particularly the experiences of those on the margins that have been able to make fundamental shifts in governance and power structures that increase access to rights for all.

Economy:

Increasingly, the question of economy is becoming central to internet rights discourse. Who owns the internet? Who is economically profiting off of how the internet is being used and shaped? And who has the power to challenge the increasing corporate control of the internet as a public space?

Part of the concern around economy is spurred by the seemingly endless growth of giant technology companies—e.g. social media, internet portals, search engines, telephony companies—and their increasing corporate control of the development, spread and use of ICTs and internet spaces. As of March 2015, QQ, WhatsApp, Skype, Google+, Instagram[25], and Twitter, for example, all had active monthly user populations in the hundreds of millions of people[26]—and Facebook over one billion—which makes their 'populations' bigger than many nation states combined. These companies make their 10s or 100s of USD billions in annual revenue[27] based on how, and how often, their users are interacting and engaging with the internet. As their user populations grow, their terms of service and policies increasingly dictate what forms of expression, access to information, privacy and other rights are accessible to a global population online.

Despite touting themselves as the 'upholders' of rights—to privacy and freedom of expression in particular—in practice internet intermediaries continue to cordon off rights on the internet from collective access in their pursuit of profits and a neoliberal model of expansion that reduces everything to a commodity which can be bought and sold.

---

[24] Avri Doria (2012). 'Internet Governance and Gender Issues', in Critically Absent: Women's Rights in Internet Governance, p. 13.

[25] Facebook owns both WhatsApp and Instagram, and acquired WhatsApp for USD $22 billion in February 2014, and Instagram for USD $1 billion in April 2012.

[26] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[27] For example, in 2014, Apple's global annual revenue was USD 182.8 billion; Google's was USD 66 billion (http://www.statista.com/statistics/234529/comparison-of-apple-and-google-revenues/); Facebook was USD 12.47 billion (http://www.statista.com/statistics/268604/annual-revenue-of-facebook/).

A few examples of this trend:

- As recently as November 2014, the EU and the US were considering a move that would end Net Neutrality—the idea that Internet service providers (ISPs) should treat all data that travels over their networks equally. Due to massive campaigning by civil society, Net Neutrality still stands, however, the bills in question sought to grant internet service providers the ability to provide better access to some websites that pay a fee to reach users faster.

  As explained by the Electronic Frontier Foundation,[28] "This kind of "pay-to-play" Internet stifles innovation. New websites that can't afford expensive fees for better service will face new barriers to success, leaving users with ever fewer options and a less diverse Internet."

  EFF also highlights ways in which US and Canadian ISPs have tried to discriminate in terms of access in the past, including:

  - In 2007, Comcast was caught[29] interfering with their customers' use of BitTorrent and other peer-to-peer file sharing.
  - Between 2007-2011, Bell Canada and Rogers both engaged in 'throttling'—discriminatory traffic shaping that slowed down all encrypted file transfers[30] for five years.
  - In 2012, Verizon was fined[31] for charging consumers for using their phone as a mobile hotspot.

- Social networking companies claim to respect users' privacy, but the trend is to default users' settings to 'public' when an individual signs up for a social media or networking service. These companies directly profit from the increased flow of personal information into the public realm without users' active consent,[32] and then absolve themselves of responsibility to support users who have been subject to violations such as "doxing"—researching and publishing personally identifiable information online to shame, intimidate and harass others.

- When Facebook and Twitter initially came under scrutiny for their inability to deal with gender-based hate speech and abuse of women online, both companies made uncritical deference to free speech—effectively excusing violence against women online as 'free speech' for those who threatened and promoted rape, sexual violence, torture and death threats. It was only after women's rights advocates lobbied advertisers to pull their spots in 2013—which would leave companies with a significant loss in their primary source of revenue if the boycott expanded—that Facebook and Twitter changed their tune.

  In 2013, Women, Action, Media (WAM), the Everyday Sexism project, and activist

[28] https://www.eff.org/issues/net-neutrality

[29] https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair

[30] https://en.wikipedia.org/wiki/Rogers_Hi-Speed_Internet#Throttling

[31] http://techcrunch.com/2012/07/31/verizon-can-no-longer-charge-for-tethering-fcc-declares/

[32] For a brief look at how companies profit off of individual data online, see for example: http://www.theglobeandmail.com/globe-debate/follow-your-data-from-your-phone-to-the-marketplace/article17056305/.

> Soraya Chemaly launched the hashtag #FBRape, and encouraged users to tweet it at companies to raise awareness and ask them to pull their advertising until Facebook took action. As WAM founder explained, the move to lobby advertisers was seen as the only way to get Facebook's attention: *"We thought about who it is they really care about," she said. "They clearly don't care about their users, so we thought, 'Well, maybe they care about their advertisers."* [33] About a dozen companies pulled their ads in response to the campaign, and many more were forced to begin thinking about an issue they paid no heed to before. [34]

Another controversy has arisen around Facebook's Internet.org initiative, which was launched in 2014. When it launched, the initiative aimed to bring "free access to a limited selection of basic websites" to rural areas, with a particular focus on economically developing area countries of the global 'South'.[35,36] In 2015, the initiative will create access by flying solar-powered drones into remote areas, which act as the 'satellite' that computers, mobile phones and other wireless devices can connect to.

Activists, companies and others concerned about keeping the internet open and accessible to all have raised a number of concerns around Facebook's initiative. Despite its branding as a 'humanitarian' endeavour to 'connect 2/3rds of the world's population', the platform does not give users equal access to the internet. Companies who have joined the Internet.org initiative have their platforms offered to Internet.org users, while others are effectively barred; there is no choice on the part of those who use internet.org about what content they can or cannot access.

For example, when launched in Zambia, the Internet.org app for mobile phones included a number of global sites, like Wikipedia, Facebook, Google Search, as well as local services like Go Zambia Jobs, Zambia Ureport, and Women's Rights App (WRAPP).[37] Undeniably providing these services without additional data costs to those who were unable to access the internet before is an immense resource. However, when Internet.org launched in India, the choice of sites was different—including having the only global search engine as Microsoft Bing. Facebook and Facebook Messenger are included across all countries.

As critics explain, ultimately the model of Internet.org "creates a limited, lopsided market that favors the few apps chosen by the zero-raters and not users' preferences … In the developing world, zero-rating is even more of a problem, since the entire reason for spreading the Internet—both benevolent and self-interested—is to jumpstart new digital economies. If those new markets are unbalanced from the start, they'll arguably only grow into more maladjusted digital economies, and the Internet for the "next 5 billion" will become an inherently unfair, closed system manipulated by the partnerships and whims of the world's Zuckerbergs."[38]

Additionally, there are a number of concerns around the lack of privacy and security that Internet.org provides. As outlined in an open-letter concerning Internet.org,[39] signed by 67 digital rights groups from around the world,

---

[33] http://www.ibtimes.com/facebook-rape-campaign-ignites-twitter-boycott-threats-fbrape-get-advertisers-attention-1278999

[34] http://www.womenactionmedia.org/facebookaction/campaign-wins-updates/

[35] http://www.wired.co.uk/news/archive/2015-05/05/facebook-net-neutrality,

[36] http://pando.com/2015/03/27/as-facebook-successfully-tests-its-first-drone-privacy-questions-loom/

[37] http://newsroom.fb.com/news/2014/07/introducing-the-internet-org-app/

[38] http://www.latinpost.com/articles/48498/20150418/is-internet-org-good-only-if-it-allows-for-its-own-eventual-demise.htm

[39] https://cippic.ca/uploads/LT_Facebook_re_Internet_org-20150518.pdf

> "Facebook's privacy policy does not provide adequate protections for new internet users, some of whom may not understand how their data will be used, or may not be able to properly give consent for certain practices." On top of that, the current implementation of Internet.org prohibits the use of basic web encryption such as SSL or TLS. "This inherently puts users at risk, because their web traffic will be vulnerable to malicious attacks and government eavesdropping."[40]

As of 5 May 2015, Internet.org is available in in Colombia, Ghana, Guatemala, India, Indonesia, Kenya, the Philippines, Tanzania and Zambia. However as concerns grow over the ways in which the platform model diminishes net neutrality and denies users' choice, some companies have distanced themselves from the Internet.org initiative. In response to these questions, Facebook has claimed that it will open Internet.org to all developers who meet a certain criteria, rather than just selected developers.[41]

Today, governments, private companies and individuals continue to wrestle for control of the internet, in ways that cannot be divorced from looking at economy. Numerous contentious issues are being decided upon at any time. For example at the time of writing, India is considering disrupting Net Neutrality to increase telephony companies' profiteering off of internet service provision;[42] Austrian citizens are filing a class-action lawsuit against Facebook for allegedly violating the EU's privacy laws in their mining user data;[43] Google is trying to absolve itself of the responsibility of having to uphold the EU ruling on **'the right to be forgotten' on the internet**, globally.[44, 45]

There are of course **alternatives to the neoliberal corporate models, including various kinds of open-source and people-powered software companies and collectives**.

The people-powered nature of open source software comes from the ways in which the programming codes are made available to all interested parties, who can then use and adjust them to suit their needs. As the Open Source website explains, the difference between open source and proprietary software can be summarized as follows:

> "Open source is software whose source code is available for modification or enhancement by anyone. "Source code" is the part of software that most computer users don't ever see; it's the code computer programmers can manipulate to change how a piece of software—a "program" or "application"—works. Programmers who have access to a computer program's source code can improve that program by adding features to it or fixing parts that don't always work correctly.
>
> Some software has source code that cannot be modified by anyone but the person, team, or organization who created it and maintains exclusive control over it. This kind of software is frequently called "proprietary software" or "closed source" software, because its source code is the property of its original authors, who are the only ones legally allowed to copy or modify it. Microsoft Word and Adobe Photoshop are examples

---

[40] http://www.theguardian.com/technology/2015/may/19/facebook-criticised-for-creating-two-tier-internet-with-internetorg-programme

[41] http://www.wired.co.uk/news/archive/2015-05/05/facebook-net-neutrality

[42] http://www.netneutrality.in/

[43] http://www.theguardian.com/technology/2015/mar/24/facebook-data-privacy-european-union-court-maximillian-schrems

[44] http://www.wsj.com/articles/google-advisory-group-says-limit-right-to-be-forgotten-to-eu-1423206470

[45] http://phys.org/news/2015-02-google-lip-privacy-conceal-profits.html

> of proprietary software. In order to use proprietary software, computer users must agree (usually by signing a license displayed the first time they run this software) that they will not do anything with the software that the software's authors have not expressly permitted.
>
> Open source software is different. Its authors make its source code available to others who would like to view that code, copy it, learn from it, alter it, or share it.…
>
> Some people prefer open source software because they consider it more secure and stable than proprietary software. Because anyone can view and modify open source software, someone might spot and correct errors or omissions that a program's original authors might have missed. And because so many programmers can work on a piece of open source software without asking for permission from original authors, open source software is generally fixed, updated, and upgraded quickly."[46]

Linux and Ubuntu are two examples of open-source operating software for computers, and open-source platforms, office suites, apps, and more exist.

While not all open-source platforms are created with the same political principles, they tend to buck the trend of high costs that come with proprietary software, and many open-source platforms place a deeper focus on online privacy, anonymity, collective access and ownership. Open source platforms may not appear to be as technically convenient, especially given the hegemony of the bigger firms' products, but the question is whether that extra energy spent in engaging these platforms is worth the trade-off of **having more secure, accessible tools that actually invest in a rights-based framework for users**.

Upholding rights online—including privacy, anonymity, expression and security—is connected to engaging with the development of the tools, the forums of governance, the terms and policies—from a perspective of economic power and collective ownership of ICTs and the internet. Engaging in these spaces strengthens the movement to reclaim the internet as a democratic space, both to resist abuse by governments, but also to resist corporate control.

Privacy:

The right to privacy and to exercise full control over our own data is a critical principle for a safer, open internet for all. Privacy is central to almost everything on the internet today—from ending harassment and violence online, to being able to retain control over the information you share, to being able to exercise agency in what part of your identity you choose to politicize and make public, or not, to resisting the convergence of mass surveillance and mass commodification in which we live.

Privacy is intimately connected to the issue of online security; the two are distinct, but their relationship reciprocal. In a basic sense, online security aims to stop unauthorized access to information, while making a choice about what information we do want to make public, to whom, and through what channels. What helps us differentiate between these forms of access is a consideration of privacy. For activists engaged in sensitive political work, state surveillance through technology has always been a strong point of concern, especially as the internet and digital technologies have expanded in the last 30 years. But the threat of surveillance by the

[46] http://opensource.com/resources/what-open-source

state is only one facet of online security and privacy, and threats from non-state actors are an increasing concern. Today, as networked technologies proliferate, along with the spread of online attacks—particularly against women, LGBTIQ persons, religious minorities, and various marginalized groups—privacy and security are becoming a more prominent concern for everyone. The questions we need to ask ourselves, are what aspects of our lives—online and offline—do we want to remain private, and how can we work to ensure that?

Companies are increasingly being held to account for their responsibilities to take action on upholding privacy online. Variances in companies' practices around the data they retain on users identities and online habits, how long that data is stored, and how secure that storage is, and what data they ensure is public—directly impacts state and non-state actors' abilities to access and intercept that data. Beyond surveillance and targeted attacks, companies' policies and stances on privacy have direct bearing on a host of other human rights in the day-to-day.

For example, Facebook's seemingly mundane "Real Name Policy" has come under scrutiny, because it forces people use their legally registered names on their profile pages—what FB terms 'real' or 'authentic' names (as if the names we choose to self-identify with aren't real or authentic). Facebook suggests that people are less likely to engage in abusive behaviour online when their 'real' name is attached to their own account. Even if the policy is well-intentioned, in practice Facebook's policy creates numerous obstacles to people's right to self-determination, privacy and security, and freedom of expression online.

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. People in sensitive occupations (e.g. sex workers, psychotherapists, doctors, lawyers) may also choose to use alternative names in online social networks to maintain confidentiality. In countries where freedom of expression is under threat in the mainstream media and public arena, citizens often turn to the internet as a sphere to write and express their concerns and critiques anonymously without fear of persecution.

Discussing Facebook's policy, 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**."[47]

In another article, Thoughtless Thought**,** a Native American and trans-identified person reflected on how Facebook's policy also serves the interest of a state model that has built itself on the erasure of indigenous identities, and refuses to recognize the rights to autonomy and self-determination.

> "I am Native American, transgender and undocumented. As an indigenous person I have been taught to suppress attributes of the indigenous by both my family, the social systems of Mexico and the socialization into the USA system that values homogeneity. Name(s) play into this, from dropping the accents of my given name as a child, or the outright refusal of the name given and taken as a young adult learning the Red Path; a name given by an elder to encapsulate the essence of who I was and am. Facebook is becoming more and more of an

[47] http://www.cnn.com/2014/09/16/living/facebook-name-policy/

> inescapable institution and it seems to be perpetuating the same systems of repression from which it was built."[48]

After an account has been suspended for violating the 'real name' policy, Facebook demands official government-issued IDs to 'verify' user identities.[49] Twitter similarly asks for government issued IDs in dealing with privacy complaints. This again raises questions on how these companies are implicated in mass government surveillance, and how their policies may actually decrease the privacy and security of their users online. On 26 March 2015, "The European Commission has warned EU citizens that they should close their Facebook accounts if they want to keep information private from US security services, finding that current Safe Harbour legislation does not protect citizen's data."[50]

While there may have been a trend to look at privacy as an ever more finite—if not seemingly futile—right online, social movements are not willing to give up on the right to privacy yet. In recognition of the need to reclaim privacy as a human right, especially in the age of online harassment, massive surveillance by nation states, and the implications of big tech firms in online insecurity—the UN Human Rights Council recently established the position of a UN Special Rapporteur on the Right to Privacy in March 2015.

Reflecting on importance of the mandate, Human Rights Watch highlights "A Special Rapporteur will be able to more systematically review government policies on interception of digital communications and collection of personal data; pinpoint policies that intrude on privacy without compelling justification; identify best practices to bring global surveillance under the rule of law; and help ensure that national procedures and laws are consistent with international human rights law obligations. The Rapporteur will also have the scope to explore private sector responsibilities to respect human rights under the UN Guiding Principles for Business and Human Rights in the specific context of digital information and communication technology."[51]

Agency:

The question of agency has a lot to do with sifting through the moral panics that govern the internet, and bringing contextual and nuanced specificity to policy-making. Agency is also about centring the voices and experiences of the intended beneficiaries of policies that seek to prevent harm and provide redress.

Moral panics often centre around the issue of content that is considered 'harmful content'. But as APC's 2011 EROTICS study asked, "What is "harmful content" on the internet? The definition is contestable, subjective and open to a range of interpretations, and the majority of interventions to combat it are mostly concerned with obscenity and child pornography. Sexual rights workers are troubled by the growing role of conservative forces – supported by religious extremists – and their attempts to encourage new legislation that would treat all online sexual exchanges as sexual predation and all adult content on the internet as pornography. This protectionist approach overshadows other important aspects of the internet that directly impact on internet users' lives and their ability to access vital information on sexuality, sexual health and sexual rights."[52]

---

[48] http://www.huffingtonpost.com/2015/03/27/facebook-authentic-identity-policy_n_6949318.html

[49] https://www.facebook.com/help/159096464162185

[50] http://www.theguardian.com/technology/2015/mar/26/leave-facebook-snooped-on-warns-eu-safe-harbour-privacy-us

[51] http://www.hrw.org/news/2015/03/16/why-un-special-rapporteur-privacy-matters

[52] http://www.apc.org/en/node/7904

Bringing nuance and specificity to the discussion allows us **to distinguish between consensual sexual acts**—that are consensually filmed, consensually photographed and consensually distributed online—**and those that are non-consensual, and thus a violation of fundamental rights.**

As the EROTICS study documented, using 'pornography' as a catch-all term for 'harmful content' on the internet tends to lead to policies and software development that results in censoring information related to sexuality in its entirety, including sexual health, sexual education, LGBTIQ rights. **What is often missing from the discussions on pornography are a focus on agency, consent, autonomy and choice around sexual acts and practices**—for adults as well as youth.

The question of how to enable children and youth to engage with the internet in ways that support their healthy psychological, emotional, and personal development and growth also centres on agency. This includes ensuring access to positive information about sexuality at critical times in their development—rather than leaving them without the analytical and practical tools to negotiate healthy sexuality, due to a fear of them accessing pornography or being subject to sexual predation online. **Children and youth need to be supported in knowing their rights, by bringing their voices and perspectives to the discussions and decisions about their experiences online.**

Digital Security as a Feminist Practice

> *"As feminists, we challenge the status quo. That comes with a risk. You expose yourself online. Digital security should therefore be on the feminist agenda."*
>
> *- Participant at the 2012 "Connect Your Rights: Strategic Global Dialogue"*[53]

> *"Being safe online is not only about protecting ourselves against governments and corporates but we need to secure our activism and identities from individual users"*
>
> - Jennifer Radloff, 2013

The Feminist Principles of the Internet were developed in a bid to imagine the kind of public spheres we want to see, on the internet and 'in real life'; and to ground discussions around policy advocacy to this end. What ran current throughout the discussions, especially when looking at how rights violations are increasingly happening online, was a need to engage with 'digital security' in order to build awareness on how to really develop and use ICTs in a way that encourages personal choice, privacy, agency, and freedom of knowledge and expression.

As the first quote above reflects, the reality is that feminist activists working for the rights of women, LGBTIQ people, ethnic minorities, and religious minorities particularly, are subject to intense violence, intimidation and harassment online. In 2013, APC conducted a global survey 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.[54] The report states

[53] http://www.apc.org/en/press/digital-security-becomes-key-concern-women-rights

[54] http://www.genderit.org/articles/survey-sexual-activism-morality-and-internet

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."[55]

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)[56]

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 offline raid were serious, and connected to the online activities of WONETHA and the online/offline lives of the communities they worked with:

> "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."'[57]

In the case of WONETHA, state actors were directly responsible for the attack; in the case of LACWHN however, the perpetrators were unknown—as is so often the case with digital attacks.

The continuum between offline and online threats are also evident when we look at the issue of technology-related violence against women and girls (VAW). Briefly, technology-related VAW can be defined as those forms of gender-based VAW that are committed through the use of

[55] Cited in http://agi.ac.za/sites/agi.ac.za/files/standpoints_digital_security_as_feminist_practice.pdf.

[56] Op Cit. p. 149

[57] Op. Cit.

ICTs. APC's research documenting women's lived experiences of tech-related VAW documented some of the following forms:[58]

- Taking and/or uploading and distributing intimate photos and/or videos without consent: the woman agreed that the photographs be taken for personal consumption, but did not consent to sharing the photographs; the girl/woman was unaware she was being videotaped during a sexual act, then the video was uploaded and distributed online.

- Altering photos/videos and uploading in pornography sites: a photo of the woman's face was attached to the naked body of another woman and later uploaded to pornography sites, then tagged with the woman's profession and city.

- Harassment: women receiving harassing comments, messages and texts, which often use sexualised insults.

- Stalking: activities monitored online.

- Blackmail/threats, often to force a women/girl to submit to rape and other forms of sexual violence: a girl receiving messages asking her to have sex or her family will be harmed; a woman threatened that her intimate photos will be made public unless she goes back to having a relationship with the perpetrator.

- Accessing and/or dissemination of private data: email account hacked; accessing a woman's social network account and messaging her contact list without her knowledge; leaking private documents and information to the public.

- Creation of fake profile/identity theft: profile containing the name and picture of the woman, and filling the profile page with derogatory descriptions.

- Gender-based hate speech and incitement to violence against women: calling for women to be murdered, or raped. Attacking women on the basis of their gender, sexuality and physical appearance.

- Child exploitation images and videos: children forced to pose naked and perform sexual acts using video-chat.

In 2006, the UN Secretary General Ban Ki-moon called for more attention to tech-related VAW, although it is only in recent years that governments and companies have finally began to take action to stop the unchecked proliferation of VAW online. Legislation has been brought in to make the distribution of private/intimate photos/videos without consent an offense, and companies have begun to update their Terms of Service and user policies to also reduce the amount of abuse that goes unchecked online.

More research is being conducted by civil-society to ensure governments and corporations take action on these issues—documenting women's experiences, and calling for improvements to the online security and privacy settings, as well as redress mechanisms, that are available to users. In February 2015, APC published a report that reviewed the terms of service of 21 internet intermediaries, and outlined various steps companies could take to improve the privacy settings,

[58] Namita Malhotra (2014) Good Questions on Technology-related violence against women, https://www.apc.org/en/pubs/good-questions-technology-related-violence. See also: http://www.genderit.org/resources/cases-women-s-experiences-technology-related-vaw-and-their-access-justice

security settings, and redress mechanisms available to users.[59] In May 2015, Women, Action, Media released a report exploring the kinds of online harassment that is reported specifically to Twitter, how the company responds, and what challenges users face in finding redress when reporting harassment.[60]

Working with governments and companies is an important strategy in building a culture of digital security, especially as many of the forms of violence above demand state accountability and corporate responsibility to prevent the spread of such violence. However as we have seen, state and corporate actors often undermine online security. Equipping individuals and communities with the tools and knowledge to take security into their own hands is an essential strategy in creating cultures of privacy and security online.

For individuals reflecting on this, exploring the connection between digital security and privacy is again important. Engaging with digital security as a strategy, means taking steps that could enable us as individuals to reduce the risk of being harassed or attacked online and offline. In some of the common forms of technology-related VAW mentioned above, risk could result from keeping private photos on your computer in an unencrypted file, or sending photos/videos unencrypted over email, online chat, or mobile chat apps—which makes it easier for others to hack, access and spread those photos around. Engaging in digital security is the process, the outcome of which greater (or less) privacy, depending on the steps you take for yourself.

As activists have highlighted, digital security is also an important consideration in creating solidarity movements, especially when it comes to activism online and the ways in which we tag, share, and spread information:

> "Digital security is a huge concern for WHRDs whose accounts are surveilled and hacked, whose whereabouts can be mapped through social media creating potential online and physical risks. It's important for all of us to pay attention to these issues, for our own protection and to make sure we don't put others at risk by tagging or posting about people who are vulnerable to threats and attacks – or who simply don't want to be tagged."[61]

In articulating a political framework of what we value and defining the change we want to see, a feminist approach to the internet flips the idea that we have to wait for our rights to be granted to us. Engaging with digital security, and the politics behind the tools we use and the actions we take, enables us to proactively challenge, interrupt and counter the move by states, companies and individuals that seek to undermine democratic participation and rights online.

[59] http://www.genderit.org/resources/impunity-justice-improving-corporate-policies-end-technology-related-violence-against-wo-0

[60] http://womenactionmedia.org/cms/assets/uploads/2015/05/wam-twitter-abuse-report.pdf

[61] http://www.genderit.org/feminist-talk/solidarity-imprisoned-activists-or-without-facebook