Digital security as feminist practice

Jennifer Radloff

In the beginning

For years communication rights activists encouraged women to get online, to use the new technologies that could be used to connect, mobilise, advocate and bring worlds together in quick and responsive ways. We lobbied via the Commission on the Status of Women (CSW), motivated for more language in Section J of the Beijing Platform, hosted workshops to teach women's rights activists to build websites, create and maintain mailing lists and manage digital archives of information. Discussions were included in regional and global conferences on information and communications technology (ICT) for development to insist that the gender digital divide had to be addressed. Gender was raised by women's rights activists in forums as technology was considered "the domain of men." Progressive institutions encouraged women to register for computer degrees and women started creating their own networks of women "techies."

These networks and organisations had as their core work the connection between activism and women's rights work. They were trying to demonstrate that ICTs were not necessarily the preserve of urban, middle-class, resourced people but that it was retrogressive not to engage with the new communication technologies. Although African feminists debated new communication technologies as potentially divisive to the movement, given unequal access and all the "offline" social exclusions which were replicated "online"; we are now seeing appropriation, adaptation and creative engagement with and the use of ICTs.

With the introduction of mobile phone technologies and their increasingly ubiquitous reach, more activists began to see the possibilities of using the internet and digital channels for advocacy, communication and information sharing. ICTs are now being used to advocate, to meet, protest, communicate and interact with new speed and with positive results.

In the mid-1990s we saw the creation of Women'sNet[1] in South Africa, Women of Uganda Network (WOUGNET)[2] in Uganda and Linux Chix Africa to name a few. Beijing +5 was a particularly interesting time. FLAMME, a network of African women online, committed to strengthening the capacity of women through the use of ICTs to lobby, advocate and participate in the Beijing +5 process was established. What was particularly powerful was the methodology used to develop this platform and network. Women from organisations across Africa gathered together and were trained in various technology skills whilst they built the website. The African initiative was part of a global network called WomenAction[3] whose mission it was to develop a communications network and information-sharing strategy to allow women in every world region to participate in and impact on the five-year review of the implementation of the 1995 Beijing Platform for Action.

And then comes social media

As Web2.0 (Wikipedia, 2013b) and social media use became commonplace, more and more women ventured online and took to digital communications easily. Blogs proliferated and citizen journalism became a popular way for women to write and self-publish on a range of issues. Facebook became not only a social connecting space but a way for activists to reach a wide audience at very little cost. Twitter enabled activists to share, almost in real-time, updates from meetings and conferences and include links to videos, websites and online petitions. People not able to attend important policy spaces could comment and include their opinions. YouTube facilitated the instant uploading of video clips which, for activists on the frontline, enabled violations to be made visible, often being picked up by mainstream media. Photo and music sharing sites gave rise to mashups (blending information from different sources) and challenged traditional notions of copyright. Online conferencing connected people in a virtual space and global organisations can now meet regularly using digital platforms. Skype and Voice Over Internet Protocol enables inexpensive voice and video connections which creates a sense of closeness and deepens virtual relationships.

A parallel phenomenon was the huge increase in the development of mobile applications (apps) which are being used for anything from checking weather, to banking (look at the quick uptake of M-Pesa) to safety apps etc. Cultural theorist, Donna Harraway, one of the first feminists to engage with the question of cyberspace and the implications of technological advances, published her seminal work "The Cyborg Manifesto" (Harraway, 1990). This prompted academics to begin theorising about the digital body as they saw virtual and physical identities becoming blurred. Women were using technology with more confidence and curiosity and forging spaces to discuss, theorise, train and share skills.

All of this excitement, connectivity and engagement with the positive and creative aspects of communications technology has led to many women using ICTs and social media confidently.

Big Brother's watching and there are monsters out there in cyberspace

What is now increasingly obvious is that the internet and digital tools and spaces have a profound impact on the magnitude of threats and have simultaneously broadened and increased the kinds of surveillance and harassment to which human rights defenders, both men and women, are being subjected. Attacks against women are invariably sexualised and women human rights defenders (WHRDs) are often more at risk online (as they are offline) than their male counterparts. Invariably WHRDs can experience more hostility, and at the same time lower levels of protection, compared to their male colleagues.

As Joy Liddicoat says:

> Because they are women, women human rights defenders face many unique threats and obstacles. The reasons include the nature of patriarchal systems for subordination of women, various socially constructed gender roles and norms, and religious and other fundamentalisms which seek to constrain women's public and private lives. This results in restrictions on women's autonomy, freedom of movement, freedom of expression and freedom of association, constraining their activism and their right to be human rights defenders. (Liddicoat, 2013)

Digital threats and combinations of offline and online issues are seriously compromising women's rights activists' freedom of expression and association and their right to participate actively as citizens. This happens in different ways, from monitoring of internet and email traffic, virus and spyware attacks, filtering, censorship, contenting blocking and receiving unwanted emails. These digital threats are not only happening online. Confiscation of computers and corruption of document archives can be as vicious and damaging as online attacks.

One such case which illustrates how offline digital attacks can be damaging occurred in Uganda on 7 May 2012 when police authorities in the Ugandan city of Gulu – a city located approximately 320 kilometres north of Kampala by road – raided a sex-worker drop-in centre. They arrested two staff and three members of the Women's Organisation Network for Human Rights Advocacy (WONETHA), the organisation that runs the centre.

The raid is in direct violation of the rights of WHRDs at WONETHA. "We find this to be an attack on WONETHA and sex workers' freedom of association, assembly, speech and expression, and we strongly protest against this," says a release by Macklean Kyomya, WONETHA's executive director. Beyond those rights, the raid also raises the question of digital security. One of the three members who was arrested recounts how the raid took place: "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).

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."

A more recent example of a digital attack against sexual rights activists occurred in Quito, Ecuador. 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 on 21 September 2013 immediately following the launch of several campaign activities including the #28SAbortoLegal social media campaign, part of advocacy initiatives for the September 28 Global Day of Action for Access to Safe and Legal Abortion and September 28 Campaign, Day for the Decriminalization of Abortion in Latin America and the Caribbean.

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)

It is not known who orchestrated and carried out this attack. It could have been state actors or non-state actors, individuals who often constitute into groups and regularly perpetrate sexualised attacks on women, usually through social media. "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" (Radloff, 2013).

In 2013 the Association for Progressive Communications 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: "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."

Many are familiar with the "Arab Spring" which saw thousands of Egyptians converging on Tahir square, using social media to organise, mobilise and report on army and police abuses. A popular platform for Egyptian women to report sexual harassment is Harassmap[10] which encourages women to speak up against harassers and report incidents via their map. But there is an underside. The "digital dangers" are multiple and there is now an increased focus on digital safety and secure online communications for women and human rights defenders and their organisations who are invariably the ones targeted for digital attacks. These attacks directed at activist organisations are now commonplace. Increasingly the internet, which was a revolutionary space, mostly ungoverned and open, is now a contested space with governments regulating through curtailing freedom of expression and association as they see the power it gives citizens.

To illustrate the lengths to which repressive states will go in using digital channels to surveil and track and trap activists is the Syrian Electronic Army

(Wikipedia, 2013a). It is aligned to the Syrian President and uses strategies such as Denial of Service attacks, defacement, spreading of viruses and malware (or malicious software) and creating fake Facebook profiles to entrap activists. Razan Ghazzawi, a Syrian blogger, campaigner and activist, was arrested by Syrian authorities and charged with spreading false information and weakening national sentiment. Although she was released after a month of imprisonment, she still could face 15 years imprisonment for her online activism.

Violence against women continues, this time mediated via technology

In the mid-2000s, communication activists started seeing cases of attacks against women via digital channels. Technology was being used as a medium of tracking, harassing and abusing women. Women leaving abusive relationships were tracked using geolocation or the abusive partner was reading their browsing history to find out where they were seeking advice or shelter. It wasn't only online that these abuses were proliferating. In Uganda there were two cases of women being murdered by their husbands who read SMS messages on their wives' mobile phones from unknown numbers and assumed they were being unfaithful (Fialova and Fascendini, 2011). In South Africa, young women are being raped with their rapists recording the violations using mobile phones and sending these abusive videos viral.

In 2012, seven young men were charged with gang-raping a mentally handicapped teenage girl and recording the act on a mobile-phone video that then went viral. This is not an isolated incident. Consensual and intimate photographs are circulated or morphed and manipulated when relationships end and one partner turns abusive. The internet does not forget and once an image or words are uploaded, the control of these is lost. Re-vicimisation is inevitable.

Technology-related violence against women is pernicious, frightening and often treated by police and institutions as "not that serious" as there is no physical evidence of harm. But the harm is profound and damaging. Technology related violence impacts women as seriously as other forms of violence. The frightening part is that often the attackers cannot be identified. In some instances it is state actors using surveillance and monitoring to track and infiltrate organisations or it could be non-state actors who want to take down the digital spaces occupied by activists.

A high-profile incident which illustrates the misogynistic and profoundly violent nature of technology-related violence is the Anita Sarkeesian case. Sarkeesian is a media critic and the creator of Feminist Frequency, a video webseries that explores the representations of women in pop culture narratives.[13] She was raising funds for a series of videos "exploring female characterstereotypes throughout the history of the gaming industry" (Sarkeesian, 2012). A campaign against Sarkeesian began which included calls for her to be gangraped and emails sent to her that contained images of her being raped by video game characters. It culminated in the "Beat Up Anita Sarkeesian" "game" which allowed gamers to punch her image until the screen turned red with her "blood." This harassment and blatant misogyny would be unacceptable offline but an online culture which is deeply male and accepting of this kind of violence, exposes how people do not take technology-related violence against women seriously.

Although generally, policymakers, police and the justice system lag behind in ways of apprehending and prosecuting abusers using technology to perpetuate violence and intimidation, there are some positive gains. South Africa recently introduced protection orders via the Anti-harassment Law "enabling South Africans to approach the courts for protection from sexual harassment – including harassment via SMS or email. Those hiding behind anonymity to send offensive SMSes will be able to be traced because the Act compels service providers to give the addresses and ID numbers of offenders when asked to do so by the courts" (SouthAfrica.info, 2013).

At the 57th session of the Commission on the Status of Women in 2013, the Association for Progressive Communications Women's Rights Programme (Association for Progressive Communications, 2013a) presented a statement on violence against women and information and communications technology. They pointed out that: "Since 2006, cyberstalking, online harassment, image manipulation, and privacy violations have increasingly become part of intimate partner violence and sexual harassment. This compromises women and girls' safety online and off-line in many countries (Fialova and Fascendini, 2011). These technology-related forms of violence against women cause psychological and emotional harm, reinforce prejudice, damage reputation, cause economic loss and pose barriers to participation in public life. Reporting and responses of these violations are generally limited and the harm and abuse are poorly understood" (Association for Progressive Communications, 2013b).

They further define how ICTs are changing the way that women experience violence. To summarise what they identify:

Anonymity: Widespread usage of digital technology has increased the potential for an abuser to remain anonymous.

Automation: The automation enabled by ICTs allows abusers to check their partners' mobile phones for SMSs, monitor social networking activity, check their browser history and log into their personal accounts with little effort in ways that do not require any special knowledge or skills.

Action at a distance: ICTs permit sexual harassers to send abusive messages from anywhere in the world to anywhere in the world. This makes it more difficult for a survivor to identify and take action against an abuser. This violation is a result of multiple actions done at a distance without contact with the victim.

Affordability: New ICTs have also significantly reduced the difficulty and cost of production and propagation of information. Anyone with a mobile phone can take and upload images or videos. One-to-many and many-to-many distribution through one click in an email application, Facebook or YouTube allow the images to be replicated thousands of times at no cost.

Propagation: In cyberspace settings abuse can happen every day, all year round. The internet "records everything and forgets nothing." The continuous traffic of harassing text and images makes it hard if not impossible to track down and stop further circulation. Moreover, the propagation of texts and images re-victimises women.

Taking back the tech!

Given the positive uses of ICTs in women's rights activism and the increased access to the digital tools that can create change, how do activists ensure their digital safety? At the core of it is the fact that we are as secure as the least secure person in our networks. Taking digital safety seriously is a responsibility each activist should take to heart. Digital security is now necessarily central to our activism. A mantra we should chant repeatedly! The first step is being personally safe. This will mean that your community will not be compromised through you. If you are part of an organisation or network, discuss issues of digital safety, create a policy for all members to adhere to.

The second step to to build knowledge around digital safety.

- Know how the internet works. This enables you to see where the potential threats come from.
- Keep your computer healthy. Condomise! Ensure that you regularly update your anti-virus package as viruses are dangerous and can contain spyware.

- Protect the data on your computer. Password protect your computer and encrypt sensitive data. Securely delete old files using Ccleaner.
- Search the internet securely using https everywhere and regularly clear your browsing history.
- There are many ways that people can gain access to our private accounts that never entail actual hacking, but one of the most common is our own poor password management. Find out what the risks are, and how to build better passwords and practice.
- Mobile phones are ubiquitous and used by many activists to connect, communicate and to mobilise. They can also be used to track and monitor someone's location or private communication. Learn how to better protect your privacy on mobile phones.
- Social media platforms can create vulnerabilities that we need to guard against. Make sure that you read the privacy statements of platforms such as Facebook and twitter. Do not upload compromising photos and never upload or tag people without their permission. Keep your passwords or passphrases safe, change them regularly and remember to logout once you have finished. (Radloff, 2013)

There are organisations that are developing toolkits and guides for activists to be safe online. Networks are organising digital security trainings and in most ICT capacity-building workshops, digital safety is a core module. Increasingly there is a realisation that there is no “one size fits all” approach that is effective in digital security. Particular communities face different threats. An example of this is the Tactical Technology Collective who have developed a toolkit for Lesbian Gay Bisexual and Transgender activists in the Middle East and North Africa Region. They have named this “security in context” in order to contextualise digital security threats for LGBT persons and human rights defenders from the Arabic-speaking countries, as well as the tools and tactics that can be used for overcoming them (Tactical Technology Collective, 2013). Sexual rights activists and those working to combat violence against women face particular, usually sexualised threats and need the strategies and responses to defend themselves from particular threats.

Feminist agency

Responses to the digital dangers are seeing activists finding new solutions and approaches to the threats. We know that new technologies are changing women's realities and they can be developed and appropriated to support and facilitate women's rights agendas (Feminist Tech Exchange, 2009). Examples include the Take Back the Tech campaign which "is a collaborative campaign that takes place during the 16 days of activism against gender-based violence. It is a call to everyone - especially women and girls - to take control of technology to end violence against women" (Take Back the Tech, no date). The #orangeday campaign organised by the Secretary-General's "UNiTE to End Violence against Women" campaign has proclaimed the 25th of every month as Orange Day to highlight issues relevant to preventing and ending violence against women and girls. ihollaback is a movement to end street harassment with platforms in 22 countries and 64 cities around the world documenting, mapping, and sharing incidents of street harassment.[3] Breakthrough, an organisation in India, is developing a data-driven digital toolkit to reduce gender-based violence to enable anyone to launch an effective anti-violence campaign.

As feminists we need to ensure that these digital dangers don't push us (and policymakers) towards a protectionist stance but that women and girls claim their agency and take back the tech!

Now be Safe! Resources on practical steps to defend yourself

Be Safe – Take Back the Tech resources
https://www.takebackthetech.net/be-safe

Digital Security First Aid kit for Human Rights Defenders
https://www.apc.org/en/irhr/digital-security-first-aid-kit

Security in a Box from the Tactical Technology Collective
https://securityinabox.org/

Endnotes

[1] Available at <http://harassmap.org/en/>

[2] Available at <http://www.feministfrequency.com/>

[3] Available at <http://www.ihollaback.org/>

References

Association for Progressive Communications. 2013a. *Communications and Information Policy – Africa*. Available at <https://www.apc.org/en/about/programmes/womens-networking-supportprogramme-apc-wnsp>.

Association for Progressive Communications. 2013b. *Statement to the 57th Session of the CSW Violence against Women and Information and Communications Technology*. Available at <https://www.apc.org/en/system/files/CSW%20APC%20statement%20FINAL%20VERSION.pdf>.

Feminist Tech Exchange. 2009. *FPT as a Critical Perspective & Analysis of Technology*. Available at <http://ftx.apcwomen.org/node/4>.

FD. 2012. "Digital Security: Drop-in Centre of Ugandan Sex Worker Organisation Raided", *Association for Progressive Communications*. Available at <https://www.apc.org/en/news/digital-security-drop-centre-ugandan-sex-worker-or>.

Fialova, K. and Fascendini, F. 2011. *Voices from Digital Spaces: Technology Related Violence against Women*. Available at <http://www.apc.org/en/system/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf>.

Haraway, D. 1991. "A Cyborg Manifesto: Science, Technology, and Socialist Feminism in the Late Twentieth Century", in *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge. Electronic version available at <http://www.egs.edu/faculty/donna-haraway/articles/donna-haraway-a-cyborgmanifesto/>.

Liddicoat, J. 2013. "Internet Rights are Women's Rights!", *GenderIT.org*. Available at <http://www.genderit.org/node/3456>.

Radloff, J. 2013. "How Activism Shapes your Experience of being a Citizen on the Internet", *GenderIT.org*. Available at <http://www.genderit.org/node/3832/>.

Sarkeesian, A. 2012. "Tropes vs Women in Video Games", *Kickstarter*. Available at <http://www.kickstarter.com/projects/566429325/tropes-vs-women-in-videogames>.

Sivori, H. and Zilli, B. 2013. Survey on Sexual Activism, Morality and the Internet". *GenderIT.org*. Available at <http://www.genderit.org/articles/survey-sexual-activism-morality-and-internet>.

SouthAfrica.info. 2013. *Anti-harassment Law Comes into Effect*. Available at <http://www.southafrica.info/services/rights/harassment-250413.htm#.Ume4ZRDpeSo>.

Tactical Technology Collective. 2013. *Security in Context: Tools and Tactics for the Arabic-speaking LGBT Community*. Available at <https://securityinabox.org/sbox/pdfs/SecurityinContext_en.pdf>.

Take Back the Tech. No date. *About the Campaign*. Available at <https://www.takebackthetech.net/page/about-campaign>.

Wikipedia. 2013a. *Syrian Electronic Army*. Available at <http://en.wikipedia.org/wiki/Syrian_Electronic_Army>. Last modified 21 November.

Wikipedia. 2013b. *Web 2.0*. Available at <http://en.wikipedia.org/wiki/Web_2.0>. Last modified 2 December.

Women Human Rights Defenders International Coalition. 2013. "WHRD IC Condemns Systematic Digital Harassment of LACWHN", *Association for Progressive Communications*. Available at <https://www.apc.org/en/news/whrd-ic-condemns-systematic-digital-harassment-lac>.