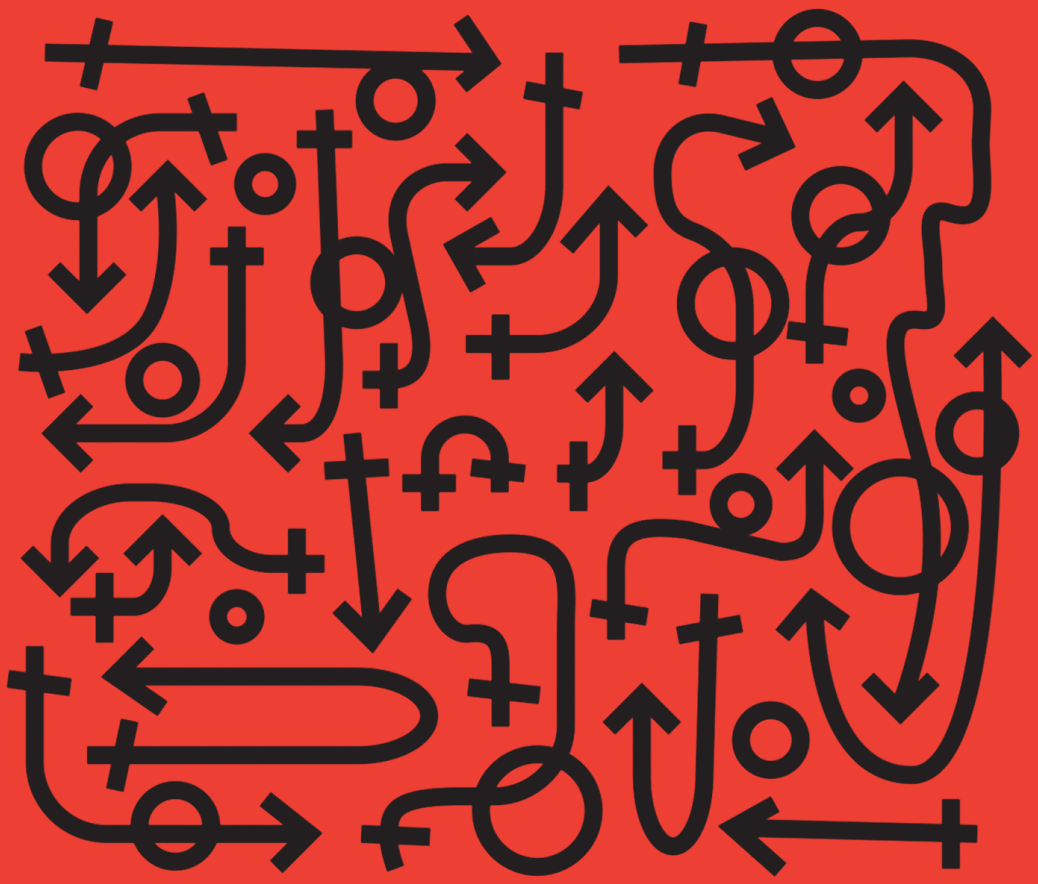
GLOBAL INFORMATION SOCIETY WATCH 2015

Sexual rights and the internet



Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch 2015
Sexual rights and the internet

Steering committee
Anriette Esterhuysen (APC)
Will Janssen (Hivos)

Coordinating committee
Monique Doppert (Hivos)
Valeria Betancourt (APC)
Mallory Knodel (APC)
Jac sm Kee (APC)
Nadine Moawad (APC)

Project coordinator
Roxana Bassi (APC)

Editor
Alan Finlay

Assistant editor, publication production
Lori Nordstrom (APC)

Proofreading
Valerie Dee
Stephanie Wildes

Graphic design
Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

Cover illustration
Matías Bervejillo

Financial support provided by
Humanist Institute for Cooperation with Developing Countries (Hivos)

Hivos

APC and Hivos would like to thank the Swedish International Development Cooperation Agency (Sida) for its support for Global Information Society Watch 2015.

Sida

Published by APC and Hivos
2015

Printed in USA

ISBN 978-92-95102-41-5
APC-201510-CIPP-R-EN-P-232

Feminist autonomous infrastructures

Sophie Toupin and Alexandra Hache
Media@McGill and Tactical Tech Collective
media.mcgill.ca and https://tacticaltech.org

Introduction

Women, feminists, and gay, lesbian, bisexual, trans*, queer and intersex (GLBTQI) individuals share common experiences online: they can easily become targets of online harassment, discrimination or censorship, be it by government, private actors or corporations. When trying to understand the relationship between gender, violence and technology, one should keep in mind that online violence is intrinsically linked with real-life situations. When bigotry, sexism and homophobic attitudes exist in societies, they will almost inevitably be amplified in the online world.

"Real" name policies, data mining, tracking and surveillance technologies have become so intertwined that the days when no one knew if you were a dog or a cyborg on the internet are largely over. In fact, the creation of an industry around the profiling of users, coupled with the centralisation and contraction of the internet, have led to a situation where it is not a safe space (if it ever was). In 1996 the Declaration of the Independence of Cyberspace announced the creation of "a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."[1] But nowadays it is all too common to see the work and voices of women, feminists and GLBTQI being deleted, censored and/or prevented from being seen, heard or read.

Much of this gender-based online violence happens on corporate social media platforms such as Facebook, Twitter, Reddit and the blogosphere, in addition to other non-profit online spaces such as Wikipedia. All of them involve large communities, which are led by a set of practices and policies. Despite the existence of certain rules that govern these spaces and because of certain practices, silencing, intimidation and/or discrimination continue. So far, responses from GLBTQI to violence have involved organised public shaming, doxxing of harassers,[2] feminist counter-speech, active research and documentation, awareness raising around privacy and security, advocacy for amendments to corporate terms of service, and lobbying of institutions contributing to the governance of the internet, among others. While these tactics are paramount to the embodiment of everyday forms of online resistance,[3] there is also a need to think about adopting strategies that are not only reactive, but also project us into the future we want. In other words, it is about dreaming and pre-figuring our technologies actively.

Proactive practices involve understanding what it means to take back the command and control of technologies by using, creating and maintaining our own ones and shaping our communication and technological infrastructures. Using corporate services such as Facebook or Twitter may be very convenient, and at times strategic because they are generally provided for free and because this is where the so-called critical masses are. But using them also means accepting their terms of service, which are primarily shaped by profit, and in which human rights and gender social justice still remain of negligible importance. When using these online services, we and our networks are at their mercy, which means we cannot fully control our data, social networks and historical memories (or traces) on the internet.

While the future of the internet often looks bleak, it is paramount to not only continue to investigate into the processes and governance structure of the internet, but to continue to build a communication and technological ecology that puts human well-being front and centre, rather than profit. What will happen when big data has its proper algorithms? What will be the combined relationships

1 Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. https://projects.eff.org/~barlow/Declaration-Final.html

2 Doxxing of harassers means searching for and publishing private information about a harasser on the internet with the aim of shaming the individual.

3 An example of the embodiment of everyday forms of resistance is that of feminist social media practices that resist rape culture by hijacking Twitter feeds and hashtags that blame victims and perpetuate myths and stereotypes.

between these algorithms and the Facebook project internet.org or the "Internet of Things", to name only two of the upcoming situations that will again redefine people's rights to privacy and free expression? When our data remain under corporate control, they can be sold or given to third parties to exploit, or they can be deleted or shut down. Ultimately, they become our digital shadows,[4] enabling others to track, profile and control our voices, opinions and expressions.

Part of the answer lies in developing, supporting and using not-for-profit, independent, privacy-aware and secure alternatives to corporate online services. Collectives such as Riseup, Nadir and Autistici/Inventati have been powered by hacktivist collectives for almost two decades now.[5] They have provided – through volunteer work and community contributions – valuable and basic online services such as email, mailing list servers, wikis, pads,[6] blogs and virtual private networks (VPN)[7] to activists all around the world. But where are the feminist tech collectives that design and maintain feminist autonomous infrastructures for feminists, queer and trans* people and activists at large? We also need to ask ourselves, why are those feminist tech collectives still so embryonic? And what does this tell us about the discrimination and violence happening when women and feminists do not control, own and manage the technological infrastructure they need to express themselves and act online?

Shaping autonomy within our technologies

One of the main constitutive elements of feminist autonomous infrastructures lies in the concept of self-organisation already practised by many social movements that understand the question of autonomy as a desire for freedom, self-valorisation and mutual aid. In addition, we understand the term technological infrastructure in an expansive way, encompassing hardware, software and applications, but also participatory design, safe spaces and social solidarities. Concrete examples of feminist autonomous infrastructures include the Geek Feminism Wiki,[8] developing specific technologies that tackle gender-based online violence, such as bots against trolls, and building feminist online libraries and feminist servers, but also enabling offline safe spaces such as feminist hackerspaces which allow feminist, queer and trans* hackers, makers and geeks to gather and learn with others.

When talking about these examples of feminist autonomous infrastructures, we recognise that none of them can be fully autonomous, but rather relative in their autonomy, as they still depend, for instance, on already existing communication networks and technologies designed by mainstream companies (such as computers, servers and access devices). Having said that, their autonomy is based on different governance models, the values they embrace and the principles they promote. If feminist autonomous infrastructures are diverse in scope and in shape, they do share in common a desire to proactively create the conditions for their autonomy while following an ethic of care[9] which is embedded into the active practice of social solidarities. Caring and recognising the importance of such infrastructures are two aspects that are central to attempt to address the cycle of technology that is rife with inequality from the production of technology, to its access, uptake, development and governance, until its end cycle. This intersectional and integrated approach to technology goes hand in hand with a feminist posture that does not shy away from addressing all forms of violence, whether it be online violence or the violence that is intrinsic in resource extraction or the factory and assembly line work that is gendered and raced.[10]

Recently, momentum has gathered around the building of feminist autonomous infrastructures. These initiatives are still in their embryonic stage, mainly representing a set of scattered and fragmented initiatives. Below we highlight two different examples – one addressing the need for physical safe spaces enabling women and feminists to gather and uplift their skills, and another addressing the slow-politics around the creation of feminist servers.

Breaking the circle of isolation by learning together

The Gender and Technology Institute[11] was organised by the Tactical Technology Collective and the Association for Progressive Communications (APC)

4 See "My shadow" by theTactical Technology Collective: https://myshadow.org/

5 For a more extensive list of autonomous servers visit: https://help.riseup.net/en/radical-servers and http://backbone409.calafou.org/participants/index.en.html

6 The following is a great activists etherpads that can be used: https://pad.riseup.net/

7 Riseup.net offers VPN to know more visit: https://help.riseup.net/en/vpn

8 To go to the Geek Feminism Wiki visit: http://geekfeminism.wikia.com/wiki/Geek_Feminism_Wiki

9 Adam, A. (2003). Hacking into Hacking: Gender and the Hacker Phenomenon. *ACM SIGCAS Computers and Society, 33*(4).

10 Nakamura, L. (2014). Indigenous Circuits: Navajo Women and the Racialization of Early Electronic Manufacture. *American Quarterly, 66*(4), 919-941.

11 To know more visit: https://tacticaltech.org/gender-tech-institute

at the end of 2014. The event brought together almost 80 participants and facilitators, mostly from the global South, to focus on some of the issues faced daily by women and trans* persons on the internet, to share strategies and tools for better protecting our privacy and security online, and to discuss how to spread knowledge and skills in our communities and organisations. Since then, the network has expanded, with different outcomes ranging from the creation of a collaborative online space enabling the documentation of the activities around privacy and digital security delivered by its members on the ground, to the production of a manual specifically addressing gender-related issues which also offers various strategies and tools for taking control of our online identities and learning how to shape safe spaces.

All these outcomes are informed by the stories and creative practices of women and feminist grassroots activists, located in 22 different countries, who are actively and creatively using and making technology to tackle gender-based online violence. Meanwhile they become digital security trainers, and privacy advocates, and they are helping others to understand how they can adopt safer and more joyful practices when engaging online and offline.

Eight months after its realisation, the Gender and Technology Institute has become an international informal network of support, a friendly resource space based on social solidarities that helps to break the circle of isolation.[12] This contributes to strengthening the technological autonomy of its participants and, by extension, women, feminists and GLBTQI individuals and organisations, in order to face the challenges and threats derivative of their use of the internet.

Feminist servers

A server can be defined as a computer connected to a network that provides services such as hosting files, websites and online services. Because all online resources are hosted on servers, they constitute a base for the internet as we know it. All servers are ruled by different terms of service, governance models and national legislation in relation to privacy and access to data by third actor parties (or "trackers") and are dependent on a variety of business models. This somewhat technical definition can obscure the possibilities for understanding the political aspect behind the setting up and management of a server.

In that sense, what would be the purposes[13] and principles[14] of a feminist server? Can feminist servers support women, feminists and GLBTQI in their fight for having their rights such as freedom of expression and opinion respected? Can we create trust among us to develop cooperative approaches to the management of those spaces of resistance and transformation? These were more or less the questions that a group of people interested in gender asked themselves during the first Feminist Server Summit[15] in December 2013 and at the first TransHackFeminist (THF!) Convergence[16] held in August 2014.

The discussions that emerged out of those meetings recognised that we do not yet have feminist tech collectives that design feminist autonomous infrastructures for the feminist, queer and trans* movement(s) and that this should become a priority.[17]

For example, two feminist servers that were dormant re-emerged during the THF! Convergence:

- The Systerserver project, which was originally launched in early 2000 by the Genderchangers[18] and the Eclectic Tech Carnival (/etc), and focuses on hosting online services such as etherpads and a voice over internet protocol (VoIP) application.
- The Anarcha server,[19] started by the TransHackFeminists from Calafou, an eco-industrial post-capitalist colony located in Catalonia. It hosts a mediawiki, a WordPress farm and a media publishing platform.

These feminist servers are composed of a loose coalition of women, queer and trans* from around the world, with some explicitly interested in hacking heteronormativity and patriarchy. They are also about demonstrating that it is possible to create safe spaces where the harassment of women, feminists and GLBTQI is not allowed and where all can learn about technology in a non-hierarchical and

12 One example is the International Feminist Hackathon Day (a.k.a. FemHack) held on 23 May 2015. To know more about this initiative see: www.f3mhack.org

13 For a history of where the desire for feminist servers arose read: Alarcon, S. et al. (2015, 30 April). Exquisite Corpse. *New Criticals*. www.newcriticals.com/exquisite-corpse/page-8

14 Following discussions at the Feminist Server Summit, Femke Snelting came up with a list that defines what a feminist server is, available here: http://esc.mur.at/en/werk/feminist-server

15 vj14.constantvzw.org

16 transhackfeminist.noblogs.org/post/2015/01/25/a-transhackfeminist-thf-convergence-report and anarchaserver.org/mediawiki/index.php/Main_Page

17 The theme of the second edition of the TransHackFeminist (THF!) Convergence is aptly titled "Error 404. Dissent Technologies Not Found": transhackfeminist.noblogs.org

18 A video about the GenderChangers is available at: https://vimeo.com/4090016

19 anarchaserver.org

non-meritocratic way. However, even if these server initiatives are inspiring to many, they still remain at the embryonic stage. Moreover, they do not consider themselves service providers; neither have they clearly decided to become stable and sustainable tech collectives providing hosting and online services to women, feminists and GLBTQI groups. In any case, they show that feminist servers are possible and that they should become a political aim for any organisations working in the field of gender social justice and GLBTQI rights – which should be concerned about achieving autonomy in communication and technological infrastructures, in addition to securing their data, social networks and historical memories on the web.

Conclusion

The targeting, silencing and censorship of women, feminists and GLBTQI people online has been and is being challenged in multiple ways. Women, feminists and GLBTQI people have been particularly creative in their everyday forms of resistance and their solidarities and care towards one another. While the initiatives outlined above are exciting, they do remain at an embryonic stage where only a few are able to participate. The reasons why so few initiatives exist ought to be at the core of a feminist analysis to understand how gendered technology actually is. Who is encouraged at a young age to tinker with technology? What kind of division of labour exists when it comes to technology? Why is the level of attrition so high for women in the tech industry?

While seriously considering the above, it remains that if we want to see the Feminist Principles of the Internet as formulated by APC become a reality, we need our own feminist autonomous infrastructures. To do so, we need to have feminist tech collectives that focus on providing these services. We need to be active in developing our expertise and that of the younger generation. But for that to happen we need the feminist and GLBTQI movement(s) to pay more attention to these issues, create more safe spaces to learn collectively, stop fearing technologies and decide collectively that we need to change gears to reshape our own communication and technological infrastructure. After all, freedom of expression is part of the feminist struggle and women, feminists and GLBTQI people can contribute by providing collectively the knowledge and means to ensure that their right to speak up remains accessible online, offline, and wherever and in any format where expression emerges.

GLOBAL INFORMATION SOCIETY WATCH 2015

Sexual rights and the internet

The theme for this edition of Global Information Society Watch (GISWatch) is sexual rights and the online world. The eight thematic reports introduce the theme from different perspectives, including the global policy landscape for sexual rights and the internet, the privatisation of spaces for free expression and engagement, the need to create a feminist internet, how to think about children and their vulnerabilities online, and consent and pornography online.

These thematic reports frame the 57 country reports that follow. The topics of the country reports are diverse, ranging from the challenges and possibilities that the internet offers lesbian, gay, bisexual, transgender and queer (LBGTQ) communities, to the active role of religious, cultural and patriarchal establishments in suppressing sexual rights, such as same-sex marriage and the right to legal abortion, to the rights of sex workers, violence against women online, and sex education in schools. Each country report includes a list of action steps for future advocacy.

The timing of this publication is critical: many across the globe are denied their sexual rights, some facing direct persecution for their sexuality (in several countries, homosexuality is a crime). While these reports seem to indicate that the internet does help in the expression and defence of sexual rights, they also show that in some contexts this potential is under threat – whether through the active use of the internet by conservative and reactionary groups, or through threats of harassment and violence.

The reports suggest that a radical revisiting of policy, legislation and practice is needed in many contexts to protect and promote the possibilities of the internet for ensuring that sexual rights are realised all over the world.

GLOBAL INFORMATION SOCIETY WATCH
2015 Report
www.GISWatch.org

APC Hivos

ISBN 978-92-95102-07-1