Contribution to the report of the Office of the High Commissioner on Human Rights on how to create and maintain the space for civil society to work freely and independently

Association for Progressive Communications (APC)
July 2015

Table of contents

1. Introduction

The Association for Progressive Communications (APC) is an international network and non-profit organisation working to empower and support organisations, social movements and individuals in and through the use of information and communication technologies (ICTs). Formed in 1990, we were granted category one consultative status to the United Nations Economic and Social Council (ECOSOC) in 1995.

APC welcomes the focus of the Office of the High Commissioner for Human Rights on practical recommendations to create and maintain the space for civil society to work freely and independently. The political and public environment for civil society, the free flow of information, space for dialogue and collaboration, long-term support and resources are continually evolving and under threat in many countries. In particular we view the internet and secure online communications as critical to creating and maintaining space for civil society to work freely and independently. APC works almost purely online, with staff and members in more than 60 countries and no central headquarters. Communicating day-to-day over the internet is essential to our work and increasingly to civil society around the world. Therefore, we focus our submission on the importance of access to an open and secure internet for civil society space.

2. Context

As Human Rights Council resolution 27/31 on civil society space recognised, civil society is indispensable for building peaceful, prosperous and democratic societies, including by holding governments and businesses accountable for furthering the public interest and protecting human rights. However, civil society space is being eroded by laws, policies and practices that do not respect human rights, with a disturbing trend of reprisals against civil society actors. For example, in Egypt the space for civil society has been almost completely eroded by repressive laws, including Law 107/2013, which has been used to imprison human rights defenders (HRDs) exercising the right to peaceful assembly, and to justify state violence that in January 2015 led to the killing of prominent woman human rights defender Shaimaa Sabry Ahmed El Sabbagh.[1]

Even in countries that have strong protections for human rights in some areas, new laws and official decrees have threatened the space for civil society to operate. In Ecuador, a 2013 presidential decree requires all NGOs operating in the country to obtain legal status, determined by officials of government ministries related to the NGOs' work. Officials have the authority to dissolve the organisation if they decide that it is “mov[ing] away from the objectives for which it was created,” or if the NGO “interferes with public policies that undermine national or external security of the state.”[2] In April 2015, India’s Ministry of Home Affairs cancelled the registration of 8,975 NGOs

[1]Marland, S. (2015, 30 January). WHRDIC condemns killing of Shaimaa El Sabbagh. *Women Human Rights Defenders International Coalition*. www.defendingwomen-defendingrights.org/2015/01/30/whrdic-condemns-killing-of-shaimaa-elsabbagh

[2]Human Rights Watch. (2013, 12 August). Ecuador: Clampdown on Civil Society. *Human Rights Watch*. https://www.hrw.org/news/2013/08/12/ecuador-clampdown-civil-society

working in the country, on the basis of violating reporting requirements under the highly criticised Foreign Contributions (Regulation) Act (FCRA).[3]

In contexts where civil society is constrained by legal, administrative, security and other factors, the internet assumes even greater relevance. Alarmingly, civil society's ability to use the internet as a space to work freely and independently, to mobilise and organise, is increasingly under threat by surveillance, censorship, and digital security threats by state and non-state actors. Threats to civil society online are not isolated to the digital environment; rather there is a continuum of offline and online threats, and vice versa. For example, digital surveillance of HRDs can lead to their arbitrary detention, and interrogation of HRDs can result in the compromise of their files, social media accounts, and networks, making it impossible for them to do their work freely or independently, online or offline.

3. Examples and illustrations of ways to maintain space for civil society to work

The internet and other technologies are critical for civil society in many respects, including *research, advocacy, network building, capacity development, strategic communications and outreach, and financial, administrative and fundraising work*. As noted above, internet access can be an especially critical tool when offline spaces for civil society are being eroded due to regressive legal and security situations, as well as societal and cultural barriers. Civil society groups and individuals most at risk for their activism, such as those espousing minority or dissenting views or beliefs, including criticism of the government; HRDs, including those working on sexual orientation and gender identity and expression (SOGIE), and sexual rights activists; minority rights groups, environmental activists and others, are turning towards the internet for their work.

Preliminary findings from APC's global EROTICS survey of networks of gender and sexual rights activists, scholars and policy makers found that most respondents declared a need for the internet in their work: 44% thought it would be difficult, and 46% said it would be impossible, for them to work without it.[4] Practically all respondents attributed some degree of importance to the internet in their work on sexual rights (only 1% said it was not useful in any way). Most respondents found the internet useful to share information (87%) and search for information (73%), while almost half of the sample also found it useful for public action and support (47%) – which roughly coincides with the 49% who work on raising public awareness or campaigning for rights. A significant 37% of this sample of gender and sexuality activists and intellectuals declared that the internet allows groups to network in safer conditions than face-to-face, and 26% thought that it allows dialogue between people with diverse opinions.

In Indonesia, the internet has been an essential tool to create space for individuals discriminated against based on SOGIE to connect, share information and organise safely to advocate for their rights. Institut Pelangi Perempuan (“Women Rainbow Institute”, IPP),[5] a lesbian, bisexual and

[3]International Service for Human Rights. (2015, 26 May). India: End legal restrictions against civil society. *International Service for Human Rights*. www.ishr.ch/news/india-end-legal-restrictions-against-civil-society

[4]erotics.apc.org/research/survey-sexual-activism-morality-and-internet

[5]www.pelangiperempuan.or.id

transgender youth organisation based in Jakarta, uses ICTs as a medium for community organising.[6] IPP started a mailing list in 2005 with lesbian, bisexual and transgender youth, which later transformed into an online discussion forum and then into an organisational website. Visitors to the website contact IPP "to extend their network, consult IPP, or participate in their activities by becoming volunteers at IPP."[7]

The internet is also an important space for individuals and communities to organise peaceful demonstrations in response to human rights violations, particularly in contexts where offline demonstrations are dangerous. When 145 people, including 132 schoolchildren, were killed at an Army Public School in December 2014 in Peshawar, Pakistan, an Islamabad cleric refused to condemn the attack. A group of activists, politicians and students gathered in front of the mosque of this cleric, Lal Masjid, and using the hashtag #ReclaimYourMosque on Twitter sparked a national movement with protests in Karachi, Lahore, Sialkot and Sargodha.[8] Gathering in front of mosques in Pakistan can be extremely dangerous, and one organiser received a threatening phone call to halt the demonstration.[9] However, the social media campaign that developed was able to create enough public attention and pressure that Lal Masjid's deputy *khateeb* along with representatives of the federation of seminaries joined the civil society activists to condemn the massacre.[10]

Civil society in India is using the internet as a platform to organise online events and campaigns, reach the masses, and respond to government circulations and policy drafts. For example, SavetheInternet.in is an Indian web petition portal started in 2015 to support the principle of net neutrality in India. Due to this mass campaign, one million emails were sent to the Telecom Regulatory Authority of India (TRAI) as of 23 April of this year, demanding net neutrality in India.[11]

The internet is not only an important tool for civil society organisations for their internal management and fundraising; sometimes there is also a requirement by the government to use the internet in order to meet registration regulations. The same controversial new law in India mentioned above, the FCRA,[12] includes guidelines for NGOs to maintain their records and utilisation of FCRA funds electronically. These guidelines make access to the internet and related technologies an imperative for NGOs, requiring investments in infrastructure and education.

---

[6]Institut Pelangi Perempuan. (2014). *Queering Internet Governance in Indonesia*. erotics.apc.org/sites/erotics.apc.org/files/queering_internet_governance_in_indonesia_final_research_book_.pdf

[7]Ibid., p. 20.

[8]Rezwan. (2014, 21 December). Pakistanis Say #ReclaimYourMosques From Radicalism in Rare, Bold Protests. *Global Voices*. globalvoicesonline.org/2014/12/21/pakistanis-say-reclaimyourmosques-making-a-rare-bold-statement-against-taliban-apologists-and-extremists-everywhere

[9]Dawn. (2014, 22 December). Lal Masjid protest activist receives threatening phone call. *Dawn*. www.dawn.com/news/1152467

[10]Junaidi, I. (2014, 21 December). Lal Masjid tries to ease out pressure. *Dawn*. www.dawn.com/news/1152222

[11]Tech2. (2015, 24 April). Net Neutrality deadline: Trai receives over million emails from netizens asking to save the Internet. *Tech2*. tech.firstpost.com/news-analysis/net-neutrality-deadline-trai-receives-over-million-emails-from-netizens-asking-to-save-the-internet-264548.html

[12]mha1.nic.in/pdfs/draftamendment_170615.pdf

4. If there are limitations, how do you continue to carry out your activities

4.1 Limitations

Surveillance, censorship and digital security threats by state and non-state actors are limiting civil society's ability to use the internet as a space to carry out its work freely and independently.

Surveillance

While government surveillance is often justified as a necessary tool to combat terrorism and threats to national security, broad and ill-defined notions of national security have justified the surveillance of civil society in many parts of the world. From Azerbaijan and Belarus to the United Kingdom and United States, surveillance of civil society is well-documented.

Digital surveillance has a chilling effect on civil society's ability to use the internet as a space to organise, share information, and mobilise. It leads to arrests, compromises networks of civil society, and undermines trust in the technology itself among activists.

To highlight just one case, in Malaysia online democratic space is shrinking as a result of repressive laws and policies of government surveillance, investigation and selective prosecution of internet users, HRDs, opposition lawmakers, students and academics. Reprisals for statements, publications and comments online have increased dramatically since the 2013 general elections, with amendments to the 1948 Sedition Act that confer power on the Malaysian Communications and Multimedia Commission (MCMC) to investigate, monitor and perform surveillance on internet content and users and restrict user access to electronic devices.

With the increasing international outrage in response to revelations of mass surveillance, we have observed a disturbing trend of governments that target HRDs and others in civil society justifying their surveillance practices as “targeted surveillance” while denouncing mass surveillance carried out by other governments.

Censorship

Blocking, filtering and censoring online content, including websites of human rights organisations, pose a serious threat to the space for civil society to work freely and independently.[13] The internet can be a critical tool, and in some contexts, the only tool to access certain types of information that is otherwise outlawed or unavailable. Online censorship limits the ability of civil society to raise public awareness, engage in advocacy, and also to conduct research. Beyond censorship of content, the blocking and filtering of social media platforms and other sites that allow for online networking, campaigning and other forms of advocacy online and offline, are an enormous challenge to civil society.

An extreme form of censorship, which unfortunately can be observed in many countries, is the cutting off of entire parts of communication networks, in the form of disruptions and blackouts. These measures are often introduced at times of political and social unrest specifically to disrupt the work of civil society. A recent joint statement by independent experts on freedom of expression

[13]For examples of online censorship see the Open Net Initiative: https://opennet.net

from the United Nations, the Organization for Security and Co-operation in Europe, the Organization of American States and the African Commission on Human and Peoples' Rights noted that "Filtering of content on the Internet, using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law."[14]

Online threats

Civil society and HRDs are increasingly facing online attacks as a result of their work. Hacking or defacement of websites, compromising of individual users' accounts, distributed denial of service (DDoS) attacks, and man-in-the-middle attacks are all examples of the types of online threats that civil society faces online. To give an example from a coalition partner in the Women Human Rights Defenders International Coalition, the website of the Latin America and Caribbean Women's Health Network (LACWHN) was hacked in September 2013 following the launch of campaign activities for safer abortions and reproductive health. The website hacking is indicative of the serious threat that online attacks pose to sexual and reproductive rights activists and a severe challenge to their ability to provide information and communicate, as well as a threat to the right to information on health and bodily integrity.[15]

4.2 How does civil society continue to carry out its work?

In order to continue carrying out work in the face of surveillance, censorship and online threats, best practices for civil society include using anonymity and encryption tools, such as pretty good privacy (PGP) email encryption; virtual private networks (VPNs); proxy or onion routers (such as Tor); off-the-record (OTR) private chat applications such as Cryptocat; instant messaging services such as Jabber and Pidgin; and mobile apps like TextSecure and Telegram. Different tools will be more effective and appropriate for civil society working in different contexts. We provide links to various resources and guides below.

4.3 Practical recommendations for creating and maintaining spaces for civil society

In the interest of providing practical recommendations for creating and maintaining spaces for civil society online and offline, we suggest the following for OHCHR and other stakeholders' consideration:

- OHCHR should continue its work within human rights bodies and mechanisms to create and maintain spaces for civil society to work freely and independently, including by: supporting HRDs and civil society under threat; documenting laws, regulations and practices that limit civil society space; and providing guidance to states on how to improve laws, regulations

[14] https://www.article19.org/resources.php/resource/37951/en/joint-declaration-on-freedom-of-expression-and-responses-to-conflict-situation

[15] WHRDIC. (2013, 14 October). WHRD IC condemns systematic digital harassment of LACWHN. *APC.org*. https://www.apc.org/en/node/18613; see also APCNews. (2012, 11 May). Digital Security: Drop-in centre of Ugandan sex worker organisation raided. *APCNews*. https://www.apc.org/en/news/digital-security-drop-centre-ugandan-sex-worker-or

and practices to better protect spaces for civil society so that they are in line with international human rights standards.

- OHCHR and the broader UN system should revise their communication practices and tools and invest resources in enhancing security and confidentiality for civil society through digital communications. As UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye recommends in his recent report,[16] particular attention must be paid by human rights protection mechanisms when requesting and managing information received from civil society and witnesses and victims of human rights violations.
- States, international organisations, corporations and civil society groups should systematically promote access to encryption and anonymity without discrimination and provide digital literacy and capacity building on the above-mentioned technologies and strategies to create and maintain civil society space online.
- States should not place restrictions on strong encryption and anonymity. As Kaye recommends, states should avoid all measures that weaken security online, such as backdoors, weak encryption standards and key escrows. In addition, states should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. As previously mentioned, these measures often justified as necessary to maintain national security are often used to target civil society. And even if civil society is not specifically being targeted, weakening encryption standards puts everyone's security at risk.

5. Useful links, tools, resources, guides

5.1 Digital security resources

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

APC's Take Back the Tech Safety Toolkit: https://www.takebackthetech.net/be-safe/safety-toolkit

APC's Take Back the Tech strategies against blackmail, cyber stalking and hate speech: https://www.takebackthetech.net/know-more

Tactical Tech's Security in a Box: https://securityinabox.org

Online Directory of Urgent Responses for WHRDs from the Association for Women's Rights in Development and the WHRD International Coalition: https://urgent-responses.awid.org

Electronic Frontier Foundation's Surveillance Self-Defense: https://ssd.eff.org/en

Riseup's Security Resources: https://help.riseup.net/ca/security/resources

Deflect – a free service for human rights defenders and civil society organisations that mitigates distributed denial of service (DDoS) attacks and keeps websites operating: https://deflect.ca

[16]Kaye, D. (2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*. ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

5.2 Resources for civil society working with ICTs

Closer than Ever: A guide for social change organisations who want to start working online: https://www.apc.org/en/news/closer-ever-guide-social-change-organisations-who-

APC’s contribution to the CIVICUS report on the State of Civil Society 2013, focusing on the role of information and communications technology (ICT) in 2012/13 from a civil society perspective: https://socs.civicus.org/wp-content/uploads/2013/04/2013StateofCivilSocietyReport_full.pdf

APC's Internet Rights Charter: https://www.apc.org/en/node/5677

APC's Feminist Principles of the Internet: https://www.genderit.org/articles/feminist-principles-internet