The rights to freedom of peaceful assembly and of association in the digital age: Submission to the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association by the Association for Progressive Communications (APC)

Association for Progressive Communications (APC)
January 2019

Table of contents

1. Introduction

The Association for Progressive Communications (APC) is an international network and non-profit organisation founded in 1990 that works to help ensure everyone has affordable access to a free and open internet to improve lives, realise human rights and create a more just world. As an organisation that has worked at the intersections of human rights and technology for nearly three decades, we welcome the focus of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (FoAA) in his next report on the rights to freedom of peaceful assembly and association in the digital age.

For those who have access to the internet, it is becoming increasingly difficult to imagine life without it. Meaningful use of the internet[1] has become a necessary precondition for exercising human rights, online and offline, including the rights to FoAA. But not everyone has such access. When considering challenges and opportunities concerning FoAA in the digital age we urge the Special Rapporteur to keep in mind that meaningful access to the internet is still out of reach for around half of the world's population.[2] As the internet becomes more ubiquitous, less is being heard from those who are unconnected – the less wealthy and more marginalised – who are unable to exercise their rights on the same footing as those who are connected. This can create new forms of exclusion and amplify existing ones. Disparities in internet access mirror other disparities that women, in particular, face in society, be they based on location, economic power, age, gender, racial or ethnic origin, social and cultural norms, education, or other factors. **Those who do not have access are doubly excluded: excluded from the "new" opportunities to exercise their rights to FoAA online, and also excluded from the "old" analogue world they used to have access to – even if imperfectly – because so many of those services and opportunities are increasingly only available online.**[3] We therefore encourage the Special Rapporteur to take an intersectional approach when considering challenges to FoAA in the digital age. Intersectionality as a framework questions and gives visibility to exclusions, powers and privileges that emerge as a result of gender, race, ethnicity, class, and other social and cultural hierarchies.

While limitations/restrictions on FoAA are relatively well defined, if not always respected, there is not yet a common understanding of protections for and permissible restrictions on FoAA online. As a result, states and internet intermediaries place arbitrary and excessive limitations on the exercise of FoAA in online spaces. Guidance from the Special Rapporteur reaffirming the right to FoAA in online spaces and defining limitations consistent with international human rights law and best practices in this regard would be immensely valuable for safeguarding FoAA in the digital age.

In addition, it is increasingly difficult to distinguish between the online and offline dimensions of FoAA, both because digital technologies are more integrated into people's lives, including in how they exercise FoAA, and because states are deploying digital technologies for a range of governmental functions that

[1]"Meaningful internet access" should be construed as pervasive, affordable connectivity (of sufficient quality and speed) to the internet in a manner that enables the user to benefit from internet use, including to participate in the public sphere, exercise human rights, access and create relevant content, engage with people and information for development and well-being, etc., irrespective of the means of such access (i.e. whether via a mobile or other device; whether through private ownership of a device or using a public access facility like a library).

[2]The International Telecommunication Union estimates that in 2018, 51.2% of the global population, or 3.9 billion people, had use of the internet. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[3]APC. (2016). *Ending digital exclusion: Why the access divide persists and how to close it*. Association for Progressive Communications. https://www.apc.org/en/system/files/APC_EndingDigitalExclusion.pdf

impact on FoAA. For example, the use social media can enable assemblies to continue over time and across geographies to build longer-term sustainable movements. During offline assemblies, information and communications technologies (ICTs) are used by both citizens and media to monitor how authorities behave and to document abuses, and by law enforcement authorities to maintain public order, but can be abused to profile activists, infiltrate associations, and undermine movements. Data-intensive systems, like smart cities, can be used for surveillance and to control people's movements and minimise the impact of protests, strikes and other forms of peaceful assembly. These are just a few examples of how, in today's world, rights are often exercised along a continuum between online and offline spaces, to underline that it is critical to pay attention to how digital technologies are developed, designed and regulated in order to better understand how to safeguard FoAA in the digital world.

2. Freedom of assembly and association online in international standards

The UN Human Rights Council (HRC) and several human rights treaty bodies[4] have affirmed the applicability of human rights in the digital environment. For example, the HRC established that the same rights that people have offline must also be protected online.[5] This applies to the right to freedom of peaceful assembly and association (FoAA) as enshrined in Article 20 of the Universal Declaration of Human Rights and guaranteed in Article 21 (assembly) and Article 22 (association) of the International Covenant on Civil and Political Rights (ICCPR). Any restrictions placed on the exercise of the right to FoAA must not impair the essence of the right, must be prescribed by law and must be proportionate and "necessary in a democratic society".[6] Though states are primarily the duty bearers to enforce and protect these rights, private sector actors, like internet companies, must uphold their responsibility to respect FoAA through any medium.[7] This includes the internet.

The current and former UN Special Rapporteurs on FoAA and other UN bodies have already recognised the significance of ICTs in facilitating FoAA online and offline. In their reports, the former Special Rapporteurs on FoAA recognised the increased use of the internet, in particular social media, and other ICTs as basic tools which enable individuals to organise peaceful assemblies and associate with one another. They also noted various restrictions placed on these rights exercised online.[8] Furthermore, both the HRC and UN General Assembly (UNGA) have reinforced the need to promote and protect FoAA online with thematic resolutions. For example, with its 2013 resolution on "The rights to freedom of peaceful assembly and of association", the HRC reiterated "the important role of new information and communications technologies in enabling and facilitating the enjoyment of the rights to freedom of peaceful assembly and of association, and the importance for all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries."[9] The 2018 HRC resolution on "The promotion and protection of human rights in the context of peaceful protests" went further, noting that "although an assembly has

[4]For example, Human Rights Committee General Comment 34 CCPR/C/GC/34 (2011) and CEDAW General Recommendation 35 CEDAW/C/GC/35 (2017).

[5]For example, UN HRC resolutions on "The promotion, protection and enjoyment of human rights on the internet" 20/8 (2012), 26/13 (2014), 32/13 (2016), and 38/7 (2018).

[6]A/HRC/20/27, para 16, para 39-42.

[7]Ruggie, J. (2011). *UN Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*. www.ohchr.org/EN/Issues/TransnationalCorporations/Pages/Reports.aspx

[8]Some examples include A/73/279 (2018), A/72/135 (2017), A/68/299 (2013), A/HRC/38/34 (2018), A/HRC/35/28 (2017), A/HRC/31/66 (2016), A/HRC/29/25 (2015), A/HRC/26/29 (2014), A/HRC/23/39 (2013) and A/HRC/20/27 (2012).

generally been understood as a physical gathering of people, human rights protections, including for the rights to freedom of peaceful assembly, of expression and of association, may apply to analogous interactions taking place online."[10] The resolution also expresses concerns about various measures to unduly restrict internet use, such as the deployment of disinformation and the prevention of internet access at key political moments (generally referred to as "shutdowns"), and their impact on the ability to organise and conduct assemblies. Finally, the resolution calls on all states to "refrain from and cease measures seeking to block internet users from accessing or disseminating information online, when in violation of international human rights law."A 2018 UNGA resolution on "Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association"[11] reinforced HRC resolutions and further highlighted the online dimensions of these rights by:

- Expressing grave concern about the growing "threats, risks and dangers faced by all individuals, online and offline, for exercising their rights to peaceful assembly and freedoms of expression and association, particularly members of civil society, including but not limited to human rights defenders, including women human rights defenders, indigenous human rights defenders (…)."
- Stressing the responsibility of member states and encouraging "respect to all individuals exercising their right to peaceful assembly and freedoms of expression and association, online and offline, in cases of threat, harassment, violence, discrimination, racism and other violations and abuses committed against them."
- Calling upon all states to ensure "that the same rights that individuals have offline, including the right to freedom of expression, peaceful assembly and association, are also fully protected online" and refrain from "Internet shutdowns and content restrictions on the Internet that violate international human rights law."

Aside from the above-mentioned resolutions specifically focused on FoAA, the HRC and UNGA resolutions on the right to privacy in the digital age contribute to international standards concerning FoAA online.[12] Together, the resolutions express concern that violations or abuses of the right to privacy, such as unlawful or arbitrary surveillance, interception of communications, and collection of personal data, can interfere with the right to FoAA, and call on states not to interfere with the use of technical solutions to secure and protect the confidentiality of digital communications – like encryption and anonymity technologies, which can be important to ensure the enjoyment of freedom of FoAA – with any restrictions thereon complying with states' obligations under international human rights law. Additionally, the HRC resolution on the promotion, protection and enjoyment of human rights on the internet recognises that for the internet to remain global, open and interoperable, it is imperative that states address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of association, and calls on states to address security concerns on the internet in accordance with their international human rights obligations to ensure the protection of all human rights online, in particular, among others, freedom of association.

[9]Human Rights Council. (2013). The rights to freedom of peaceful assembly and of association, A/HRC/RES/24/5. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/24/5

[10]Human Rights Council. (2018). The promotion and protection of human rights in the context of peaceful protests, A/HRC/RES/38/11. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/11

[11]#UN General Assembly. (2018). Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association, A/RES?73/173. http://undocs.org/A/C.3/73/L.41/Rev.1

[12]Human Rights Council. (2017). The right to privacy in the digital age, A/HRC/RES/34/7 and UN General Assembly. (2018). The right to privacy in the digital age, A/RES/73/179.

3. Definition of FoAA online and distinction with offline exercise

Based on international standards, FoAA refers to the rights of all persons to join together with other individuals and engage in activities related to civil, political, economic, social and cultural rights. It also refers to the right to be part of or form associations. While freedom of peaceful assembly and freedom of association are considered two separate rights,[13] it is essential to consider how the two rights are closely interrelated and interdependent.[14] An "assembly" is an intentional and temporary gathering in a private or public space for a specific purpose. It therefore includes demonstrations, inside meetings,[15] strikes, processions, rallies or even sits-in.[16] An "association" refers to any groups of individuals or any legal entities that come together in order to collectively act, express, promote, pursue or defend common interests.[17] These rights can be enabled or enhanced through new technologies, including the internet, and the limitations to these rights when exercised through new technologies must be in accordance with international human rights law. ICTs can offer a unique and enabling space for the exercise and enjoyment of FoAA, making it possible for persons who may not be willing or able to take part in physical assemblies or associations to exercise these rights. ICTs can also be used to limit access to the exercise and enjoyment of FoAA and can create new barriers for those who are without meaningful use of the internet.

FoAA online is the use of ICTs to exercise FoAA either wholly in online spaces or in conjunction with offline spaces. We consider FoAA online to have two dimensions: one in which the exercise of FoAA is carried out wholly online, such as online petitions, protests and groups – including virtual protests and "hacktivism";[18] and one in which ICTs are used to support, enable, enhance and facilitate FoAA online and offline[19] – for instance, the mobilisation of people through online posts to gather in offline spaces and extend the conversation on the agenda. In many instances, FoAA is exercised online even after the physical exercise of it ceases to exist.

Associations or associating online refers to the act of forming groups, including informal ones, online, with or without moderators or group leaders.[20] Peaceful assembly online refers to an intentional and temporary gathering in a private or public online space for a specific purpose. While it is established that human rights standards apply in online spaces, often ICTs enable new expressions of rights which do not

[13]A/HRC/20/27.

[14]A/72/135.

[15]Referring to private meetings in private spaces.

[16]A/HRC/20/27.

[17]Ibid.

[18]According to ARTICLE 19, "hacktivism" or "hacktivism" is defined as "a collective action of technologically-skilled individuals through the use of digital technologies to protest without gathering in person." Most acts in this category are considered a form of "electronic" civil disobedience due to related violation of the law. The organisation argues that international law allows for consideration of these actions as forms of freedom of expression and assembly. See the ARTICLE 19 for their background paper on the right to protest: https://right-to-protest.org/wp-content/uploads/2015/06/Right-to-Protest-Background-paper-EN.pdf

[19]Venkiteswaran, G. (2016). *Freedom of assembly and association online in India, Malaysia and Pakistan: Trends, challenges and recommendations*. Association for Progressive Communications. https://www.apc.org/en/pubs/freedom-assembly-and-association-online-india-mala

[20]Based on former UN Special Rapporteur Maina Kiai's definition, "Association refers, inter alia, to civil society organisations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, foundations or even online associations as the Internet has been instrumental, for instance, in facilitating active citizen participation in building democratic societies." See Kiai, M. (2012). Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-27_en.pdf

have direct parallels with traditional expressions of those rights. Freedom of assembly carried out wholly online is one of these cases. As HRC resolution 38/11 noted, although an assembly has generally been understood as a physical gathering of people, human rights protections, including for freedom of assembly, may apply to analogous interactions taking place online.[21] Some examples of freedom of assembly carried out wholly online include people gathering in an online social media platform to jointly protest a law, policy, or act of injustice. While offline assemblies may be restricted to physical spaces and limited to the participation of individuals present in that space in real time, online assemblies can be more fluid and witness the simultaneous and extended participation of individuals situated in different physical spaces, yet meeting in the online space for a common purpose. Other examples of the simultaneous use of digital technology to engage in collective action, such as "virtual sit-ins", distributed denial of service (DDoS) attacks, website redirects or defacement, Twitter storms,[22] and coordinated website blackouts or changing of profile photos, are emerging as a form of protest or awareness raising.

There are also a number of forms of freedom of assembly which include both online and offline dimensions: for example, the acts of coordinating, mobilising, organising, gathering, planning or meeting on platforms available online such as instant messaging, voice over internet protocol (VoIP), chat applications, email groups and mailing lists, among others.[23] Another key contribution of ICTs is providing associations the ability to undertake actions and sustain them online for prolonged periods, especially in relation to online campaigns and targeted advocacy aimed at different stakeholders. Online and offline spaces can no longer be regarded as distinct and disconnected; rather, like people's lives, they must be viewed as a continuum.

As a result, the exercise of FoAA online may take different and evolving forms, which in spirit are similar to the exercise of FoAA offline. Therefore, standards and protections available to FoAA offline must be extended and adapted to online spaces keeping in mind the dynamic, fluid and ever evolving nature of ICTs.

4. FoAA online as enabling the enjoyment of other rights, including best practices toward this aim

ICTs have emerged as powerful tools for social and political change. They are central today to protect diversity and empower people and groups in positions of marginalisation – such as persons with disabilities, LGBTIQ communities, and linguistic, religious and other minorities – to exercise their right to FoAA. As physical civic space is shrinking around the world, online platforms are viewed as the new places for people to associate, gather and demonstrate, where doing so physically is no longer possible. Additionally, mobilisation online is also central today for supporting and strengthening offline assemblies.

Tools like websites, email groups, WhatsApp groups, mailing lists and social media and other messaging platforms are used to share information, organise protests, issue joint statements, and mobilise citizens across geographic boundaries. ICTs are effective for mobilisation and democratising participation in public affairs, including among persons with disabilities and others who are not in positions to participate in

[21] A/HRC/31/66 (2016), para 10.

[22] https://www.techopedia.com/definition/29624/twitterstorm

[23] In his 2012 report to the Human Rights Council, Kiai "noted the increased use of the Internet, in particular social media, and other information and communication technology, as basic tools which enable individuals to organize peaceful assemblies." Kiai, M. (2012). Op. cit.

physical assemblies. For people who do not have easy affordable access to transport, who live in remote places, or who have long work hours, ICTs have enabled them to participate in civic spaces which were out of reach previously. People no longer have to travel to the capital to be part of a movement to lower sales tax, or to challenge corruption. Where the exercise of FoAA offline is dangerous, particularly in authoritarian and undemocratic regimes, the ability of people to exercise FoAA online comes as a relief. The exercise of FoAA online counteracts the mediation of information by dominant media and circumvents prohibitions on dissemination of information. It impacts significantly on the scope of the action: with the use of the internet, assemblies have a greater reach and are more sustained across borders. They take up greater space and provide the possibility to articulate dissent beyond the gathering.

With regard to association, the relative anonymity that the internet facilitates as well as its cross-border nature enable people to develop identities and associate with others in a way that is simply not possible for them offline. For those who face social stigma or whose very identity is criminalised – such as people who face discrimination based on their sexual orientation and gender identity, religious or ethnic minorities, and political dissidents – the internet can be a lifeline to form meaningful associations.

The rights to FoAA are key enabling rights that ensure that individuals can act collectively by coming together to advocate for, and sometimes orchestrate, change. They are a vehicle for the exercise and realisation of many other civil, cultural, economic, political and social rights. The rights to FoAA also play a decisive role in the emergence and existence of effective democratic systems as they are a channel allowing for dialogue, pluralism, tolerance and broadmindedness, where minority or dissenting views or beliefs are respected.[24] There have been several instances across the globe, and more specifically the global South, where individuals and groups have effectively leveraged ICTs for the exercise of FoAA online and offline towards the defence of a whole host of other human rights. Below we include some examples:

Right to enjoy the benefits of scientific progress and its applications:[25] The means through which people access and use ICTs can in themselves be an example of exercising the right to freedom of association to enable enjoyment of the benefits of scientific progress and its applications. As mentioned previously, only around half of the world's population is currently online, and people and groups who face exclusion on the basis of location, economic power, age, gender, racial or ethnic origin, social and cultural norms, education, or other factors do not benefit from purely commercial connectivity initiatives such as ones from mobile national operators and satellite providers. As a result, there is increasing interest in exploring alternative and complementary strategies for connecting the unconnected. Among the strategies available to enable local access infrastructure models, bottom-up locally developed communications infrastructure, such as community networks, are proving to be particularly effective in connecting the unconnected. Community networks can be broadly defined as locally owned and operated networks. They can be commercial or non-commercial, and ownership can be either by the community or

[24]A/HRC/20/27, para 84.

[25]The Committee on Economic, Social and Cultural Rights has considered the provision of accessible and affordable internet access as part of the State's obligation under Article 15 of the International Covenant on Economic, Social and Cultural Rights. See for example, Committee on Economic, Social and Cultural Rights. (2018). Concluding observations on the initial report of South Africa, E/C.12/ZAF/CO/1. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=E%2fC.12%2fZAF%2fCO%2f1&Lang=e

an individual, as long as they are local to the communities they serve.[26] Community networks exist in all geographic regions, shaped by the communities that build them.[27] On top of providing affordable connectivity in places where there was none, or it was too expensive for people to use it meaningfully, community networks contribute to the empowerment of marginalised populations by fostering to the local economy, creating local employment, developing technical and entrepreneurial skills, and contributing to the social cohesion of the communities they serve. Community networks, themselves associations, can act as enablers for the exercise of multiple rights, including the right to enjoy the benefits of scientific progress, to take part in cultural life, freedom of expression and access to information, FoAA, education, health, work, and to take part in the conduct of public affairs.

Freedom of expression: FoAA online is frequently exercised to advance the closely related right of freedom of expression. In particular, we highlight several movements online that have addressed censorship and criminalisation of expression. When six members of the online Egyptian satirical group Atfal al-Shawarea (or "Street Children") were arrested in May 2016 for uploading satirical videos to YouTube and Facebook mocking the Egyptian regime, thousands of Egyptians came together to launch a social media campaign to protest the arrest under the hashtag "Freedom for Street Children". The protesters posted selfies of themselves with the tagline: "Does a mobile phone camera shake you?"[28] In Europe, a large-scale online campaign has been mobilising (using the hashtags #SaveYourInternet and #CensorshipMachine) to protest against Article 13 of the EU Directive on Copyright in the Digital Single Market, over fears that it could shut down the ability of creators and everyday internet users to upload and share content online.[29]

Right to information: Civil society organisations and other associations use online spaces and ICT tools to seek, receive and impart information. The Save the Internet campaign in India for net neutrality and equal access to the internet was initiated to mobilise the public to send in suggestions on retaining net neutrality to the Telecommunication Regulatory Authority of India.[30] By the last day of submission, a month after the process was started in April 2015, over one million emails had been sent in support of net neutrality. The campaign was reported to be one of the biggest online protests in India, combining the use of a website as a resource page, Twitter (using the hashtag #savetheinternet), Facebook, a petition and emails to the authorities as action tools. The campaign ultimately resulted in the Telecommunication Regulatory Authority of India taking the position that no platform will have preferential access,[31] thereby ensuring equal access to the internet to all actors and preventing monopolies on the generation and access to information. Similarly, a government plan to introduce a

[26]Innovations in low-cost communication technology have created new possibilities for the development of affordable, locally owned and managed communication infrastructure. A growing number of communities and small, local and regional operators have taken a more pragmatic approach, using off-the-shelf low-cost commodity networking equipment to provide themselves and others with Wi-Fi, GSM and fibre connections. For more on community networks see: APC. (2018). *Global Information Society Watch 2018: Community Networks*. https://www.giswatch.org/community-networks and https://www.apc.org/en/project/local-access-networks-can-unconnected-connect-themselves

[27]For a few examples, see: APC. (2018). *Contribution from the Association for Progressive Communications to the IGF intersessional work on Policy Options for Connecting and Enabling the Next Billion(s) – Phase IV*. https://www.apc.org/sites/default/files/APC_contribution_to_IGF_intersessional_work_on_Policy_Options_for_Connecting_and_Enabling_the_Next_Billions.pdf

[28]Jimmy Wales Foundation. (2016, 3 June). Egypt: Satirical Group "Street Children" Arrested Over YouTube Videos. http://jimmywalesfoundation.org/egypt-satirical-group-atfal-al-shawarea-arrested-over-youtube-videos

[29]See https://saveyourinternet.eu and https://www.liberties.eu/en/campaigns/protect-free-speech-campaign-online-censorship/249

[30]The campaign website acts as a resource tool and also shares action items. See: https://internetfreedom.in/campaigns-savetheinternet

single gateway for all international internet traffic in Thailand, restricting freedom of expression and access to information, was leaked to the public in September 2015. This saw thousands of people organise online using petitions and attacks on government websites. In the span of a month, a petition against the plan garnered more than 150,000 signatures and a Facebook page called "Anti-CAT Tower Mob" received 129,420 page likes.[32] The government subsequently responded by saying that it was merely considering the plan, but later disclosures showed it was still keen to implement the single gateway.

Right to privacy: While the right to privacy faces massive threats in the digital age, people also utilise online tools to exercise FoAA online to defend their privacy and promote greater protection and prevent regulations that compromise the right further. For example, Pyrawebs was a successful online joint action in Paraguay, which resulted in the prevention of legislation to institutionalise data retention.[33] In Tunisia large scale coordinated online and offline protests lead to the biometric ID card proposal officially being withdrawn from consideration in the Assembly of the Representatives of the People.[34]

Right to participation in public affairs: Sustained assemblies and associations online and offline have often resulted in significant political shifts across the globe. FoAA online can be pivotal to electoral processes and outcomes, and can even contribute to the calling of an election or ushering in a new political regime. The Bersih[35] (translated as "clean") rallies and their sea of yellow t-shirts have become a symbol of people power in contemporary Malaysia. The first Bersih rally was held in 2007, organised jointly by leaders from political parties, civil society groups and NGOs, to reform the electoral process that was argued to be skewed towards the then ruling coalition. Since 2007, several editions of Bersih have been organised, with the most recent one in 2018. This movement has heavily relied on online mobilisation, which ultimately resulted in multiple offline rallies and prolonged online protests.[36] This movement undoubtedly played a significant role in demanding electoral reforms and enhancing political participation of individuals in Malaysia, which ultimately witnessed a regime change. ICTs were especially crucial for organisers given the size of the rallies to coordinate internally and communicate externally. Further, given the tight control on print and electronic media in Malaysia, social media platforms were viewed as a critical space for discourse and protest that was otherwise invisible.

Freedom of religion or belief: Online assemblies and associations have significantly aided religious minorities and those holding opinions contrary to majoritarian perspectives, in particular by facilitating the push-back against incitement of hatred and violence on the basis of religion or religious views.[37] The

[31]Guha, R. (2017, 29 November). Trai backs net neutrality; says internet services must be non-discriminatory. *The Economic Times*. https://economictimes.indiatimes.com/tech/internet/trai-provides-recommendations-on-net-neutrality/articleshow/61831481.cms

[32]www.facebook.com/antimobcattower

[33]Rodríguez, K. (2015, 12 March). Pyrawebs: Paraguayans Rise Up Against Mandatory Data Retention. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2014/12/pyrawebs-paraguayans-rise-against-mandatory-data-retention

[34]Sayadi, E. (2018, 11 January). Biometric ID vs. privacy: Tunisians win on privacy! But it's not over yet. *Access Now*. https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet

[35]https://www.bersih.org

[36]EMPOWER. (2016). *Freedom of Assembly and Association Online in Malaysia: Overview and Case Studies*. https://www.apc.org/sites/default/files/APC_IMPACT_FOAA_Malaysia.pdf

[37]Venkiteswaran, G. (2017). *"Let the mob do the job": How proponents of hatred are threatening freedom of expression and religion online in Asia*. Association for Progressive Communications. https://www.apc.org/en/pubs/%E2%80%9Clet-mob-do-job%E2%80%9D-how-proponents-hatred-are-threatening-freedom-expression-and-religion-online

Tehrik-e-Taliban Pakistan, a proscribed organisation, claimed the responsibility for a heinous attack on the Army Public School in Peshawar on 16 December 2014, murdering 148 people, including 132 children. It was a massive tragedy borne by the Pakistani nation because of the huge toll of children's deaths. This incident was widely condemned around the world. The same evening, during a talk show on national television, a controversial cleric from the Red Mosque in Islamabad, Maulana Abdul Aziz, refused to condemn the killings and said the only solution to such problems was the implementation of Islamic Sharia law in the country, which is also what the Taliban have been demanding. This stance from the cleric became the impetus for a wide cross-section of Pakistani society to come out against radical ideology and protest against terror advocates. Enraged citizens took to social media and come out on the streets, calling for the arrest of the cleric. The protests were spearheaded by activist and politician Jibran Nasir, who raised the slogan "Reclaim Your Mosques".[38] The curious case of the Ready to Wait campaign on Facebook[39] – where women came out in defence of an age-old patriarchal (read chauvinistic) tradition of a temple in Kerala, India prohibiting women under the age of 55 from entering the temple – merits some examination.[40] This campaign was a response to many men and women taking to the internet calling for the end of the practice of prohibiting women of menstruating age from entering the temple. Given the extremely polarised context and security concerns involved in challenging religious practices in India, any discussion on religion online is to be welcomed, irrespective of whether we subscribe to the views presented. The Ready to Wait campaign in this sense is a positive development as the internet aided women, who would have otherwise not been able to coordinate and voice their views through traditional media, to speak out. The issue has gained national importance with the Supreme Court of India declaring the tradition to be unconstitutional,[41] despite which women who have entered or tried to enter the temple have faced mob violence.

Women's rights to equality and to live free from discrimination and violence: FoAA online has been utilised by women's rights activists and feminists to assert their rights to equality and to be free from discrimination and violence. The Pink Chaddi Campaign[42] in India was initiated by a group of women who came together to take collective action, using Facebook, against members of the right-wing Hindu group Sri Ram Sena who had attacked women and men in a pub in the Indian city of Mangalore in January 2009.[43] The founder of the right-wing group, Pramod Muthalik, publicly endorsed the attacks and announced plans to forcibly marry unmarried couples spotted at public places on Valentine's Day. In response to this, a group of women formed the "Consortium of Pubgoing, Loose and Forward Women"

[38]Jamal, S. (2014, 31 December). From #ReclaimYourMosques to #ReclaimPakistan, Pakistanis Call for an End to Extremism. *Global Voices*. https://globalvoices.org/2014/12/31/from-reclaimyourmosques-to-reclaimpakistan-pakistanis-call-for-an-end-to-extremism and APC. (2017, 10 January). Groundbreaking report on the shrinking spaces for online freedom of assembly and association in Pakistan. https://www.apc.org/en/news/groundbreaking-report-shrinking-spaces-online-free

[39]DNA. (2016, 29 August). #ReadyToWait: Women explain why they are willing to delay their entry into Sabarimala. https://www.dnaindia.com/india/report-women-devotees-of-lord-ayappa-say-they-are-readytowait-to-enter-sabarimala-2249993

[40]Khandhadai, G. (2016, 31 October). "Not ready to wait": Freedom of expression and religion. *APC*. https://www.apc.org/en/node/22215

[41]Rautray, S. (2018, 29 September). Women of all ages can enter Sabarimala Temple, rules Supreme Court. *The Economic Times*. https://economictimes.indiatimes.com/news/politics-and-nation/supreme-court-allows-women-to-enter-sabarimala-temple/articleshow/65989807.cms

[42]Susan, N. (2009, 15 February). Why we said pants to India's bigots. *The Guardian*. https://www.theguardian.com/commentisfree/2009/feb/15/india-gender

[43]Srivastava, R. (2017). *Shrinking Spaces: Status of Freedom of Association and Assembly in India*. Digital Empowerment Foundation. https://defindia.org/wp-content/uploads/2018/04/Shrinking-Spaces.pdf

(PLFW) on Facebook and started sending pin chaddis (pink underpants) to members of the right-wing group. Within a week, 40,000 members had joined this Consortium. On Valentine's Day that year, Sri Ram Sena offices received 2,000 pink chaddis from India and abroad.

The #SmashBrahmanicalPatriarchy movement in India deserves attention as well. In November 2018, a photograph of Twitter co-founder and CEO Jack Dorsey along with women activists in the Indian region was circulated online and led to a furore, as Dorsey was standing with a poster with the message "Smash Brahmanical Patriarchy". This is a popular slogan for Dalit women and their movements and campaigns online, but the photograph with Dorsey led to virulent attacks, hate speech and threats against Dalit women activists online. While a sizeable population of Indians online saw the poster as an attack on the upper-caste and privileged community of Brahmins and especially men, there was mobilisation by Dalit women, feminists and others about the need to smash and upend caste- and gender-based violence, exclusion and discrimination.[44]

Perhaps one of the most recognisable exercises of FoAA online to galvanise support for gender equality and the fight against discrimination has been the #MeToo movement, which in the last year has found resonance across countries in the global South. As the movement spread across Asia, Latin America and parts of Africa, millions of survivors described online their experiences of groping, rape, unwanted kissing, abuse and threats by people in positions of power in the government, private corporations and the entertainment industry; others simply posted "me too" on social media. The movement has seen high-profile perpetrators lose positions of power and face trial in some cases, reignited long simmering movements pushing for gender equality in the global South, and become a chance to shape national conversations about gender inequality and discrimination.[45]

Economic, social and cultural rights: FoAA online is also a tool to advance a range of economic, social and cultural rights. For example, in Tamil Nadu, India, residents of the Thothukudi district mobilised both offline and online to protest against the expansion of Vedanta's Sterlite Copper Smelting Unit, which was causing significant contamination of the groundwater supply and an adverse impact on the right to health. In response, the government shut down the internet in the district for many days, and the ensuing protests resulted in the death of over 10 people, some of them shot by police. The movement was ultimately successful, with the Madras High Court staying the re-opening of the plant.[46] Students in South Africa came together online to assert their right to education through the #FeesMustFall campaign. Starting with #RhodesMustFall campaign in March 2015 at the University of Cape Town that called to decolonise the education system, #FeesMustFall was a nationwide movement calling for affordable and accessible post-secondary education in South Africa. The movement was noted as an internet-age student movement, with students using social media platforms such as Twitter, WhatsApp, Facebook and YouTube, as well as blogs and cloud-based services, to mobilise, organise and gather support for their activism. Students utilised internet-based communications for information sharing and coordinating their local engagements around fees. As a result of the movement, there was no increase in university fees in 2016 and a Commission of Inquiry into Higher Education and Training was established and released a

[44]Kaur, N. (2018, 21 November). How Brahminical Patriarchy Smashed Twitter. *The Wire*. https://thewire.in/caste/should-twitter-smash-the-brahminical-patriarchy

[45]Sexuality Policy Watch. (2018, 5 March). The #MeToo reflections in the Global South. https://sxpolitics.org/the-me/18150

[46]Newsclick. (2018, 24 December). Madras High Court Stays Re-opening of Sterlite Thoothukudi Plant. https://www.newsclick.in/madras-high-court-stays-re-opening-sterlite-thoothukudi-plant

report on the feasibility of providing free tertiary education. However, the struggle for accessible and affordable university education continues. The Occupy Wall Street movement started as a protest movement against economic inequality in New York's Wall Street financial district in September, 2011. However, through the use of social media, including Facebook pages and Twitter hashtags for communication at general assemblies, calls for action through videos on YouTube, Vimeo and Livestream, and sharing of personal accounts through blogs, the movement was able to mobilise people from across 100 cities in the United States and over two dozen cities worldwide to join their protests against governments and corporations' exploitative practices. Their rallying call of "We are the 99%" sparked a discussion on income inequality that continues to this day.[47]

Sexual rights: FoAA online be a critical way for people who face strong social discrimination, for example based on their sexual orientation and gender identity, to exercise other rights, such as sexual rights. According to the findings of the global survey conducted by APC as part of the EROTICS (Exploratory Research on Sexuality and the Internet)[48] project, respondents indicated that they use the internet to express their identities, to network, to search for and share information, as well as to advocate for their rights.[49] Dating apps, for example, can provide a unique space to communicate and associate within a safe community without the persecution or stigma that may be experienced in other dating methods. However, design choices, as well as terms and conditions of use, impact how safe and secure such apps are. While the internet is an essential tool to communicate and spread critical information regarding LGBTIQ activism, these activists also face significant threats online, including harassment.

5. Limitations on and restrictions to assembly and association online

As the previous Special Rapporteur noted in her 2017 report to the UN General Assembly,[50] the rights to FoAA in the digital sphere are increasingly the subject of restrictive laws and policies. In addition, ICTs can be used to violate or infringe on the exercise of FoAA online and offline as well. Threats to FoAA online come from both state and non-state actors, such as the private sector and other internet users, and disproportionately impact politically vocal individuals, those who face discrimination based on their gender, gender identity or expression, and minorities including those holding minority views among majority communities.

FoAA online is often disrupted during crucial moments. The former Special Rapporteur recognised the importance of preserving FoAA and threats to FoAA during elections.[51] This holds true for FoAA online, because when curfews, bans on physical gatherings and restrictions on political associations take place offline, online spaces become even more important. Unfortunately, restrictions to FoAA online around

[47]Ngak, C. (2011, 13 October). Occupy Wall Street uses social media to spread nationwide. *CBS News*. https://www.cbsnews.com/news/occupy-wall-street-uses-social-media-to-spread-nationwide

[48]EROTICS is a network of activists and researchers working at the intersections of sexuality and the internet. More information at: https://erotics.apc.org/about-erotics

[49]APC. (2017). *EROTICS Global Survey 2017: Sexuality, rights and internet regulations*. https://www.apc.org/sites/default/files/Erotics_2_FIND-2.pdf

[50]https://undocs.org/A/72/135

[51]https://undocs.org/A/68/299

elections are becoming increasingly common and blunt tools. In Africa[52] and Asia[53] especially, we have noted several network shutdowns being ordered around elections and websites of political parties being taken down.[54] A recent example was seen in Bangladesh, where mobile operators were asked to downgrade 3G and 4G services in late December 2018.[55] This significantly impacts the rights to FoAA around critical democratic practices as well as diminishing the ability of individuals to participate in public affairs. Similarly, during times political or social unrest, restrictions are imposed that make the exercise of FoAA nearly impossible.

FoAA online also faces limitations and restrictions in the context of national security and terrorism. While states grapple with legitimate concerns of national and human security in relation to the use of the internet for illegal violent and terrorist activities, they often respond with excessive and overly broad restrictions. This results in undue restrictions on and undermining of the exercise of FoAA in online spaces. In many cases restrictions placed on online assemblies in the name of national security are not in line with international human rights standards. Recent legislations and proposed regulations on cybercrime allow the state to impose unilateral restrictions on the use of the internet which violate FoAA online.[56]

Below is a non-exhaustive list of challenges to FoAA online, and the various forms they take:

- **Access to ICTs and digital divides:** Access to the internet is a necessary precondition to the exercise of FoAA online, and is increasingly necessary for the exercise of FoAA offline. However, there exist multiple digital divides both between and within countries, with disparities in meaningful access to the internet[57] being determined by a number of factors, including age, disabilities, sexualities, gender identities and expressions,[58] socioeconomic locations, political and religious beliefs, ethnic origins, and racial markers. Individuals and groups within society that would benefit most from the internet to exercise FoAA, like those who live in rural areas, or who are marginalised or socially excluded for any number of factors, are also those who are less likely to have meaningful access to it.
- **Internet shutdowns:** Internet shutdowns, defined as the "intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information," are inconsistent with international human rights law, and disproportionately interfere with FoAA

[52]Anyango Odhiambo, S. (2017, 18 May). Internet Shutdowns during Elections. *Africa Up Close*. https://africaupclose.wilsoncenter.org/internet-shutdowns-during-elections

[53]For instance, authorities in Jammu and Kashmir, India suspended both mobile and broadband services in three districts ahead of by-elections in April 2017.

[54]See, for example, the blocking of the Awami Workers Party's website ahead of the 2018 general elections in Pakistan: http://mediamatters.pk/we-condemn-the-blocking-of-access-to-the-awami-workers-partys-website-weeks-ahead-of-general-elections-2018-and-call-upon-relevant-authorities-including-the-election-commission-of-pakistan-to-take

[55]Al Jazeera. (2018, 29 December). Bangladesh shuts down mobile internet in lead up to election day. https://www.aljazeera.com/news/2018/12/bangladesh-shuts-mobile-internet-lead-election-day-181229111353218.html

[56]Vietnam: https://www.reuters.com/article/us-vietnam-socialmedia/vietnam-releases-cybersecurity-draft-decree-idUSKCN1N71XY; Iraq: https://www.igmena.org/Internet-Freedom-Laws-and-Regulations-In-Iraq and Saudi Arabia: https://www.eff.org/pages/crime-speech-how-arab-governments-use-law-silence-expression-online#saudi_arabia

[57]APC. (2016). Op. cit.

[58]APC. (2017). *Bridging the gender digital divide from a human rights perspective: APC submission to the Office of the High Commissioner for Human Rights*. https://www.apc.org/sites/default/files/APCSubmission_OHCHR_BridgingGenderDigitalDivideHumanRightsPerspective_0.pdf

online.[59] Internet shutdowns are being observed with increasing frequency and duration. States invoke a range of justifications for the imposition of communications shutdowns, including national security, public order, public safety, countering disinformation, and protecting school examinations. In 2016, 75 internet shutdowns were observed globally; in 2017, there were at least 108 shutdowns observed. This number grew to 188 instances of network shutdowns in 2018.[60] Asia and Africa are the primary regions where internet shutdowns are imposed at an alarming rate. Throughout the African continent, recent weeks have seen a fresh spate of internet shutdowns that have hindered public access to information and communications. Sudan, Gabon and the Democratic Republic of Congo (DRC) are three of the latest countries to experience government-led restrictions on internet access.[61] In Cameroon, a shutdown was imposed on the Anglophone region of the country for 93 days. Most recently, Zimbabwe experienced a total shutdown on 14 January 2019.[62] Moving to Asia, the number of internet mobile application blackouts in India has been on the rise over the last few years, with over 277 network disconnections since 2012.[63] Sri Lanka experienced a large-scale government-ordered shutdown during communal tensions in 2018.[64] These network shutdowns have affected free speech, FoAA and access to information, among other rights and aspects of daily life.[65] We observe that shutdowns do not just interfere with the exercise of FoAA online; they are imposed when governments anticipate public assemblies and are intended to disrupt citizens' ability to protest peacefully, in the name of maintaining public order or national security. As the former Special Rapporteur emphasised, "All communication tools including mobile networks and internet connections must remain active and any interference with the connections or content on these connections must only be acted on under the order of a judicial authority,"[66] which is apparently not the standard followed across the globe.

- **Criminalisation and arrests:** Laws that are used to criminalise expression online[67] are used in combination with specific laws on assemblies and associations to violate the rights of users. Several instances of those calling for protests, organisers of WhatsApp groups[68] coordinating protests and those participating in online assemblies being charged and sentenced have been recorded. Leopoldo López in Venezuela was sentenced for publishing a tweet through which he called for a demonstration/protest. The text of the tweet said: "We have to go out to the streets to conquer democracy." The accusation by the government was instigation to not recognise legitimate authorities.[69] In this case, the OHCHR working group on arbitrary detention expressed

[59]The definition comes from the "Keep It On" campaign to fight internet shutdowns: https://www.accessnow.org/keepiton/#problem; see also Human Rights Council. (2016). The promotion, protection and enjoyment of human rights on the Internet, HRC/RES/32/13. https://undocs.org/en/A/HRC/RES/32/13

[60]https://www.accessnow.org/keepiton/#problem

[61]APC. (2019, 16 January). Internet shutdowns in Africa: "It is like being cut off from the world". https://www.apc.org/en/news/internet-shutdowns-africa-its-being-cut-world

[62]Various. (2019). #KeepitOn: Joint letter on keeping the internet open and secure in Zimbabwe. https://www.apc.org/en/node/35256

[63]https://www.internetshutdowns.in

[64]Gross, G. (2018, 26 March). Sri Lankan Shutdown of Web-Based Services Creates Huge Social Costs. *Internet Society*. https://www.internetsociety.org/blog/2018/03/sri-lankan-shutdown-web-based-services-creates-huge-social-costs

[65]Srivastava, R. (2017). Op. cit.

[66]Kiai, M. (2012). Op. cit.

[67]APC. (2017). *Unshackling expression: A study on laws criminalising expression online in Asia*. https://www.giswatch.org/2017-special-report-unshackling-expression-study-law-criminalising-expression-online-asia

[68]For instance, a WhatsApp group administrator was arrested in Karnataka, India for receiving a message insulting the prime minister. Express News Service. (2017, 3 May) Karnataka: WhatsApp group admin in jail over PM Narendra Modi post. *Indian Express*. www.indianexpress.com/article/india/karnataka-whatsapp-groupadmin-in-jail-over-pm-narendra-modi-post-4638071

[69]http://cdn.eluniversal.com/2014/06/02/ACUSACION_LEOPOLDO.pdf

its position about this case and concluded that the Venezuelan state violated civil and political rights including FoAA.[70] In July 2017, a Muslim man was arrested in the south Indian city of Chennai on charges of sedition, on the basis of WhatsApp messages that he had received on his phone. One of the messages had called on people to protest at Jantar Mantar, New Delhi's officially designated protest site, against those who disrespected the Koran. The man was released after a magistrate found no evidence of anti-national activity or calls for violence.[71] Artists who participate in online assemblies and generate satirical content that is political have also been targeted.[72] In October 2018, a couple was arrested for running an LGBTIQ Facebook group in Indonesia, amid a crackdown by the authorities on queer nightclubs and private residences of same-sex couples. This is one case among the growing instances where those managing websites and user groups online for queer persons are being arrested and their sites shut down.[73]

- **Takedown and blocking of content:** States also order the takedown or blocking of content to interfere with the exercise of FoAA online, and more specifically the right to freedom of association online. For example, in Malaysia, internet service providers (ISPs) are subject to takedown and blocking orders issued by the regulatory body, the Malaysian Communications and Multimedia Commission (MCMC).[74] The electoral reform group Bersih had its website blocked days ahead of a major rally in August 2015. In Pakistan, in 2013, the government shut down the first and only openly gay website, Queer Pakistan, which was started as an online support platform for the LGBTIQ community, on grounds of religious and social values.[75]
- **Surveillance:** As the previous Special Rapporteur noted in her report,[76] the rapid pace of technological development enhances the capacity of states, the private sector and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights. It should be noted that both mass and targeted surveillance may interfere with FoAA online, especially as human rights defenders (HRDs) and activists are disproportionately impacted by targeted surveillance. For example, in the United States, the FBI's COINTELPRO, founded in 1956, did not distinguish between political and criminal activity and sought only to neutralise dissent. One of the initiative's priorities was to "expose, disrupt, misdirect, discredit, or otherwise neutralize the activities of the Black nationalists," according to FBI documents. Most of the groups it monitored, outside of white supremacist groups, were seeking racial, gender and class justice.[77] While the programme was eventually shut down, it was recently revealed that the Department of Homeland Security has been monitoring the Black Lives Matter movement since 2015 in a manner reminiscent of COINTELPRO.[78] In Chile, Operation Hurricane illegitimately restricts and

[70] http://cdn.eluniversal.com/2014/10/08/resolucio-n-26-2014-ohchr-org-.pdf

[71] Karthikeyan, D. (2017, 19 July). Arrest of Muslim Man for Receiving Phone Message Highlights Police Misuse of 'Sedition'. *The Wire*. https://thewire.in/159367/sedition-whatsapp-chennai-anti-national

[72] For instance, Zunar, a celebrated cartoonist had developed many satirical images towards participation in the movement against corruption in Malaysia. He was arrested for sedition – see: https://www.theguardian.com/world/2018/jun/24/malaysia-top-political-cartoonist-zunar-will-miss-pm-najib-razak Subsequently, charges have been dropped.

[73] VICE. (2018, 22 October). A Gay Couple Were Just Arrested in Indonesia Over a Pro-LGBTQ Facebook Group. https://www.vice.com/en_asia/article/8xjj5z/a-gay-couple-were-just-arrested-in-indonesia-over-a-pro-lgbtq-facebook-group

[74] EMPOWER. (2016). Op. cit.

[75] Bytes for All, Pakistan. (2017). *Shrinking Spaces: Online Freedom of Assembly and of Association in Pakistan*. https://www.apc.org/en/pubs/shrinking-spaces-online-freedom-assembly-and-assoc

[76] https://undocs.org/A/72/135

[77] Craven, J. (2015, 20 August). Surveillance Of Black Lives Matter Movement Recalls COINTELPRO. *Huffington Post*. https://www.huffingtonpost.com/entry/surveillance-black-lives-matter-cointelpro_us_55d49dc6e4b055a6dab24008

[78] Joseph, G. (2015, 24 July). Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson. *The Intercept*. https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-

violates the civil and political rights of the Mapuche people through interception of private communications of their political leaders and representatives, violating not only their right to privacy, but also exercising new forms of institutional violence through the use of technology. The criminalisation of members of Mapuche organisations through the planting of false evidence on their cell phones has been compounded by the action of police and intelligence services agents who have monitored and monitored political activists, journalists and communications media, both in physical and digital spaces, restricting freedom of expression and their ability to organise politically.[79] New tactics used by law enforcement to monitor digital communications, such as infiltration in social networks, were detected in Brazil in 2016, with the news of an Army representative infiltrating Tinder to find protestors, which ended with the arrest of 21 youths who were organising to go to a protest. After some hours, the youths were released; the judge in charge considered the action as abusive.[80]

States are also using an array of technologies in public spaces which pose risks to FoAA. A few examples include drones to surveil protests; facial recognition software which, utilising artificial intelligence (AI), can be used to analyse drone footage or other sources of data;[81] and "stingrays" or "IMSI catchers", which are deployed to track suspects, but can gather information about the phones of countless bystanders.[82]

- **Government hacking:** In an effort to obtain data, law enforcement and intelligence agencies engage in attacks on the security of networks and devices. Sometimes these attacks are specifically targeted at associations and NGOs. Attacks can come in the form of state-sponsored malware, which deploys malicious code that infects computers; stockpiling or exploiting vulnerabilities, which leaves the public vulnerable to having their data stolen and exploited; and malicious hacking, whereby agents actively break into computers remotely, and may access, copy, delete or even create data in order to suit their needs.[83] The recent UNGA resolution on the right to privacy in the digital age[84] calls on states to "refrain from employing unlawful or arbitrary surveillance techniques, like hacking." In 2017, it was revealed that Egyptian NGOs were being targeted by Nile Phish, a large-scale phishing campaign. Almost all of the targets identified are also implicated in Case 173, a sprawling legal case brought by the Egyptian government against NGOs, which has been referred to as an "unprecedented crackdown" on Egypt's civil society. Nile Phish operators demonstrate an intimate knowledge of Egyptian NGOs, and are able to roll out phishing attacks within hours of government actions, such as arrests.[85]
- **Crackdown on encryption:** Following from the above, secure digital communications such as encryption, virtual private networks (VPNs) and similar technologies are essential for the exercise of FoAA online. Governments are cracking down on the use of secure digital communications in various ways. A number of governments in recent years have been threatening to legislate "backdoors" to encryption, enabling them to access private communications when they believe

matter-since-ferguson

[79]https://derechosdigitales.org/upr32/index.en.html and https://www.derechosdigitales.org/wp-content/uploads/tecnologia-y-vigilancia-en-huracan.pdf

[80]https://derechosdigitales.org/wp-content/uploads/Latin-America-in-a-Glimpse-eng.pdf and http://ponte.org/wp-content/uploads/2016/09/decisao-manifestacoes-relaxamento.pdf

[81]Dwoskin, E. (2018, 22 May). Amazon is selling facial recognition to law enforcement – for a fistful of dollars. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/?noredirect=on&utm_term=.32800603aefb

[82]https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices

[83]https://www.eff.org/issues/government-hacking-digital-security

[84]A/RES/73/179.

[85]Scott-Railton, J., et al. (2017, 2 February). Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society. *The Citizen Lab*. https://citizenlab.ca/2017/02/nilephish-report

they have a justification for doing so.[86] In December 2018, Australia's parliament passed controversial legislation that will allow its intelligence and law enforcement agencies to demand access to end-to-end encrypted communications. The legislation also empowers Australian authorities to compel technology companies like Facebook and Apple to make backdoors in their secure messaging platforms. The implications of Australia's legislation are global. If Australia compels a company to weaken its product security for law enforcement, that backdoor will exist universally, vulnerable to exploitation by criminals and governments wherever they may be. Additionally, if a company makes an access tool for Australian law enforcement, other countries will inevitably demand the same capability.[87] Backdoors expose all communications running through them to potential compromise by malevolent actors, including criminals, stalkers and terrorists. An equally worrying trend is states' treating the use of secure communications as a crime, or as evidence of "terrorist" activity. In particular, we highlight Turkey's 2017 arrest of IT consultant Ali Gharavi and non-violence trainer Peter Steudtner at a digital security and information management workshop and their pre-trial detention for over 100 days facing charges of aiding terrorism.[88] Interfering with access to encryption means that communications used for FoAA, including the data of large networks of people, are vulnerable to data breaches and malevolent hacking by state and non-state actors.

- **Trolling and harassment:** While ICTs have been used widely for mass gathering and mobilisation, they have also proven to be the medium through which counter-assemblies and trolls engage in cyberbullying, trolling,[89] hijacking of hashtags, harassment, intimidation, doxxing and hate speech, which have the impact of impeding the legitimate exercise of FoAA. This was specifically evident in the case of Bersih 2017 in Malaysia[90] and several campaigns in India.[91] Similarly, persons participating in online assemblies, especially those that touch upon issues relating to religion or politics, are often subjected to hate speech which is observed to be orchestrated in a coordinated fashion.[92] Often times, such harassment has serious offline consequences, as was the case with Sabeen Mahmud who was shot by gunmen for her online activism.[93]
- **Gender-based violence online:** Just as violence is used to silence, control and keep women out of public spaces offline, women and girls' experiences online reflect the same pattern. Online gender-based violence (GBV) – such as cyberstalking, cyberbullying, harassment and misogynist speech – has led to women withdrawing from online spaces, limiting their exercise of FoAA. It has also led to attacks on prominent women with a view to intimidate or discredit them or their work. Online GBV is also targeted at feminist causes, and, ironically, at websites and online campaigns aimed at increasing people's awareness of issues of violence against women. A huge leap in recognising online GBV as a violation of women's human rights, in 2018 the HRC adopted its first

[86]Boland, H. (2018, 3 September). US and UK governments seek mandatory 'backdoors' in chat apps. *The Telegraph*. https://www.telegraph.co.uk/technology/2018/09/03/us-uk-governments-seek-mandatory-backdoors-chat-apps

[87]Newman. L. (2018, 07 December). Australia's Encryption-Busting Law Could Impact Global Privacy. *Wired*. https://www.wired.com/story/australia-encryption-law-global-impact

[88]Various. (2017, 19 September). Turkey: Secure digital communications are essential for human rights. Written statement at the UN Human Rights Council 36th session. https://www.apc.org/sites/default/files/G1725558_0.pdf; Gharavi and Steudtner were released on bail pending trial on 25 October 2017, following their first hearing in the Istanbul 35th High Criminal Court.

[89]See https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook for examples and analysis of state-sponsored trolling.

[90]EMPOWER. (2016). Op. cit.

[91]Srivastava, R. (2017). Op. cit.

[92]Venkiteswaran, G. (2017). Op. cit.

[93]Hashim, A. (2015, 25 April). Pakistani rights activist Sabeen Mahmud shot dead. *Al Jazeera*. https://www.aljazeera.com/news/2015/04/pakistani-rights-activist-sabeen-mahmud-killed-150424210251526.html

ever resolution on preventing and responding to violence against women and girls in digital contexts, and the Special Rapporteur on violence against women, its causes and consequences dedicated her 2018 report to "online violence against women and girls from a human rights perspective". Misogynist attacks against APC's #TakeBacktheTech Twitter campaign in 2015 are also an example of attempts to disrupt an online assembly. According to the organisers of that campaign, the scale of the attack "involved more than 20,000 tweets and memes containing anti feminist, racist, violent and abusive content, which has also been targeted at those who expressed support for the #TakeBacktheTech campaign."[94] These attacks can potentially have the impact of exposing already vulnerable individuals to further danger and cause them to engage in self-censorship.

- **Data-intensive systems:** Smart cities, biometric identities and other data-intensive systems are being deployed around the world, which opens up a number of questions around issues of consent for the collection, processing and use of data and safeguards against misuse of data, for example, for profiling and discrimination. In the context of FoAA, the use of these systems opens up questions around how the data may be used to restrict associations and control assemblies, in particular for people who are in positions of vulnerability and marginalisation. Biometric-based identity systems, especially when kept in centralised and insecure manners, can risk revealing information about people's associations that put their identity and security at risk. Smart cities, which are supposed to keep traffic and other aspects of cities running orderly and efficiently, have the potential to squash public demonstrations of dissent, given that protests are to a large extent about disrupting order. Data-intensive systems like the deployment of facial recognition software, plus biometric identity systems, plus smart cities for efficiency or specific law enforcement purposes and network triangulation, can be used for control over people in public spaces. These technologies used without sufficient checks also de-anonymise people, making it possible to identify persons taking part in assemblies. The use of cutting-edge technology in Xinjiang, China to control a minority community in the name of countering violent extremism should serve as a warning of the implications of such technologies for FoAA.[95]

6. Responsibilities beyond the primary responsibility of the state, including the responsibilities of intermediaries

As the internet becomes increasingly ubiquitous, it is not surprising that intermediaries – i.e. internet platforms and companies – play an increasing role in impacting the exercise and enjoyment of human rights online. Internet companies have become central platforms for discussion and debate, information access, commerce and human development. Companies running platforms are enigmatic regulators, establishing a kind of "platform law" in which clarity, consistency, accountability and remedy are elusive.[96] The nature of these companies, the control each of them has over technical infrastructure and the knowledge they have of people's data defines the role they play in promoting or impeding FoAA online. For instance, telecommunication companies, mobile network operators and internet service providers (ISP) play a crucial role when met with government orders for internet shutdowns or to divert or stop traffic, or requests for specific subscriber information; social media platforms facilitate the

[94]APC. (2015). Facts on #TakeBacktheTech. https://www.apc.org/en/pubs/facts-takebackthetech

[95]The Guardian. (2017, 28 December). The Guardian view on surveillance in China: Big Brother is watching. *The Guardian*. https://www.theguardian.com/commentisfree/2017/dec/28/the-guardian-view-on-surveillance-in-china-big-brother-is-watching

[96]APC. (2018). *Reorienting rules for rights: A summary of the report on online content regulation by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. https://www.apc.org/en/node/34741

formation of online groups, the coalescing around hashtags and generally act as public squares for people to gather in, and as a result hold access to personal data that might include political orientation, and have the power to take down content and group pages, or prioritise content from certain groups and movements over others with their algorithms and targeted advertisements; the technical community and technical bodies can play a significant role in building standards that facilitate or restrict FoAA online among other rights, as well as making sure that spirit of the original decentralised internet remains in technical applications.

It is no surprise that internet platforms and companies are facing unprecedented pressure to comply with state laws to regulate content and user activities online. In fact, online platforms are subject to opposing demands: "one asking them to thoroughly police the content posted on their services to guarantee the respect of national laws, and the other objecting to them making determinations on their own and exercising proactive content monitoring, for fear of detrimental human rights implications. Moreover, given that the current non-liability regimes were initially established for 'passive' intermediaries, the fear of a potential loss of protection may disincentivise companies from assuming more responsibilities."[97]

The Guiding Principles on Business and Human Rights place a duty on states to ensure environments that enable respect for human rights on the part of businesses, which must strive to ensure that their policies and practices adhere to the Principles in letter and spirit. By applying human rights in their work, they would not be restricted; to the contrary, it would offer a globally recognised framework for designing tools and a common vocabulary for explaining their nature, purpose and application to users and states. Human rights law also gives companies the tools to articulate and develop policies and processes that respect democratic norms and counter authoritarian demands.

APC underscores that companies have the responsibility to respect human rights. This means they should refrain from infringing on human rights and take measures to address adverse human rights impacts resulting from their business models, policies, practices, and the services they provide.[98] All companies, regardless of their size, have a responsibility to respect human rights, by not infringing on the human rights of users and addressing adverse human rights impacts with which they are involved. They should have in place policies and practices that are appropriate for their size and resources, and also reflective of their user bases, including:

- A policy commitment to meet their responsibility to respect human rights.
- A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights.
- Processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.

Companies should, therefore, not comply with measures imposed by states that are not consistent with Articles19, 21 and 22 of the ICCPR. However, we observe that under increasing pressure, companies are not only complying with state laws concerning user activity regulation and other measures imposed by governments; they appear to also take pre-emptive measures through, for example, adaptations to their terms of service agreements. The challenges presented by companies regulating user activities and FoAA online stem from the lack of their policy standards being rooted in international human rights law;

[97]Internet and Jurisdiction Policy Network. (2017). *Content and jurisdiction policy options*. https://www.internetjurisdiction.net/uploads/pdfs/Papers/Content-Jurisdiction-Policy-Options-Document.pdf

[98]Ruggie, J. (2011). Op. cit.

government pressure and vague national laws; extraterritorial requests by states to take down content or shut down online activities; extralegal requests by states that cannot be sufficiently addressed; placing extreme pressure on companies to address disinformation; lack of sufficient information for users reporting or users against whom action is taken; automation and over-blocking; hate speech and targeting of vulnerable groups; and insistence on "real name" policy.[99] In this regard, the recommendations made in the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression addressing content moderation and responsibilities of companies[100] can be of use when developing recommendations with regard to their responsibilities related to FoAA online.

Similarly, the technical organisations responsible for developing the system architectures and protocols that underlie the core of the internet and other communications technologies have also started to look at their obligations for human rights. The IEEE[101] has been working on the relation of human rights and technology for several years and in October of 2018, it put out a journal dedicated to Privacy, Freedom and Human Rights.[102] The Internet Society has been investigating the relation between internet technology and human rights for nearly a decade and the Internet Engineering Task Force (IETF),[103] the primary standards development organisation for internet core protocols, has been wrestling over the relevance of human rights, especially privacy and expression, to the protocols they develop and approve. Recently the Internet Research Task Force (IRTF),[104] the research sister to the engineering IETF, began work researching the relationship between FoAA and internet protocols.

In a research group called Human Rights Protocol Considerations (HRPC),[105] engineers, rights advocates and social scientists are investigating the structure of protocols and system engineering and attempting to find human rights considerations that designers should take into account when designing, and that engineers should take into when developing technology. This work has required some effort to find language in which engineers and human rights advocates could communicate. Unfortunately the UN Guiding Principles are of limited guidance since they are very specific to business and companies. The group started with an investigation of internet protocols and freedom of expression[106] referencing the human rights declarations and conventions as well as protocol specifications. In 2018 the group began looking into protocol consideration for FoAA using the same techniques. Whether it is just a short-lived fascination or the beginning of a long-term objective, some internet standards developers are currently considering human rights as part of the framework for their efforts.

7. Recommendations and best practices

UN Special Rapporteur on the rights to freedom of peaceful assembly and of association:

- Reaffirm and sustain focus on FoAA online, including by condemning violations where they occur and by highlighting the issue in thematic reports, joint statements and communications to states.

[99] APC. (2018). Op. cit.

[100] See A/HRC/38/35.

[101] https://www.ieee.org

[102] https://www.standardsuniversity.org/e-magazine

[103] https://www.ietf.org

[104] https://irtf.org

[105] https://irtf.org/hrpc

[106] https://www.rfc-editor.org/rfc/pdfrfc/rfc8280.txt.pdf

- Emphasise that human rights offline also apply online and that the exercise of FoAA in online spaces or through online mediums is protected by international standards guaranteeing FoAA, including through commenting on and engaging with states on legislation.
- Collaborate with other UN special procedure mandate holders, the technical community, the private sector, civil society and users to document violations in different contexts and develop detailed best practices for each sector.
- Use social media and other ICTs creatively and extensively to promote the work of the mandate.

States:

- Adopt and implement a rights-based approaches to bridging digital divides in order to facilitate the exercise of FoAA online and offline. Such approaches must be rooted in the principles of accountability, equality and non- discrimination, participation, transparency, empowerment and sustainability, and also address the underlying multiple and intersecting social, economic, political and cultural barriers to meaningful access to the internet.
- Adopt a rights-based approach when developing policies and regulations that seek to govern ICTs and, more specifically, when restricting the exercise of FoAA online.
- Extend the protection of FoAA to online spaces and ensure that limitations on FoAA online meet established conditions of legality, necessity and proportionality for democratic societies.
- Provide for notification systems for assemblies and associations through online systems to ease the burden on organisers.
- Refrain from disrupting access to the internet and the exercise of FoAA online, especially during crucial moments like elections, conflict, violence, political unrest or disasters.
- Repeal any law that criminalises or unduly restricts the exercise of FoAA online or offline.
- Ensure that any limitations to the right to privacy are consistent with the international standards of legality, necessity and proportionality. Refrain from engaging in surveillance practices, both mass and targeted, that create a chilling effect on the exercise of FoAA.
- Protect and promote the availability and use of encryption and anonymity enhancing technologies, and refrain from interfering with the use of such technologies, and from employing disproportionate or arbitrary surveillance techniques, including through hacking.
- Refrain from engaging in trolling and harassment of users online, including through amplification, and ensure that any measures aimed at addressing trolling and harassment are consistent with established norms concerning freedom of expression.
- Ensure that legal frameworks adequately protect women’s right to be freedom from violence when exercising their FoAA, and that any restrictions to freedom of expression to respond to gender-based violence are necessary and proportionate, avoiding overbroad or vague in terms, criminalisation of speech or censorship of women's sexual expression.
- Ensure that all programmes that collect, process and retain biomentric data do so only when necessary and proportionate to achieve a legitimate aim, while protecting the data with comprehensive legal and technical safeguards and that digital identity programmes remain voluntary for all participants, and only collect, process, and retain biometric data with explicit and informed consent.
- Uphold the duty to protect against human rights abuses by third parties, including business by ensuring an enabling environment in which companies operate transparently, carry out human

rights impact assessments, provide access to remedy and empower users to make informed choices about whether and how to use online platforms for the exercise of FoAA online.

- Refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content generated by those exercising FoAA online by companies.
- Refrain from adopting models of regulation in which government agencies, rather than judicial authorities, become the arbiters of lawful exercise of FoAA online.

Companies:

- Recognise international human rights law as the authoritative global standard for ensuring FoAA on their platforms, not their own private interests or the varying laws of states. Revise ToS and community standards accordingly.
- Direct all business units, including local subsidiaries, to resolve any legal ambiguity in favour of respect for FoAA, freedom of expression, privacy and other human rights.
- Make blocking, content and takedown standards clear and specific. Provide examples to help users interpret and apply specific rules.
- Commit to maintain platforms as spaces where users, consistent with human rights law, can develop opinions, express themselves, assemble and associate and access information freely.
- Conduct rigorous human rights impact assessments on all products and policies. Include meaningful consultation with users and civil society and seek comments from interested users and experts, especially from the global South.
- Adopt the Guiding Principles on Business and Human Rights, along with industry-specific guidelines, e.g. those developed by civil society, intergovernmental bodies and the Global Network Initiative.

National human rights institutions:

- Improve use of ICTs to effectively monitor and address human rights violations.
- Adopt digital security measures and protocols to ensure the safety and security of stakeholders including members, staff, complainants, witnesses and collaborators.
- Monitor, comment on and participate in legislation and policies which create processes that may undermine the exercise of human rights and more particularly FoAA online.

Civil society:

- Engage in systematic monitoring and reporting of violations of FoAA online and offline though effectively leveraging ICT tools.
- Adopt digital security and encryption tools towards protection of self and other stakeholders.
- Build and share capacity among civil society and particularly among marginalised communities and individuals to utilise the potential of ICTs for FoAA online and offline effectively.