The Promotion and Protection of Human Rights in the Context of Peaceful Protests: Submission to the Office of the High Commissioner for Human Rights by the Association for Progressive Communications (APC)[1]

October 2019

1. Introduction

APC is an international network of civil society organisations founded in 1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs). We work to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies. As an organisation that has worked at the intersections of human rights and technology for nearly three decades and fully recognises the critical importance of ICTs for the fundamental right to protest, we welcome the focus of the Office of the High Commissioner on Human Rights on this topic.

It is increasingly difficult to distinguish between the online and offline dimensions of human rights in the context of assemblies, including peaceful protests. As Human Rights Council resolution 38/11 states, "human rights protections, including the rights to freedom of peaceful assembly, of expression and of association, may also apply to analogous interactions that take place online."[2]APC considers human rights in the context of assemblies and peaceful protests to have two dimensions:[3] one in which the exercise of these rights is carried out online, such as through

1 We thank APC member, Damian Loreti, for providing inputs for the development of this submission.

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

3 APC. (2019). *The rights to freedom of peaceful assembly and of association in the digital age: APC submission to the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association.*

online campaigns, ranging from awareness raising to working groups, petitions, protests – including virtual protests – and "hacktivism";[4] and one in which technology is used to support, enable, enhance and facilitate the rights of assembly and peaceful protests online and offline – for instance, the mobilisation of people through social media and online messages to gather in offline spaces. Hence, this submission covers these two dimensions. ICTs, including the internet, offer a unique and enabling space for the exercise and enjoyment of the rights to freedom of peaceful assembly, association and expression. Peaceful assembly online, within this submission, refers to an intentional and temporary gathering in private or public spaces for a specific purpose which includes 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.[5]

2. Laws, policies and programmes that have been developed to address the impact of new technologies, including information and communications technologies, on human rights in the context of assemblies, including peaceful protests.

Human rights in the context of assemblies, including peaceful protests, are enabled by new technologies, including the internet, and any limitation to these rights must be the exception and in accordance with international human rights law.[6] However, limitations on the rights to freedom of peaceful assembly and association on the internet take various forms, and often do not comply with human rights standards.[7] Examples of restrictions to the rights to freedom of assembly and peaceful protest include policies and measures that enable internet shutdowns, surveillance, censorship and laws that seek to tackle terrorism and cybercrime but are used to criminalise expression online. APC research has found that laws governing content regulation and national security, *sharia* laws, counter terrorism, and cybercrime laws are most to likely impact on the exercise of freedom of assembly online. Civil society groups and experts have pointed to the frequent use of laws, some dating back a century or more, against activities and expression online.[8] For example, in Pakistan, the Protection Ordinance of 2014 could affect citizens' right to assemble since it includes vague terms such as internet offences and other offences related to ICTs. As APC and our members in Pakistan have highlighted, this regulation

https://www.apc.org/en/pubs/rights-freedom-peaceful-assembly-and-association-digital-age-apc-submission-united-nations and Venkiteswaran, G. (2016). *Freedom of assembly and association online in India, Malaysia and Pakistan: Trends, challenges and recommendations.* Johannesburg: Association for Progressive Communications. https://www.apc.org/sites/default/files/FOAA_online_IndiaMalaysiaPakistan.pdf

4 See ARTICLE 19's background paper on right to protest: https://right-to-protest.org/wp-content/uploads/2015/06/Right-to-Protest-Background-paper-EN.pdf

5 APC. (2019). Op. cit.

6 Voule, Clément Nyaletsossi (2019). Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/41, p. 4.

7 APC. (2012). *The Rights to Freedom of Peaceful Assembly and Association and the Internet: Submission to the United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association*. https://www.apc.org/sites/default/files/APC_Submission_FoA_Online_0.pdf, para. 9.

8 Venkiteswaran, G. (2016). Op. cit., p. 22.

could negatively impact on individuals and organisations that rely on social media and digital news outlets to mobilise around issues of injustice and human rights. The Penal Code of Pakistan criminalises sedition[9] as well as blasphemy.[10] In terms of limitations to the rights to freedom of assembly and peaceful protest, this provision on blasphemy is the most likely to be used.[11] The Prevention of Electronic Crimes Act, approved in Pakistan in 2016 in spite of objections over human rights implications, employs vague language such as "obscenity and vulgarity" and "glory of Islam" while imposing restrictions on online expression in the country. These broad terms could legitimise the blocking of accounts and content disseminated by activists. This law also empowers the state to crack down against any online protests since "any commission or threat with intent to coerce, intimidate, create a sense of fear, panic or insecurity in the government or the public" is equivalent to cyberterrorism, and the perpetrators may be punished with up to 14 years imprisonment, a PKR 50 million (USD 478,000) fine, or both.[12] In Malaysia, in 2015, the Sedition Act 1948 was amended to include a provision that empowers the Session Court to prohibit a person from accessing any "electronic device" with no definition as to what this would constitute. This disproportionate penalty has the potential to restrict freedoms of assembly and to fully participate in public life. Section 505 of the Malaysian Penal Code deals with criminal defamation and incitement, and is used as an alternative provision to the Sedition Act to restrict freedom of assembly offline and online.[13]

In Kenya, meanwhile, the government enacted the controversial Computer Misuse and Cybercrimes Act of 2018 and has used it as a tool for targeting its critics, including journalists and bloggers. In May 2018, the Bloggers Association of Kenya successfully obtained orders suspending 26 sections of the law.[14] As the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) has observed, initiatives used to curtail online expression and dissent have also emerged recently in Tanzania, Rwanda and Malawi.[15] In Egypt, the Anti-Cyber and Information Technology Crimes Law (2018) authorises the mass surveillance of communications, requiring ISPs to keep and store customer usage data for a period of 180 days, including data that enables user identification, data regarding content of the information system, and data related to the equipment used.[16] This means that internet service providers (ISPs) have the data related to all user activities, including phone calls and text messages, websites visited, and applications used on smartphones and computers, which can be used to

9 Penal Code of Pakistan, Section 124A. https://www.oecd.org/site/adboecdanti-corruptioninitiative/46816797.pdf
10 The related provisions are Sections 295A, 295B, 295C, 298 and 298A.
11 Venkiteswaran, G. (2016). Op. cit., p. 23.
12 Bytes for All. (2017). *Shrinking Spaces: Online Freedom of Assembly and of Association in Pakistan*. https://www.apc.org/sites/default/files/FoAA_Online_Report_Final_0.pdf, p. 40.

13 Venkiteswaran, G. (2016). Op. cit., p. 23.
14 CIPESA. (2019). *State of Internet Freedom in Africa 2019*. https://cipesa.org/?wpfb_dl=307 , p. 11.
15 Ibid., p. 5.
16 APC, et al. (2018, September). *Statement opposing Egypt's legalisation of website blocking and communications surveillance*. https://www.apc.org/en/pubs/statement-opposing-egypt%E2%80%99s-legalisation-website-blocking-and-communications-surveillance

target civil society and protesters.

Another recent phenomenon has been the passage of laws that are meant to be aimed at combating so-called "fake news" but can be used to stifle the exercise of rights online, including the rights to freedom of assembly and peaceful protest. In 2019, Singapore passed its Protection from Online Falsehoods and Manipulation Act with the aim of combating fake news. This law bans the spread of what the government decides is "false or misleading" or is deemed to be against the public interest, and demands that it be corrected or taken down. The law can be applied across a broad range of platforms, from social media to news websites and potentially to closed private platforms such as chat groups and social media groups, including apps with end-to-end encryption.[17] In Egypt, the Egyptian Media and Press Law of 2018 allows the Supreme Media Council to "suspend any personal website, blog, or social media account that has 5,000 followers or more if it posts fake news, promotes violence, or spreads hateful views." Bloggers can be subjected to prosecution for publishing false news or incitement to break the law.[18] Malaysia passed in March 2018 the controversial Anti-Fake News Law that imposes up to seven years of prison for knowingly spreading vaguely defined "fake news".[19] This broadly termed law prompted criticism since it allowed maximum discretion to target critics of the ruling party and the government.[20] In October 2019, Malaysia's parliament took steps towards repealing the law.[21] Effective uses of such technologies as enablers of the exercise of human rights in the context of assemblies, including peaceful protests (e.g. how new technologies have facilitated the organisation of assemblies, including peaceful protests)

3. Effective uses of such technologies as enablers of the exercise of human rights in the context of assemblies, including peaceful protests (e.g. how new technologies have facilitated the organisation of assemblies, including peaceful protests)

People worldwide exercise their rights to freedom of association and of peaceful assembly

17 Guest, P. (2019, July 19). Singapore Says It's Fighting 'Fake News.' Journalists See a Ruse. *The Atlantic*. https://www.theatlantic.com/international/archive/2019/07/singapore-press-freedom/592039/ and Wong, T. (2019, 9 May). Singapore fake news law polices chats and online platforms. *BBC News.* https://www.bbc.com/news/world-asia-48196985

18 Michaelson, R. (2018, 27 July). 'Fake news' becomes tool of repression after Egypt passes new law. *The Guardian.* https://www.theguardian.com/global-development/2018/jul/27/fake-news-becomes-tool-of-repression-after-egypt-passes-new-law

19 APC, Centre for Independent Journalism Malaysia, et al. (2018, June).
Oral statement delivered under Item 4: General Debate UN Human Rights Council 38th Session.
https://www.apc.org/en/pubs/joint-oral-statement-malaysia-human-rights-council-38th-session

20 Human Rights Watch (2019). *Malaysia Events of 2018.* https://www.hrw.org/world-report/2019/country-chapters/malaysia

21 Shukry, A. (2019, October 9). Malaysia to Scrap Anti-Fake News Law Once Used Against Mahathir. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-10-10/malaysia-to-scrap-anti-fake-news-law-once-used-against-mahathir

through digital technologies.[22] Websites, email lists, social media and chat groups over messaging platforms, among others, are used for mobilisation and to organise peaceful protests.[23] The anonymity that the internet facilitates as well as its cross-border nature enables people to develop identities and associate with others in ways that are not possible for them offline, particularly in contexts where repressive regimes make protest illegal or dangerous. Digital technologies are also central to protect diversity and empower vulnerable groups, such as persons with disabilities, LBGTIQ communities, and linguistic and other minorities, to exercise their right to assembly, including peaceful protests. ICTs allow people to associate, gather and demonstrate, and to participate in civic spaces that were out of reach previously.

Mobilisation online is also central today for supporting and strengthening offline assemblies. ICTs, in particular social media, enable assemblies to continue over time and across geographies to build longer-term sustainable movements. New technologies are also used by citizens to monitor how authorities behave during physical assemblies, and to document abuses. Below are some examples of technologies as enablers of human rights in the context of assemblies, including peaceful protests.[24]

3.1 Social media

Social media platforms and advocacy hashtags are used to mobilise people online, coordinate conversations, raise awareness and generate support for causes. For instance, in India, the #SavetheInternet campaign to defend net neutrality in 2015[25] was reported to be one of the biggest online protests in the country. The campaign combined the use of Twitter and Facebook with a website and emails to the authorities.[26] Mobilisation online is also central today for supporting and strengthening offline assemblies. In particular, social media platforms enable assemblies to continue over time and across geographies to build longer-term sustainable movements. Students in South Africa, for instance, came together online to assert their right to education through the #FeesMustFall campaign. Starting with the #RhodesMustFall campaign in March 2015 at the University of Cape Town, which 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

22 However, digital divides – between and within countries – represent an obstacle to exercise these rights equally through digital technologies. Please see more at Souter, D. (2016, August). *Inside the Information Society: How the digital divide has changed.* https://www.apc.org/en/blog/inside-information-society-how-digital-divide-has-changed
23 Venkiteswaran, G. (2016). Op. cit., p. 4.
24 APC. (2019). Op. cit., p. 7-8.
25 Venkiteswaran, G. (2016). Op. cit., p. 7.
26 Ibid., p. 32.

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 report on the feasibility of providing free tertiary education.[27]

One of the most recognisable recent exercises of the rights to freedom of peaceful assembly and of association both online and offline is connected to the fight for women's rights. The origins of the Argentinian movement #NiUnaMenos (Not One Woman Less) can be traced to the murder of a 14-year-old girl in March 2015. That case and a tweet from a journalist that said "They are killing us: aren't we going to do anything?" were the seeds of the first of many massive protests.[28] Led by a group of 10 women journalists who did not know each other in person, and through the hashtag #NiUnaMenos, a march to the Congress in Buenos Aires was organised and replicated all over the country. This was the first of numerous massive mobilisations across the country that moved beyond the geographical limits of Argentina: ICTs helped spread these protests outside national borders. Similar mobilisations were organised on 7 November 2015 in Spain through the hashtag #7N,[29] and in Mexico on 24 April 2016 using #VivasNosQueremos and #24A.[30] On 13 August 2015, a "Ni Una Menos" protest took place in Peru; on 3 October that year in Poland, there was a strike against the criminalisation of abortion; on 19 October, the first women's strike in Argentina took place; and #26N marked "Non Una Di Meno" in Italy on 26 November 2017.

The #MeToo movement, which 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.[31] 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. In 2017, the Women's March inaugurated the Trump era on 21 January, and 50 countries around the world participated in the International Women's Strike on 8 March through the hashtag #8M. These protests were in many cases also accompanied by virtual action in which nearly 100,000 women participated under the hashtag #MiPrimerAcoso [My First Harrassment]; #1J, on 1 June 2016, in Brazil, based on the strength of #PrimeiroAssedio [First Harrassment] and #EstuproNaoECulpaDaVitima [Rape is Not the Victim's Fault]; and on 3 June 2016 through

27 APC. (2019). Op. cit. p. 12-13.
28 Pomeraniec, H. (2015, June 8). How Argentina Rose up Against the Murder of Women. *The Guardian.* http://bit.ly/2oBHwGs
29 Todos los partidos se suman a la marcha contra la violencia machista. (2015, 7 November). *El País*. https://elpais.com/politica/2015/11/06/actualidad/1446832225_319685.html
30 Gire. (2016, 24 April). #24A Todas a la calle. *Animal Político.* https://www.animalpolitico.com/punto-gire/24a-todas-a-la-calle
31 APC. (2019). Op. cit. p. 12.

#3J2016 in Argentina.[32]

3.2 Websites and online petitions

Websites are used to organise protests and assemblies through a variety of means, and online petitions can be also be used for mobilisation.

In Pakistan, for instance, The Collective of Freethinkers was a website where non-believers and progressive intellectuals were gathering online. The website was routinely attacked by hackers but stayed online until 2010. Finally, the website was taken down by the Pakistan Telecommunication Authority in 2010 and two of its members were accused of blasphemy and detained.[33] Queer Pakistan, launched in 2013, was the first website for the lesbian, gay, bisexual and transgender community in the country. The aim of the portal was to "act as a virtual support group" for the community, pushed to the peripheries of Pakistan's mainstream and largely conservative society.[34] That same year the government shut down the website.[35]

Online petitions, such as those hosted by change.org and avaaz.org, are also widely used for numerous issues, and can form a base of mobilisations. Other petitions have also been created, adding to the extensive campaigning over Facebook – "Delhi for Women's Safety", "Gang Raped in Delhi" – and Twitter through the hashtags #Damini, #Nirbhaya, #Delhirape, #DelhiProtest #RapeFreeIndia, together with street mobilisation.[36]

In Thailand, a government plan to introduce a single gateway for all international internet traffic, which could restrict freedom of expression and access to information, was leaked to the public in September 2015. Thousands of people organised around this issue using online petitions. In the span of a month, a petition against the plan gained more than 150,000 signatures and the Facebook page, "Anti-CAT Tower Mob", received 129,420 likes. The government subsequently responded by saying that it was merely considering the plan.[37]

3.3 The right to record

Sometimes, the mere presence of cameras can discourage law enforcement officials from resorting to violence. And when repressive practices do occur, the journalistic record provides an independent portrayal of events and promotes accountability and transparency.[38]

32 Alcaraz, M. Florencia. (2017). #NiUnaMenos: Politicisng the Use of Technologies. GenderIT. https://www.genderit.org/feminist-talk/special-edition-niunamenos-politicising-use-technologies
33 Bytes for All. (2017). Op. cit.,p. 40 and 41.
34 Ibid., p. 38.
35 www.queerpk.com and www.humjins.com
36 Bytes for All. (2017). Op. cit.,p. 32.
37 APC. (2019). Op. cit.,p. 9-10.
38 CELS. (2017) El Rol de Periodistas y Reporteros. In *El derecho a la protesta social en la Argentina*. Ciudad Autónoma de Buenos Aires: CELS. http://www.cels.org.ar/protestasocial/#periodistas

According to WITNESS, which has worked extensively on the right to record, this is defined as the "right to take out a camera or cell phone and film the military and law enforcement without fear of arrest, violence, or other retaliation" during assemblies and protests, but not only during these activities. As WITNESS states, the right to record is protected under provisions of international human rights standards such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, which protect freedom of expression, freedom of assembly, and the right to information. The right to record at protests has been explicitly recognised by the UN.[39] For example, the UN Human Rights Council recognised and protected this right explicitly in resolution 38/11.[40] A 2015 report from the former Special Rapporteur on extrajudicial, summary or arbitrary executions directs states to respect and protect "the individual's right to make a recording of a public event, including the conduct of law enforcement officials."[41] In a 2016 joint report, the Special Rapporteurs on extrajudicial, summary or arbitrary executions and on freedom of peaceful assembly and of association expanded on this, stating that "all persons enjoy the right to observe, and by extension monitor, assemblies."[42] The notion of the "right to record", said the rapporteurs, encapsulates not only the act of observing an assembly, but also the active collection, verification and immediate use of information to address human rights problems.

For example, and as WITNESS documents, in Argentina, the activist group "Antena Negra" held a live broadcast of the arbitrary detention of women during International Women's Day protests on 8 March, and "Emergentes" documented the aggressions that occurred during a convening of women activists in November 2016.[43]

3.4 Coordinated online attacks as a form of public protest

Distributed denial of service (DDoS) attacks are a form of online protest where protesters attempt to disrupt the availability of an online service by overwhelming it with traffic from different sources, thereby slowing down the website or even preventing the site from loading at

39 https://lab.witness.org/projects/right-to-record/

40 HRC/RES/38/11 recalls "the rights to freedom of peaceful assembly, of expression and of association, which encompass organizing, participating, observing, monitoring and recording assemblies," expressing its concern at the criminalisation of individuals and groups solely for having organised, taken part in or observed, monitored or recorded peaceful protests. It calls upon all states to pay particular attention to the safety of journalists and media workers observing, monitoring and recording peaceful protests, and underlines the necessity to address the management of assemblies, including peaceful protests, so as to contribute to their peaceful conduct, and to prevent injuries, including those that lead to disability, and loss of life of protestors, those observing, monitoring and recording such assemblies.

41 Heyns, C. (2015, 24 April). Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions. *Use of information and communications technologies to secure the right to life*. https://undocs.org/A/HRC/29/37

42 Kiai, Maina & Heyns, C. (2016, February). Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/31/66

43 https://lab.witness.org/activists-argentina-use-videos-denounce-increasing-institutional-violence/ and https://www.pagina12.com.ar/223937-periodistas-procesados-tras-la-represion-en-la-marcha-por-sa

all. Services running on the same server as the website, such as email, may also be impacted.[44] The attacks are often carried out by botnets – an army of computers that work together to deploy malicious attacks with virtual anonymity – or manually by getting large numbers of people to visit a website.[45] An example of DDoS being used as a form of online protest to advance human rights includes hackers associated with Ghost Squad and the Anonymous collective launching a DDoS attack against the official Ku Klux Klan website to protest its glorification of "blunt racism".[46] However, as noted in section 4, DDoS attacks are also a tactic used to target human rights defenders and civil society to interfere with their right to peaceful assembly and protest. There is an ongoing debate about whether DDoS attacks are a legitimate form of social protest or a criminal act.[47] In APC's view, DDoS attacks should not be criminalised as a form of protest, but their use may need to be balanced against other rights in assessing the effects of such protests.[48]

3.5 Encryption

Anonymity is an important enabler of the rights to freedom of assembly online. The relative anonymity that the internet offers enables individuals and minority groups, among others, to associate on sensitive matters such as sexual orientation or religion. Encryption preserves confidentiality in online communications. Hence, encrypted messaging is important for the organisation of protests and demonstrations, especially within repressive regimes and against the government.[49] Encryption allows people to engage in online association and assemblies based on identities or beliefs that are illegal in some countries, like LGBTIQ groups, political opposition, or religious minorities.

For example, a study conducted as part of APC's EROTICS project revealed that 98% of sexual rights activists, women's rights activists, safe abortion activists, LGBTIQ activists, sex education activists, and others responded that the internet is "absolutely crucial for sexual rights." Only 10% of these activists said that "they could perform [their] advocacy work without the internet." According to this research, 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

44 Moyer, K. (2016). Attacks on social movements increase online, tech support comes to the rescue. https://www.apc.org/en/news/attacks-social-movements-increase-online-tech-supp
45 Venkiteswaran, G. (2016). Op. cit., p. 33.
46 https://www.digitaltrends.com/computing/kkk-hacker-attack/
47 https://www.pcmag.com/article/327887/ddos-attacks-legitimate-form-of-protest-or-criminal-act
48 Venkiteswaran, G. (2016). Op. cit., p. 40.
49 APC. (2015). The right to freedom of expression and the use of encryption and anonymity in digital communications. Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression. https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf, p. 4-5.

26% thought that it allows dialogue between people with diverse opinions.[50]

The case of Lebanese feminist lesbians engaging anonymously online shows how women can create safe spaces online which can lead to mobilisation. The queer movement in Lebanon, the research found, would not exist if it was not for the ability to assembly and mobilise online. The movement traces its roots to the ability to access online spaces where lesbians could meet anonymously and safely, to discuss issues from dating to rights.[51]

4. The human rights challenges posed by interferences with the availability and use of such technologies in the context of assemblies, including peaceful protests

Various measures to unduly restrict internet use, such as the prevention of internet access at key political moments (generally referred to as “internet shutdowns”) and taking down of content, among others, are inconsistent with international human rights law, and disproportionately interfere with the ability to organise and conduct peaceful assemblies.[52]

4.1 Internet shutdowns

Internet shutdowns, defined as measures to intentionally prevent or disrupt access to or dissemination of information online, are in violation of international human rights law, and disproportionately interfere with the use of the internet as civic space.[53] In 2016, the UN Human Rights Council unequivocally condemned measures to intentionally prevent or disrupt access to or dissemination of information online and called on all governments to refrain from and cease such measures.[54] Governments frequently impose shutdowns during demonstrations and other critical political moments, and in violation of international norms guaranteeing the rights to freedom of expression and assembly.[55]

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.[56] In early 2019, Sudan, Bangladesh and the Democratic Republic of Congo all experienced government-led restrictions on internet access.[57] On 7 January 2019, Gabonese citizens

50 Ibid. p. 8.
51 Ibid.
52 APC. (2019). Op. cit., p. 14.
53 This definition comes from the “Keep It On” campaign to fight internet shutdowns: https://www.accessnow.org/keepiton/#problem
54 HRC/RES/32/13. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13
55 https://www.apc.org/en/node/35631
56 APC. (2019). Op. cit., p. 15.
57 Taye, B. (2019, 10 January). Sudan, Bangladesh, DRC, Gabon start 2019 with major digital rights violations. https://www.accessnow.org/sudan-bangladesh-drc-gabon-start-2019-with-major-digital-rights-violations and 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-it-being-cut-world

experienced a 48-hour blackout following an attempted military coup.[58] A week later, Zimbabweans experienced a seven-day internet shutdown that moved from a total obstruction to a partial blockage of social media platforms,[59] which were justified as a standard practice "whenever there are very serious civil disturbances in any country."[60] On 5 August 2019, the Indian government imposed a severe communications blackout in the region of Kashmir that included all digital and non-digital modes of communication, including internet via broadband and mobile and also landline phones.[61] In the context of demonstrations against the government and an opposition campaign in September 2019, Facebook Messenger, social media and news sites were disrupted in Egypt.[62] During the recent political crisis and protests in Ecuador in October 2019, social media, mobile communications, and websites, were also temporarily disrupted during the ten days of social mobilisation and protest. This particularly affected protesters' availability to share in real time what was happening and to communicate for security purposes, to organize and to gather support for the mobilizations, and, more specifically, negatively impacted on independent media that could not cover repression against protesters.[63] These shutdowns were imposed in the context of significant political developments, interfering with the right of people to publicly demonstrate and peacefully assemble and protest.

4.2 Taking down and blocking of content and applications

States also order, through legal and extralegal means, the takedown or blocking of content and platforms to interfere with the right to freedom of association and peaceful assembly.

As mentioned above, 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.[64] In Malaysia, internet service providers were subject to takedown and blocking orders issued by the regulatory body, the Malaysian Communications and Multimedia Commission. The electoral reform group Bersih had its website blocked days ahead of a major rally in August 2015.[65] In April 2019, the Egyptian government blocked access to around 34,000 internet domains in an apparent bid to restrict

58 https://www.apc.org/fr/node/35336
59 Majama, Koliwe. (2019, 22 February).The bigger picture: Assessing Zimbabwe's internet blockade. https://www.apc.org/en/blog/bigger-picture-assessing-zimbabwe%E2%80%99s-internet-blockade
60 Ibid.
61 https://www.apc.org/en/node/35631
62 NetBlocks. (2019, April 15). Egypt filters 34,000 domains in bid to block opposition campaign platform. https://netblocks.org/reports/egypt-filters-34000-domains-in-bid-to-block-opposition-campaign-platform-7eA1blBp and NetBlocks. (2019, September 22). Facebook Messenger, social media and news sites disrupted in Egypt amid protests. https://netblocks.org/reports/facebook-messenger-social-media-and-news-sites-disrupted-in-egypt-amid-protests-eA1Jd7Bp
63 NetBlocks. (2019, October). Evidence of social media disruptions in Ecuador as crisis deepens https://netblocks.org/reports/evidence-of-social-media-disruptions-in-ecuador-as-crisis-deepens-oy9RN483 and https://netblocks.org/reports/evidence-of-social-media-disruptions-in-ecuador-as-crisis-deepens-oy9RN483
64 Bytes for All, Pakistan. (2017). Op. cit.
65 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

online content related to an opposition campaign, according to NetBlocks internet measurement data. The original website for the campaign was first blocked hours after it reportedly gathered 60,000 signatures after gaining popular support against proposed changes to Egypt's constitution.[66]

In Turkey, a court in Ankara decided to block 136 web addresses including independent news websites such as Bianet.org in August 2019.[67] The court's decision was based on what is widely known as the Internet Law of Turkey, which allows the blocking of websites on grounds of protection of the right to life, national security and public order, and protection of general health on the request of relevant ministries or the Presidency. According to Amnesty International, the decision did not provide any justification as to how any of the addresses listed in the decision fall under this provision.

4.3 Restrictions on encryption

Tools for secure digital communications such as encryption and similar technologies are essential for the exercise of the rights to freedom of association and peaceful assembly. A number of governments in recent years have been threatening to legislate "backdoors" to encryption, enabling them to access private communications when they believe they have a justification for doing so. Backdoors expose all communications running through them to potential compromise by malevolent actors, including criminals, stalkers and terrorists.

In December 2018, Australia's parliament passed controversial legislation that allows 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 could be 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. Recently, it was revealed that the governments of the United States, the United Kingdom and Australia are pressuring Facebook to limit its plan to implement end-to-end encryption across its messaging services.[68]

An equally worrying trend is states' treating the use of secure communications as a crime, or as

66 NetBlocks. (2019, April 15). Egypt filters 34,000 domains in bid to block opposition campaign platform. https://netblocks.org/reports/egypt-filters-34000-domains-in-bid-to-block-opposition-campaign-platform-7eA1blBp

67 Amnesty International. (2019,6 August). Turkey: Mass blocking of social media and news sites is full-frontal attack on freedom of expression. https://www.amnesty.org/en/latest/news/2019/08/turkey-mass-blocking-of-social-media-

68 Open Letter: Facebook's Privacy First Proposals. (2019, October). https://cdt.org/files/2019/10/US-UK-Australia-letter-to-Zuckerberg-10-4-19.pdf

evidence of “terrorist” activity – for instance, 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. Interfering with access to encryption means that communications used for freedom of assembly, including the data of large networks of people, are vulnerable to data breaches and malevolent hacking by state and non-state actors.[69]

4.4 Distributed denial-of-service (DDoS) attacks

As previously mentioned, DDoS attacks are often used to target human rights defenders and civil society engaged in peaceful assemblies and protests. According to APC member May First Movement Technology,[70] which is a non-profit service provider for social movements and activists, attacks on social movements have increased online in recent years.[71] For example, Github.com was the target of a large-scale attacked and was temporarily disabled in 2015, with the attacks apparently linked to its support for internet freedoms in China.[72] Zimbabwean human rights activist organisations were targeted with DDoS attacks during the controversial 2013 elections.[73] Fair Trade Africa, Privacy International and the Zimbabwe Human Rights Forum had their sites disabled, ostensibly for monitoring the elections for potential human rights abuses. The website of the Boycott, Divestment and Sanctions (BDS) movement, which aims to non-violently pressure Israel to comply with international law and to end international complicity with Israel’s violations of international law, has come under frequent attack. According to eQualit.ie, an APC member that builds software for social movements including Deflect, a DDoS mitigation tool, the bdsmovement.net website has been one of the most frequently targeted domains in their portfolio.[74]

5. The human rights challenges posed by the use of new technologies, including ICTs, in the context of assemblies, including peaceful protests

While new technologies offer new opportunities for the realisation of the rights of assembly and of peaceful protests, these technologies also offer states and other actors new possibilities to hinder them.[75] Some examples of the threats to these rights are outlined below.

69 APC. (2019). Op. cit., p. 17 and 18.
70 https://mayfirst.coop/en/index.html
71 https://www.apc.org/en/news/attacks-social-movements-increase-online-tech-supp
72 https://github.blog/2015-03-27-large-scale-ddos-attack-on-github-com/
73 https://www.theinquirer.net/inquirer/news/2287433/zimbabwe-election-hit-by-hacking-and-ddos-attacks
74 Moyer, K. (2016). Op. cit. and https://equalit.ie/deflect-labs-report-2/
75 APC. The Rights to Freedom of Peaceful Assembly and Association and the Internet: Submission to the United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association, para. 4. https://www.apc.org/sites/default/files/APC_Submission_FoA_Online_0.pdf

5.1 Surveillance

Both mass and targeted surveillance may interfere with freedom of assembly and peaceful protest, especially as human rights defenders and activists are disproportionately impacted by targeted surveillance. The deployment of surveillance technology in public spaces often happens in the absence of legal frameworks and presents a range of human rights risks, particularly with regard to the rights to peaceful assembly and association, as well as privacy.[76] The array of surveillance technologies deployed by states in public spaces include facial recognition software, including in protests, monitoring digital communications such as infiltration in social networks, and IMSI catchers or "stingrays" (described in more detail below), among others.

In Chile, "Operation Hurricane" illegitimately restricted and violated the rights of the Mapuche people through interception of private communications of their political leaders and representatives. The criminalisation of members of Mapuche organisations through the planting of false evidence on their cell phones was compounded by the action of police and intelligence services agents who monitored political activists, journalists and communications media, both in physical and digital spaces, restricting freedom of expression and their ability to organise politically.[77]

States also carry out targeted hacking and surveillance by deploying highly intrusive software applications used to track communications, known as spyware, as the Special Rapporteur on human rights defenders stated in his visit to Mexico in 2018, for instance.[78] Highly intrusive tools can and have been used to target human rights defenders, civil society organisations, activists and opposition political leaders, among others. These products, developed by companies such as FinFisher, Hacking Team and NSO Group, have been sold to governments that have demonstrated their propensity to violate human rights through their surveillance practices.[79]

Social media intelligence, or the techniques and technologies that allow governments to monitor social media, is another example of a highly intrusive practice used to violate the privacy of individuals and infiltrate civil society organisations and social networks, which could create a chilling effect on freedom of expression and negatively affect the exercise of the rights of assembly and peaceful protest.[80] For example, in Brazil in 2016, an Army representative infiltrated the dating app Tinder to find protestors, which ended with the arrest of 21 youths who

76 APC. (2019). Op. cit.
77 https://derechosdigitales.org/upr32/index.en.html
78 Forst, M. (2018). Report of the Special Rapporteur on the situation of human rights defenders. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_51_Add_2_EN.docx
79 APC. (2019). The surveillance industry and human rights: Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, p. 3. https://www.apc.org/sites/default/files/APC_submission_Surveillance_industry_and_human_rights.pdf

were planning to go to a protest.[81]

IMSI catchers, which are deployed to track suspects, but can gather information about the phones of countless bystanders, including protesters, are an increasingly used technology to surveil protesters and activists in the United States, according to the American Civil Liberties Union (ACLU). Also known as “stingrays” or “cell site simulators”, IMSI catchers are invasive cell phone surveillance devices that mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information. An IMSI catcher can capture call activity from thousands of uninvolved bystanders while searching for an individual or group. This kind of indiscriminate collection and (potential) retention of personal information, states the ACLU, treats everyone in a protest as a suspect and is, by definition, not justified by any individualised determination.[82]

5.2 Gender-based violence online, trolling and harassment

While ICTs have been used widely for the organisation of mass gatherings and mobilisation, they have also proven to be the medium through which counter-assemblies and trolls engage in cyberbullying, trolling, hijacking of hashtags, harassment, intimidation, doxxing and hate speech, which have the impact of impeding the legitimate exercise of assembly.[83] 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.[84]

ICTs and online spaces have also became a significant medium through which gender-based violence (GBV) against women is perpetrated. Online GBV – such as cyberstalking, cyberbullying, harassment and misogynist speech – affects women’s rights to freedom of peaceful assembly and association since it has led to women withdrawing from online spaces.[85]

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.[86] For example, misogynist attacks against APC’s #TakeBacktheTech Twitter campaign in 2015 are

80 Ibid.

81 Derechos Digitales. (2016). Latin America in a Glimpse. https://derechosdigitales.org/wp-content/uploads/Latin-America-in-a-Glimpse-eng.pdf and http://ponte.org/wpcontent/uploads/2016/09/decisao-manifestacoes-relaxamento.pdf

82 INCLO & IHRC. Defending Dissent: Towards State Practices that Protect and Promote The Rights to Protest, , p. 11. https://www.inclo.net/pdf/Defending-Dissent-Report-Complete-WEB-FINAL.pdf

83 APC. (2019). Op. cit., p. 18.

84 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-threateningfreedom-expression-and-religion-online

85 Venkiteswaran, G. (2016). Op. cit., p. 39.

86 APC. (2019). Op. cit., p. 18.

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."[87] These attacks can potentially have the impact of exposing already vulnerable individuals to further danger and cause them to engage in self-censorship.

The website of *Red de Salud de las Mujeres Latinoamericanas y del Caribe* (the Health Network of Latin American and Caribbean Women) was attacked and taken down immediately after the launch of several activities tied to #28SAbortoLegal, the September 2013 social media campaign to legalise abortion.[88] In August 2015, a series of DDoS attacks that lasted for weeks targeted reproductive rights organisations and advocates in the United States. Websites including those of the National Network of Abortion Funds and Planned Parenthood were attacked for offering reproductive services to low-income women.[89]

5.3 Data-intensive systems

Smart cities, biometric identities and other data-intensive systems are being deployed around the world. In the context of assemblies, including peaceful protests, the use of these systems opens up questions around issues of consent for the collection, processing and use of data, and in particular, how the data may be used to restrict associations and gatherings, in particular for people who are in positions of vulnerability and marginalisation.[90]

Biometric-based identity systems such as facial recognition software[91] and network triangulation can be used for control over people in public spaces. These technologies used without sufficient checks also make it possible to identify protesters, and reveal information about people's associations that put their identity and security at risk. 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 assembly and protest rights.[92] In the recent Hong Kong demonstrations, concerns regarding the collection and transfer of biometric data of residents who have participated in the protests by authorities were raised.[93] Protesters have also used lasers and covered their faces to avoid facial recognition

87 APC. (2015). *Facts on #TakeBacktheTech*. https://www.apc.org/en/pubs/facts-takebackthetech
88 https://www.apc.org/en/news/attacks-social-movements-increase-online-tech-supp
89 Moyer, K. (2016). Op. cit.
90 APC. (2019). Op. cit., p. 19.
91 This technology has been banned, for instance, in San Francisco. See: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html
92 APC. (2019). Op. cit., p. 19.
93 Kuo, L. (2019, June 14). Hong Kong's digital battle: tech that helped protesters now used against them. *The Guardian*. https://www.theguardian.com/world/2019/jun/14/hong-kongs-digital-battle-technology-that-helped-protesters-now-used-against-them

technologies and protect their anonymity.[94] The subsequent Hong Kong government ban on protesters wearing face masks was defined by Human Rights Watch as a disproportionate restriction on peaceful assembly rights.[95]

Privacy in public spaces is rapidly becoming more recognised as an essential value for the exercise of public protest. The United Nations Human Rights Committee's (HRC) draft general comment on article 21 of the International Covenant on Civil and Political Rights (ICCPR) regarding the right of peaceful assembly mentions the importance of the right to express your opinions anonymously, including in public spaces. It points out that even when "anonymous participation and the wearing of face masks may present challenges to law enforcement agencies, for example by limiting their ability to identify those who engage in violence," masks or other mechanisms to hide the identity of participants in a protest "should not be the subject of a general ban."[96]

6. Recommendations

6.1 States should:

1. Adopt and implement rights-based approaches to bridging digital divides in order to facilitate the rights to peaceful assembly and protest 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.

2. Refrain from disrupting access to the internet and access to information, especially during crucial moments like elections, conflict, violence, political crisis or disasters.

3. Repeal any law that criminalises or unduly restricts the exercise of freedom of peaceful assembly or the right to protest, online or offline.

4. Ensure that any limitations to the right to privacy are consistent with the international standards of legality, necessity and proportionality.

5. Refrain from engaging in surveillance practices, both mass and targeted, including government hacking, that create a chilling effect on the exercise of exercise of freedom

94 Adams, R. (2019, August 17). Hong Kong Protesters Are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched, *BuzzFeed*. https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers

95 Human Rights Watch (2019), Hong Kong: Face Mask Ban Violates Assembly Rights. https://www.hrw.org/news/2019/10/04/hong-kong-face-mask-ban-violates-assembly-rights

96 General Comment No. 37 on Article 21 (Right of Peaceful Assembly) of the International Covenant on Civil and Political Rights. https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx

of peaceful assembly or the right to protest, online or offline.

6. Impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime for them is in place.
7. Ensure, when purchasing or using privately developed surveillance technologies, that they only be used in accordance with human rights standards of legality, necessity and legitimacy of objectives, and that there are available legal mechanisms of redress consistent with the obligation to provide victims of surveillance-related abuses with an effective remedy.
8. Take effective measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises.
9. Protect and promote the availability and use of encryption and anonymity-enhancing technologies.
10. 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.
11. Ensure that legal frameworks adequately protect women's right to be free from violence when exercising their right to freedom of peaceful assembly or the right to protest, and that any restrictions to freedom of expression to respond to gender-based violence are necessary and proportionate, avoiding overbroad or vague terms, criminalisation of speech or censorship of women's sexual expression.
12. Ensure that all programmes that collect, process and retain biometric data do so only when there is a clear legal basis, when it is 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.
13. Impose an immediate moratorium on the use of facial recognition in public spaces until human rights safeguards are in place.
14. Ensure that the right to record during assemblies and peaceful protests, is protected, including by taking measures to ensure the safety of journalists, media workers, and human rights defenders, and any person who uses new technologies to document human rights violations.
15. Uphold the duty to protect against human rights abuses by third parties, including

businesses, 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 freedom of peaceful assembly or the right to protest;

16. Refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering by companies of content generated by those exercising freedom of peaceful assembly or the right to protest online.

17. Refrain from adopting models of regulation in which government agencies, rather than judicial authorities, become the arbiters of lawful exercise of freedom of peaceful assembly or the right to protest online.

6.2 Companies should:

1. Recognise international human rights law as the authoritative global standard for ensuring freedom of peaceful assembly or the right to protest online on their platforms, not their own private interests or the varying laws of states.

2. Direct all business units, including local subsidiaries, to resolve any legal ambiguity in favour of respect for freedom of peaceful assembly or the right to protest online, freedom of expression, privacy and other human rights.

3. 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.

4. 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.

5. Enable technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity.

6. Resist requests for user data that do not comply with international human rights standards.

7. Adopt the UN 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.