OHCHR Call for Input: The Promotion and Protection of Human Rights in the Context of Peaceful Protests

October 2019

Introduction

Access Now welcomes this opportunity to submit input and provide relevant information to the Office of the High Commissioner for Human Rights (OHCHR) on the promotion and protection of human rights in the context of peaceful protests. As an ECOSOC accredited organisation, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age.[1]

Through representation in 14 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. We engage with an action-focused global community, convene stakeholders through the RightsCon Summit Series, and operate a 24/7 Digital Security Helpline that provides real-time direct technical assistance to at-risk individuals and communities worldwide.

Call for Input

Access Now is grateful to submit input and relevant information on questions 2, 3, and 4 as outlined in the OHCHR's call for input.[2]

2. 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);

a. People are increasingly exercising their right to freedom of expression, peaceful assembly and association, online and through information and communications technologies (ICTs). Online mobilisation efforts occur on various mediums, including social media and communication apps, such as WhatsApp and Telegram. For instance, the wave of anti-government protests happening in Iraq in September and October 2019 were sparked by a call on social media in Tahrir Square, Bagdad and have since spread nationwide in several other provinces.[3]
b. However, the closing of online civic space has impacted the right to protest, as previously decentralized, secure, and open platforms and tools have become restricted, with individuals and communities subject to censorship, harassment, surveillance, and persecution that deter the use of ICTs as tools of protest. This worrisome trend against digital rights in the context of peaceful protests appears in the recent Hong Kong protest, where protesters "are keeping a low profile on social media, communicating only via secure messaging apps, deleting conversations

[1] Access Now, Access Now About Us
[2] OHCHR, Call for Input: The Promotion and Protection of Human Rights in the Context of Peaceful Protests.
[3] Aljazeera, Several killed as Iraq protests escalate, spread nationwide, 2 October 2019.

related to the protests and using pre-paid SIM cards not linked to their personal information. ... [They are also] wearing face masks in case photos are used to identify them and declining to give out their phone numbers or contacts to reporters."[4] These protesters are reverting to these techniques as a result of fears over how authorities are working to identify them through facial recognition and surveillance technologies.[5]

c. The United Nations Human Rights Council has declared that the same rights that people have offline must also be protected online.[6] Communications tools are essential to enabling the safe and effective exercise of the right to protest, so digital communication services, including new technologies, must remain open and secure for all to exercise their rights to freedom of expression, association and peaceful assembly.

3. The human rights challenges posed by interference with the availability and use of such technologies in the context of assemblies, including peaceful protests (e.g. through networks disruptions, blocking of internet services or restrictions on secure and confidential communications);

a. Internet shutdowns, sometimes called "network interference," kill switches, or blackouts, entail the blocking or throttling of internet access, and voice and data traffic, to the extent that networks become inaccessible or effectively unusable. Internet shutdowns are often carried out by telecommunication companies in response to government demands.

b. Blocking internet access, or social media apps, interferes with the right to freedom of expression by denying persons the right to seek, receive and impart information. Shutdowns frequently occur during periods of civil unrest, directly impacting the right to freedom of association and assembly.

c. Since 2011, Access Now has been identifying, documenting, and verifying internet shutdowns around the world. In 2016, we launched the Shutdown Tracker Optimization Project (STOP) to systematically collect, document, and verify internet shutdowns in close collaboration with affected communities.[7] Our process was also influenced and guided by the more than 200 organizations from 96 countries in the #KeepItOn Coalition, including SFLC.in in India, Moses Karanja's and CIPESA's work in Africa, and many others who helped develop and refined our methodology.[8] According to our STOP tracker, in 2018, there were at least 196 shutdowns in 25 countries, up from 75 in 24 countries in 2016.[9] In the first half of this year alone, there were 114 shutdowns in 23 countries.[10]

d. Governments are increasingly blocking internet services and restricting confidential and secure communications in the context of protests. Recent cases in Egypt, Iraq, Hong Kong, Zimbabwe,

---

[4] Lily Kuo, Hong Kong's digital battle: tech that helped protestors now used against them, *The Guardian*, 14 June 2019.

[5] Rosalind Adams, Hong Kong Protesters are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched, BuzzFeed News,17 August 2019.

[6] U.N. Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, U.N. Doc. A/HRC/38/L.10/Rev.1, 4 July 2018.

[7] Access Now, #KeepItOn, 2019; See also Access Now, Fighting Internet Shutdowns Around the World #KeepItOn

[8] See for example SFLC.in, Internet Shutdowns, 2019; Moses Karanja, 2019; CIPESA, 2019.

[9] Access Now, #KeepItOn, 2019.

[10] Patrick Kingsley, Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards, *The New York Times*, 2 September 2019.

Ecuador, Venezuela, Sudan, Papua, Sri Lanka and Turkey highlight the human rights impact of such government actions.

e. In Egypt, during protests against the Sisi regime, people's social media accounts are being blocked for protest-related content. For instance, Twitter temporarily suspended the accounts of over 100 human rights activists.[11] Moreover, police are stopping people in the street to check their mobile devices for anti-regime activity. This activity is taking place in the context of a massive wave of arrests, including high-profile activist Alaa Abd El Fattah – a courageous Egyptian freedom fighter, blogger and software developer arrested again only six months after being released from prison.[12]

f. At the beginning of this month, thousands of protesters took to the streets in Iraq to protest rising unemployment, failing public services, and government corruption. Thousands of protesters have been injured in violent clashes with security forces. The death toll continues to rise.[13] Iraqi authorities have responded to the protests by imposing a near-total internet shutdown, in addition to shutting down government offices, introducing a curfew in several cities, deploying thousands of heavily armed security forces, arresting hundreds of people and engaging in conflict resulting in the deaths of protesters.[14]

g. A few hours after the protests initiated, Iraqi authorities blocked Facebook, Twitter, WhatsApp, Instagram, and other social and messaging apps.[15] Since then, internet access has been cut off across the majority of Iraq. On or about 4 October, 75% of the country was offline, including Baghdad.[16]

h. This is not the first time Iraq has shutdown the internet during protests. Iraq has previously used internet controls to suppress dissent in 2018 when thousands protested against corruption and unemployment in Basra, Southern Iraq.[17]

i. This past September, as part of a larger crackdown on the ongoing protests in Hong Kong, Chief Executive Carrie Lam suggested that her administration would consider using legacy emergency legal powers to allow the Government of Hong Kong to censor, disrupt, and block social media and other communication platforms, and to shut down the internet. More recent reports captured renewed distributed-denial-of-service (DDoS) attacks and other cyber disruption activities targeting online messaging services, which put the open internet in Hong Kong in peril and interferes with the right to protest.[18]

---

[11] Memo, Twitter apologises for suspending Egypt activist accounts 11 October 2019.
[12] Access Now, Raise Your Voice for Alaa's Freedom! 2019.
[13] Hamdi Alkshali and Mohammed Tawfeeq and Tamara Qiblawi, Death toll rises to 93 in Iraq amid ongoing protests, *CNN*, 5 October 2019.
[14] Access Now, Iraq: freedom of speech and assembly under attack as over 100 killed, thousands injured,and hundreds arrested 10 October 2019; Mustafa Salim and Louisa Loveluck, Iraq is under curfew and Internet blackout as government tried to curb protests, *Washington Post*, 3 October 2019.
[15] Martin Chulov, Internet blackout in Iraq as death toll from violent protests rises, *The Guardian*, 3 October 2019.
[16] AlJazeera, Iraq protests: Death toll rises to 20 as unrest spreads.
[17] Access Now, Amid massive anti-government protests, a near total internet shutdown in Iraq, 4 October 2019; Committee to Protect Journalists, Iraqi authorities shut down internet, detain and assault journalists amid protests, 14 September 2018.
[18] Access Now, #KeepItOn coalition warns internet shutdowns would further hurt Hong Kong, 3 September 2019; Sum Lok-kei, Alvin Lum and Jeffie Lam, Hong Kong leader Carrie Lam leaves door. open on invoking sweeping emergency powers to deal with violent anti-government protests, *South China Morning Post,* 28 August 2019.

j. Last January, thousands of citizens in Zimbabwe protested the sharp increase in fuel prices.[19] In response, Zimbabwe experienced one of the most widespread internet shutdowns in Africa. Social media platforms – including Facebook and Twitter – were additionally blocked as well as other social media apps. Nonetheless, the protesters used virtual private networks (VPNs) to circumvent the social media blocking and sharing with the world evidence of the killing of protestors, injury, and numerous other human rights violations that appear to have been perpetrated by police during the protest. The internet shutdown did not end until January 24, 2019 after an interim court ruling.[20]

k. Governments often give national security, public safety, fake news, and hate speech as the main justifications for shutting down the internet. However, in reality, the actual cause that triggered the shutdown is usually not the same as the governments' given justification.[21] Shutdowns essentially allow government officials to stifle the flow of information about government wrongdoing or to stop communication among protesters and activists "by ordering service providers to cut or slow down their customers' internet access."[22] For instance, following protests related to racism towards the Papuan people, the Indonesian government imposed an internet shutdown in Papua and West Papua on 21 August 2019.[23] According to the Institute for Policy Research and Advocacy (ESLAM), "the actions taken by the Indonesian government [are considered] a form of digital repression that contravenes the public emergency principle, considering that the Indonesian government is imposing the internet shutdown under the pretext of public emergency."[24]

l. According to human rights experts – at the United Nations, the Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), and the African Commission on Human and Peoples' Rights (ACHPR) – internet shutdowns can *never* be justified under international human rights law, even in times of conflict.[25] These experts maintain that governments cannot order telecommunications companies to shut off mobile or internet services in the face of social unrest or protest.[26] Under section 4(c) the statement explains: "filtering of content on the Internet, using communications 'kill switches' (*i.e.* shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law."[27]

m. In protests particularly, it is essential that we protect the integrity of communications channels, including the internet, so that those injured can reach emergency and medical services,

---

[19] Access Now, Zimbabwe orders a three-day, country-wide internet shutdown, 15 January 2019.
[20] MacDonald Dzirutwe, Zimbabwe court says internet shutdown illegal as more civilians detained, *Reuters*, 21 January 2019.
[21] Access Now, The State of Internet Shutdowns, 8 July 2019.
[22] Patrick Kingsley, Life in the Internet Shutdown: Cross Borders for Email and Contraband SIM Cards, *The New York Times*, 2 September 2019.
[23] ESLAM, Internet Shutdown in Papua: A Digital Form of Repression that Contravenes the Principle of Emergency Situation, 22 August 2019.
[24] ESLAM, Internet Shutdown in Papua: A Digital Form of Repression that Contravenes the Principle of Emergency Situation, 22 August 2019.
[25] Joint Declaration On Freedom Of Expression And Responses To Conflict Situations
[26] Access Now, Zimbabwe orders a three-day, country-wide internet shutdown, 15 January 2019.
[27] OHCHR, Joint Declaration on Freedom of Expression and responses to conflict situations.

journalists can report stories and reach their sources, and families and friends can check in with their loved ones.[28] For instance, in Ecuador, there is evidence of targeted blocking that prevented protesters from uploading images and videos to social media documenting the protests.[29] Similarly, in Venezuela, "state-run internet provider CANTV restricted access to various social media platforms, including Twitter, Facebook, YouTube, Google and Android services."[30] According to sources, the shutdowns coincided with protests that arose "after opposition leader Juan Guaidó called on Venezuelans to join a military uprising seeking to remove President Nicolás Madura from power."[31]

n. Even with brief or partial shutdowns the human rights and economic impact can be devastating. The longer a shutdown goes on, the worse the situation becomes for everyone, with corrosive knock-on effects for the economy and development. For instance, according to estimates, shutting down the internet for three days during the Zimbabwe protest cost the country more than $17,227,262.[32]

o. Research further suggests that internet shutdowns are ineffective at quelling protests. Alarmingly, human rights violations and shutdowns often go hand in hand.[33] Shutdowns disrupt the free flow of information and create a cover of darkness that shields human rights abuses from public scrutiny. Journalists and media workers cannot contact sources, gather information, or file stories without digital communications tools. Shutdowns therefore cut off access to vital information and emergency services, plunging whole communities into fear.

p. Internet disruptions can also be linked to atrocities, conflict and other egregious human rights violations. In Sudan, while the internet was shut off, several reports indicate that more than 100 people had been killed, over 700 injured and at least 70 raped.[34] Sources suggest that the shutdown was an attempt by the Transitional Military Council (TMC), the de facto ruler of the country at the time, "to disrupt the sharing of footage and information pertaining to the dispersal of the sit-on on 3 June by security and military forces, calling for a civilian-led transitional government."[35] Therefore, unlike previous internet shutdowns in Sudan, this shutdown follows reports of systematic and organized killings and looting by the TMC.[36] Access Now spoke with locals in Sudan who suggested that the military confiscated and destroyed

---

[28] Access Now, #KeepItOn coalition warns internet shutdowns would further hurt Hong Kong, 3 September 2019.
[29] *See* Global Voices, Netizen Report Iraq and Ecuador face network shutdowns amid public protests 11 October 2019.
[30] Committee to Protect Journalists, Venezuelan authorities restrict internet, block outlets amid unrest, 1 May 2019; Access Now, Social media shutdown in Venezuela is a warning of what is to come as political tensions rise 22 January 2019.
[31] Committee to Protect Journalists, Venezuelan authorities restrict internet, block outlets amid unrest, 1 May 2019; The New York Times, Venezuela Crisis: Guaidó Calls for Uprising as Clashes Erupt, 30 April 2019.
[32] The NetBlocks and Internet Society, Cost of Shutdown Tool.
[33] Access Now, #KeepItOn coalition warns internet shutdowns would further hurt Hong Kong, 3 September 2019.
[34] Access Now, #IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan! 11 June 2019; Zeinab Mohammed Salih, Sudanese doctors say dozens of people raped during sit-in attack, The Guardian, 11 June 2019.
[35] Global Voices, Internet shutdowns and the right to access in Sudan: A post revolution perspective 16 September 2019.
[36] Access Now, #IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan! 11 June 2019.

mobile phones and protester's other electronic devices so that the atrocities documented could not be shared with the world.[37]

q. Academics, such as Anita Gohdes and Jan Rydzak, have examined the link between internet shutdowns, violence and conflict. According to Gohdes, internet shutdowns occur in tandem with higher levels of state repression, particularly in areas where government forces are actively fighting violent opposition groups, such as the Middle East and North Africa.[38] Alarmingly, Ghodes research finds that shutdowns "constitute a part of the military's strategy to target and weaken opposition groups, where the underreporting of violence is not systematically linked to outages."[39] Similarly, Rydzak's research on internet shutdowns in Sri Lanka highlights the link between internet shutdowns and violence. According to Rydazk's research "blackouts might have increased the potential for protest and violence in the wake of the attacks" on April 21 in Sri Lanka.[40] Specifically, "under a blackout, each successive day of protest had more violence than would typically happen as a protest unfolded with continued internet access."[41] From this research, it appears that shutdowns may polarize communities and encourage more violent demonstrations and protests.

4. The human rights challenges posed by the use of new technologies, including information and communications technology, in the context of assemblies, including peaceful protests (e.g. the use of surveillance and monitoring tools by the authorities, including biometrics-based recognition technology to identify protestors).

a. As we have seen in situations around the world, surveillance technologies have the potential to violate the privacy and other human rights of millions of individuals and communities. These human rights are violated, especially if there are not adequate control mechanisms for the acquisition and use of surveillance technologies and remedies for their abuse.[42]

b. From facial recognition technologies to the interception of mobile devices, protesters' right to privacy and anonymity is increasingly infringed. For instance, "facial recognition technologies in public spaces can be abused very easily to violate the people's fundamental privacy rights, in ways that are very difficult to remedy."[43] Unlike other sensitive personal information like passwords or security PINs, a person cannot change their face if the data captured is abused or compromised.

---

[37] Access Now, #IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan! 11 June 2019.
[38] *See* Anita R Gohdes, Pulling the plug: Network disruptions and violence in civil conflict 12 February 2015 Journal of Peace Research, Sage Journals.
[39] *See* Anita R Gohdes, Pulling the plug: Network disruptions and violence in civil conflict 12 February 2015 Journal of Peace Research, Sage Journals.
[40] Jan Rydzak, Jan Rydzak: The repercussions of shutting down social media, *Pittsburgh Post-Gazette*, 30 April 2019.
[41] Jan Rydzak, Jan Rydzak: The repercussions of shutting down social media, *Pittsburgh Post-Gazette*, 30 April 2019.
[42] Access Now, Argentina province in talks with Huawei over acquiring facial recognition surveillance technology 12 July 2018.
[43] Access Now, Argentina province in talks with Huawei over acquiring facial recognition surveillance technology 12 July 2018.

c. Without proper safeguards in place, public surveillance tools can be used to track people's movements in a way that can inhibit the labor right to strike, free association, free expression and enjoyment of public space in sporting and cultural events, among others.
d. In 2017, the Turkish government allegedly used a German-made spy program FinFisher to infiltrate the smartphones of Turkish opposition protesters. During the protests, fake Twitter accounts posted links to websites which promised protesters information about the demonstrations if they downloaded a smartphone app identified as FinSpy a product developed by FinFisher.[44] The spyware technology allows users to access targets' contacts, chat messages, phone conversations, photos and videos, including those on WhatsApp, Facebook Messenger and Skype. Simply put, it gives unimpeded access to a target's phone.[45] Evidence suggests FinFisher's concurrent efforts to undermine civil society outside Turkey, including the compromise of individuals in Indonesia, Ukraine, and Venezuela.[46]
e. In addition to malware-based phishing attacks, there are many other examples of attacks designed to hack protester's – particularly protest organizers' – social media accounts. In such attacks accounts are created to impersonate protest organizers to spread false information, or endanger those who follow them. For instance, last year our Digital Security Helpline received reports of social engineering attacks in Vietnam. These attacks targeted the Facebook profiles of bloggers and citizen journalists writing about democracy and human rights.[47]
f. Our Digital Security Helpline has also found instances of doxxing – maliciously publishing one's personal information, such as a phone number or addresses – to encourage physical harm to protesters and community organizers.[48] Last year, in Nicaragua there was an increase in threats to Nicaraguan activists' social media accounts, including phishing attacks aimed at obtaining the password or two-factor authentication code to accounts belonging to journalists, organizers and other community voices.[49] Local organizations estimate that 450 people have been killed, 600 disappeared and tortured, and 2,800 injured due to police violence and attacks by paramilitary groups since protests began last April.[50]

[44] Samantha Early, German prosecutors investigate spyware marker FinFisher, *DW*, 9 May 2019.
[45] Samantha Early, German prosecutors investigate spyware marker FinFisher, *DW*, 9 May 2019.
[46] Access Now, New report: FinFisher changes tactics to hook critics, 14 May 2018.
[47] Access Now, New Facebook phishing attack taking Vietnamese opposition voices online, 22 October 2018.
[48] Access Now, New wave of online attacks in Nicaragua puts opposition voices at risk of physical violence, 13 September 2018.
[49] Access Now, New wave of online attacks in Nicaragua puts opposition voices at risk of physical violence, 13 September 2018.
[50] Joshua Partlow, 'They took my humanity': Pro-government paramilitaries terrorize Nicaraguan protesters, *The Washington Post*, 2 August 2018; Access Now, New wave of online attacks in Nicaragua puts opposition voices at risk of physical violence, 13 September 2018.

For more information:
Peter Micek (peter@accessnow.org)
General Counsel, Access Now
+1-888-414-0100

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.