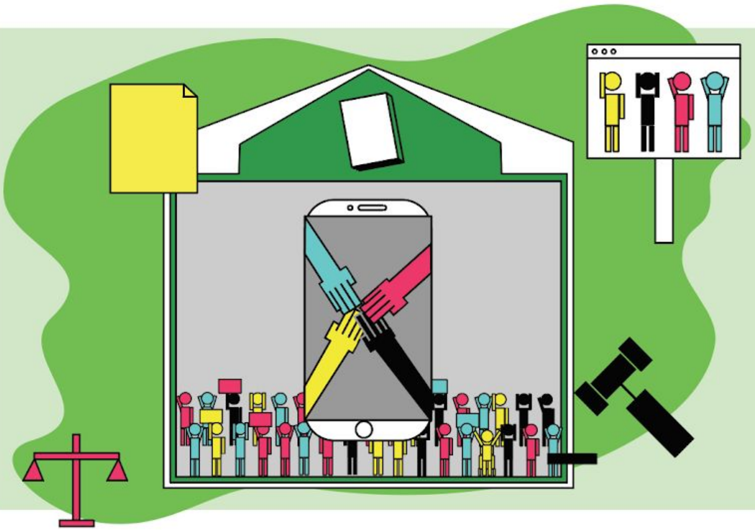

REPORT SNAPSHOT

Defending peaceful assembly and association in the digital age: takedowns, shutdowns, and surveillance

Protests can help birth and shape democracies, but they are often met with attempts to undermine privacy, muzzle protesters, and punish those speaking out. In 2020, protests across the globe are showing the power — and fragility — of our rights to peaceful assembly and association. After the police killing of George Floyd in the U.S., people across the globe are continuing mass protests against systemic forms of racial injustice, while facing authoritarian tactics of repression that combine the use of paramilitary force with invasive, rights-harming digital surveillance. Youth-led movements — from Hong Kong to Sudan — are sustaining defiance even as governments gain and exercise vast powers to silence and censor their speech.

As COVID-19 continues to spread, these movements are increasingly using the internet to organize, exercise their right to voice opinions, call others to action, express solidarity, and access life-saving information, including across national borders. They are also developing creative approaches to fight for their rights in digital spaces, working within the constraints of physical distancing measures.

However, governments are leveraging the internet and digital technologies to quell dissent and strip people of their capacity for collective action, online and off, even in contravention of their own domestic laws, and international human rights obligations.

Access Now's new report, ***Defending peaceful assembly and association in the digital age: takedowns, shutdowns, and surveillance***, spotlights three current issues that are directly impacting these rights globally: (1) **access, connectivity, and internet shutdowns**, (2) **unlawful surveillance and the right to privacy**, and (3) the **influence of the private sector in online civic space**. We provide case studies from around the world to raise the alarm about what is happening, and offer specific guidance for governments, the private sector, and international institutions to meet their duties and obligations to safeguard these rights, which are vital and necessary for any functioning democracy.

Selected summarized case studies

🇪🇹 Ethiopia: #OromoProtests

On June 29, 2020, prominent Oromo musician and social activist, Haacaaluu Hundeessaa, was shot dead by unknown attackers. In response to the killing, numerous protests sprung up in Addis Ababa and other cities in the Oromia region demanding justice. They grew in size, culminating in police clashes and military intervention, and as of July 8, 2020, at least 239 people had been killed and 3,500 arrested during the anti-government protests. In response, the government ordered a nationwide internet blackout to quell unrest.

🇭🇰 Hong Kong: #FightForHongKong and #HongKongProtest

On October 4, 2019, amid the ongoing and escalating city-wide protest, Carrie Lam, Chief Executive of the Hong Kong Special Administrative Region (HKSAR), invoked a colonial-era ruling, which authorized sweeping powers to quell social unrest, including banning face masks. Protesters have been forced to use extraordinary measures to limit their exposure to government surveillance and censorship, keeping "a low profile" on social media and using secure messaging tools and "burner" phones, as well as wearing face masks to avoid photo identification, among other tactics. Adding to the threats protesters face, the new National Security Law in Hong Kong, which took effect on July 1, 2020, granted authorities broad power to criminalize online speech, increased police powers over search and seizure, and radically removed judicial oversight from the surveillance system, along with imposing stricter requirements for compliance from internet service providers.

🇺🇸 United States: #BlackLivesMatter

On May 31, 2020, following nationwide protests, U.S. Attorney General William Barr described the so-called Antifa movement and other anti-fascist activists as "domestic terrorists." Those participating in Black Lives Matter protests have since become targets for the use of paramilitary force, with incidents including federal agents in military fatigues forcing protesters into unmarked vehicles. They have also become subject to invasive surveillance leveraging tools intended for other ends. The Department of Homeland Security has used drones, airplanes, and helicopters purchased for its customs and border enforcement to monitor Black Lives Matter protests in more than 15 cities; and law enforcement has used video footage captured by "smart streetlights" in San Diego, installed to monitor traffic and environmental conditions, to aid the persecution of protesters.

Recommendations: an overview

Following is a brief overview of the stakeholder recommendations we discuss in detail in our report.

RECOMMENDATIONS FOR GOVERNMENTS

Access, Connectivity, and Internet Shutdowns

1. Fulfill international obligations to protect the rights to freedom of peaceful assembly, association, expression, and access to information by allowing protesters to peacefully gather online or off ensuring that access to the internet is not blocked, limited, or shut down and that the media may freely operate.
2. Prioritize funding for digital development and reallocate existing funds toward building inclusive digital infrastructure, particularly amid crises.
3. Adopt and implement a human rights-based approach, integrating both civil and political rights with economic, social, and cultural rights, to close digital divides and ensure everyone can exercise their rights to freedom of peaceful assembly and of association online and off.

Surveillance and the Right to Privacy

1. Refrain from using or investing in technology, particularly mass surveillance, that uses biometric analysis to identify those peacefully participating in an assembly, including, but not limited to, facial, gait, or voice recognition.
2. Employ all possible measures to monitor and prevent the sale and use of surveillance technology (including spyware and targeted malware) for targeting protesters and others exercising their rights.
3. Protect and promote privacy-enhancing technologies, and safeguard people's use of encryption, pseudonymity, and anonymity, essential enablers of human rights.
4. Prevent and prosecute reprisals against those documenting protests, demonstrations, and other assemblies and disseminating such information through digital means.

The Influence of the Private Sector in Online Civic Space

1. Collaborations among states, authorities, and the private sector must be transparent and allow for open data, open government, open procurement standards, and transparency reporting requirements. Collaborations should also facilitate the public's access to information.
2. Clarify laws protecting the right to protest apply in digital spaces, including on private websites, applications, platforms, and services.
3. Ensure that all human rights defenders and media are able to operate without restrictions, including judicial harassment.

RECOMMENDATIONS FOR THE PRIVATE SECTOR

Access, Connectivity, and Internet Shutdowns

1. Invest in maintaining and improving networks to ensure high-quality internet access during current crises and in the future.
2. Prepare for a range of threats to the rights of users, particularly where bandwidth is overwhelmed and congested as a result of demonstrations, and ensure that the company deploys extra capacity throughout the events.
3. Challenge censorship and service limitation requests from states, using all available tools of law and policy, in procedure and practice. Notify affected users and the public of any such requests and any orders implemented, early and often.

Surveillance and the Right to Privacy

1. Protect user privacy and security through the encryption and anonymization of user data, and the transmission of user data over encrypted channels, whenever and wherever possible.
2. Treat all data traffic on an equitable basis no matter its origin, type, destination, or content.
3. Make a public commitment not to reuse or monetize data, and set clear limitations on secondary uses or further processing of data.

The Influence of the Private Sector in Online Civic Space

1. Explicitly acknowledge and publicly commit to maintain tech platforms as spaces that enable human rights, such as the rights to freedom of peaceful assembly and of association, through the full operationalization of the U.N. Guiding Principles on Business & Human Rights.
2. Implement human rights due diligence processes with respect to particular products and services that will provide in-depth consideration of the potential impact on fundamental rights that a product or policy poses as well as the various measures that are and may be taken to address them.
3. Guarantee users' rights to appeal, and facilitate effective remedies in accordance with international human rights standards that balance the rights, interests, and needs of victims, in addition to the company's capacity to effectively execute such remedial mechanisms.
4. Provide users with appropriate and accessible channels to communicate questions, concerns, and grievances about terms of use, company policies, or restrictions on access, freedom of expression, and privacy.

RECOMMENDATIONS FOR INTERNATIONAL INSTITUTIONS

Access, Connectivity, and Internet Shutdowns

1. Acknowledge states' obligation to ensure universal, affordable, open, secure, stable internet access as a means to realize human rights, including the rights to freedom of peaceful assembly and of association.
2. Urge states that are deliberately denying people access to the internet and communications, particularly in the context of assemblies, to keep the internet on.
3. Foster multi-stakeholder engagement to systematically monitor, document, and report violations of freedom of peaceful assembly and of association both online and offline. Building off the data collected, routinely develop best practices to keep up with the changing digital landscape.

Surveillance and the Right to Privacy

1. Prohibit the indiscriminate and untargeted surveillance of individuals exercising their right of freedom of peaceful assembly.
2. Require annual reporting by states of their purchase and use of surveillance technologies to their legislature and independent national oversight or human rights enforcement bodies.
3. Evaluate and strengthen existing digital security and encryption tools used in information technology initiatives like the U.N. Secretary-General's Data Strategy.

The Influence of the Private Sector in Online Civic Space

1. Commit to promptly addressing any case of intimidation or reprisal that is reported in connection to participation in public processes on a digital platform directly with the state in question and in partnership with the senior official responsible for reprisals.
2. Develop and implement a dedicated office or Special Representative to monitor public-private partnerships, ensuring transparency and respect for human rights.
3. Preserve open space: When hosting physical or virtual meetings, prioritize and be transparent about opportunities for associations and assemblies to freely self-organize, extending accessibility and respecting confidentiality as appropriate.

We extend a special thanks to Article 19, Association for Progressive Communications, and the Electronic Frontier Foundation for their decades of leadership in defense of the freedoms of peaceful assembly and of association.

For further details, see the full paper. For questions or media inquiries, please contact:

Laura O'Brien | UN Advocacy Officer, Access Now | laura@accessnow.org
Peter Micek | General Counsel & UN Policy Manager, Access Now | peter@accessnow.org
Press | Access Now | press@accessnow.org