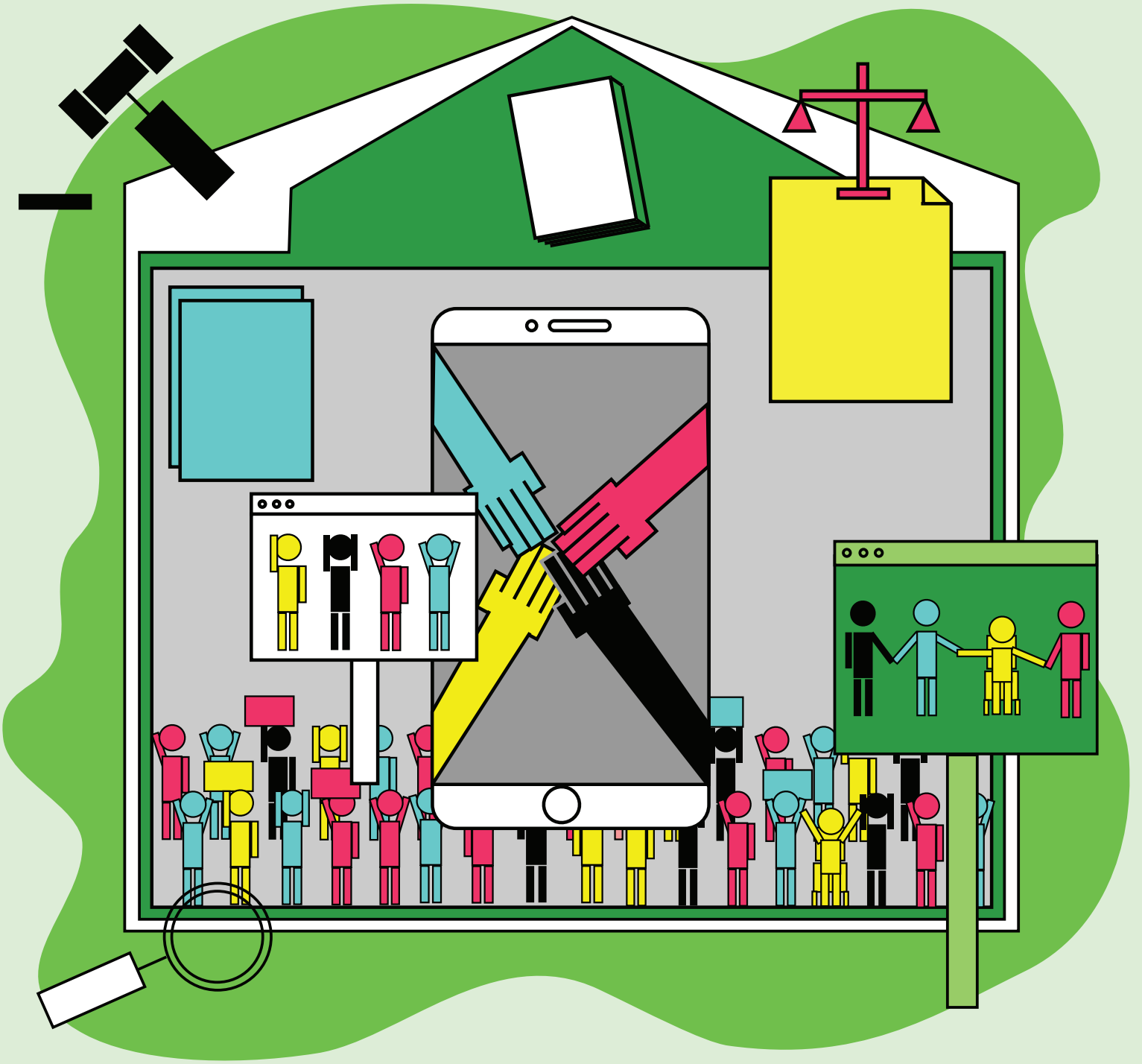
Defending peaceful assembly and association in the digital age

takedowns, shutdowns, and surveillance



accessnow

Access Now 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, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

Defending peaceful assembly and association in the digital age:

takedowns, shutdowns, and surveillance

JULY 2020

This is an Access Now publication. It is written by Laura O'Brien and Peter Micek. The authors would like to thank the Access Now team members who contributed to the report, including Javier Pallero, Alexia Skok, Berhan Taye, Carolyn Tackett, Daniel Leufer, Donna Wentworth, Eliška Pírková, Elizabeth Metts, Eric Null, Estelle Massé, Fanny Hidvégi, Isedua Oribhabor, Juliana Castro, Marwa Fatafta, Natalia Krapvia, Raman Jit Singh Chima, Sage Cheng, and Verónica Arroyo, and to our summer legal and policy interns, Alanna Fichtel, Carolina Gonçalves Berenger, and Emilia Porubcin.

It is important to note that, while this submission draws upon examples from various regions worldwide, these examples are non-exhaustive, and do not represent the lived experiences of all those attempting to exercise their right to freedom of peaceful assembly and of association across the globe. We recognize that further research and data is required to take into account intersecting structures of oppression, including but not limited to, race, gender,[1] ethnicity, sexual orientation, disability, class, language, religion, age, citizenship, and family status.[2]

[1] Noting specifically the situations of transgender people, those with non-binary gender identities, and gender non-conforming people.
[2] See, e.g., efforts like the Initiative for a Representative First Amendment, at https://www.ifrfa.org, Equality Labs, at https://www.equalitylabs.org, and Algorithmic Justice League, at https://www.ajl.org.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

This year, 2020, has revitalized national and international discussions on the rights to freedom of peaceful assembly and of association. Notable examples of such discussions include the aftermath of George Floyd's death, when global masses stood up and forced the world to look in the mirror and address systemic forms of racial injustice, and youth-led movements from Hong Kong to Sudan that sustained defiance in the face of repression.

With social distancing measures in place as a result of COVID-19, various assemblies and associations have creatively sought to restrategize, equip, and empower themselves for a physical and online existence during the pandemic.[3] From car and bike protests,[4] to clapping, dancing, and cheering outside of windows and balconies for essential workers,[5] physical assemblies and associations have taken unique forms for meaningful civic engagement. In a similar vein, COVID-19 has demonstrated the importance of digital technologies, namely the internet and information and communication technologies (ICTs), in exercising freedom of peaceful assembly and of association online.[6] Amid COVID-19, climate activist Greta Thunberg, for instance, encouraged young activists — who have grown up online — to use the digital tools they are so familiar with to participate in a "digital strike" instead of physical public gatherings in order to keep up public pressure on governments to fight against climate change.[7] Overall, the COVID-19 pandemic has reemphasized that the world is no longer connected *only* through physical assemblies and associations. Rather, we gather and connect online — across physical borders — to voice opinions, call to action, express solidarity, and access important, life-saving information during unprecedented times.

The internet and ICTs serve as enablers of human rights.[8] In 2011, the U.N. Special Rapporteur on freedom of expression noted that "the internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information,

[3] Anthony Faiola, "Coronavirus chills protests from Chile to Hong Kong to Iraq, forcing activists to innovate," *The Washington Post*, April 4, 2020, https://www.washingtonpost.com/world/the_americas/coronavirus-protest-chile-hong-kong-iraq-lebanon-india-venezuela/2020/04/03/c7f5e012-6d50-11ea-a156-0048b62cdb51_story.html
[4] Samantha Melamed, "Protesting in the time of social distancing: Philly demands action by car, bike, text, and tweet," *The Philadelphia Inquirer*, March 30, 2020, https://www.inquirer.com/health/coronavirus/protest-philadelphia-jails-social-distancing-coronavirus-covid-19-20200330.html
[5] Amanda Hess, "In Praise of Quarantine Clapping," *The New York Times*, April 9, 2020. https://www.nytimes.com/2020/04/09/arts/virus-quarantine-clapping.html
[6] Laurie Goering, "As coronavirus drives climate protests off streets, activists go online," *Reuters,* March 20, 2020. https://www.reuters.com/article/us-health-coronavirus-climate-change/as-coronavirus-drives-climate-protests-off-streets-activists-go-online-idUSKBN2170MM
[7] Zack Colman, "Climate activists shift gears in an age of 'social distancing," *POLITICO*, March 19, 2020. https://www.politico.com/news/2020/03/19/climate-activists-social-distancing-coronavirus-137216; Zoey Shipley, "Using Social Media as the Platform for Protesting in an Age of Social Distancing," *Our Daily Planet*, March 22, 2020. https://www.ourdailyplanet.com/story/using-social-media-as-the-platform-for-protesting-in-an-age-of-social-distancing/
[8] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, U.N. Doc. A/HRC/17/27 (16 May 2011). https://undocs.org/en/A/HRC/17/27, para 22-23.

and for facilitating active citizen participation in building democratic societies."[9] Take for instance, the Arab Spring revolutions in the Middle East and North Africa between 2010 and 2012, when activists inspired the world in forging new links between on- and offline action and redefining the online civic space to one where individuals and groups can voice concerns, share information, and organize for collective action.[10] Thus, states must facilitate universal, affordable, open, secure, and stable access to the internet and ICTs to enable rights holders to fully exercise their human rights, such as the rights to freedom of peaceful assembly and of association.

Yet, the closing of online civic space has impacted the rights to freedom of peaceful assembly and of association online and off. Previously decentralized and open platforms and tools have now become restricted, with individuals and communities subject to privatization (i.e. the profit motive, monopolistic tendencies, and discriminatory policies without redress or oversight), censorship, harassment, surveillance, and persecution that deter the use of ICTs as tools of protest and associating online. For example, in the past year, we witnessed the prevalence of surveillance of Black Lives Matter activists in the United States, the internet shutdown accompanying a brutal crackdown on peaceful Sudanese protesters, and the proposed sale of the .ORG domain, to name a few.

International and national laws recognize that extraordinary circumstances require extraordinary measures. This means that certain fundamental rights, including the rights to freedom of peaceful assembly and of association may be restricted — to address for instance, public order, public safety, national security interests, or the protection of morals or public health, as amplified in the current COVID-19 pandemic — as long as basic democratic principles and a series of safeguards are applied, and the interference is lawful, proportionate, limited in time and scope, and not arbitrary.[11] Nonetheless, according to data collected from Access Now and the #KeepItOn campaign — a coalition of over 220 organizations from 99 countries worldwide dedicated to combating internet shutdowns — found that "in 2019, the most commonly observed cause of internet shutdowns were protests."[12] This data indicates that when a state "says it is cutting access to restore 'public safety,' in reality it could mean the [state] anticipates protests and may be attempting to disrupt people's ability to organize and speak out, online or off."[13] Moreover, police authorities and other state departments have been given wide powers and emergency

[9] Ibid., para 2; United Nations Human Rights Council, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai*, U.N. Doc. A/HRC/20/27 (21 May 2012). https://undocs.org/A/HRC/20/27, para 84 (k). See also United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, U.N. Doc. A/HRC/32/38 (11 May 2016) https://undocs.org/A/HRC/32/38, at para 8.
[10] Access Now. *Five years later: the internet shutdown that rocked Egypt*, 2016. https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/
[11] International Covenant on Civil and Political Rights (ICCPR) Dec. 19 1966, 999 U.N.T.S. 171 and 1057 U.N.T.S. 407 (entered into force 23 March 1976). https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf, Articles 21-22.
[12] Access Now. *Targeted, Cut Off, and Left in the Dark: The #KeepItOn report on internet shutdowns in 2019*, 2020. https://www.accessnow.org/keepiton-2019-report, at page 13.
[13] Ibid.

measures during COVID-19, which are unfortunately being used by some to restrict lawful and legitimate exercises of association and assembly. Some states are prosecuting individuals and journalists under "fake news" laws or epidemic-related laws during the pandemic. Protesters are hit with even more severe restrictions. Web messaging and social media services are subject to censorship and monitoring demands by some state authorities under the cover of combating COVID-19-related disinformation or "fake news."

The COVID-19 pandemic will inevitably unearth an aftermath. The measures states put in place now will determine this aftermath. State responses must therefore promote public health, prevent discrimination, ensure access to reliable and timely information, defend unrestricted access to a universal, open, affordable, stable and secure internet, ensure the enjoyment of the rights to freedom of expression and of opinion, of peaceful assembly and of association, and protect privacy and personal data. Access Now is committed to protecting human rights and contributing to states' responses to the COVID-19 pandemic and beyond.

It is in this global context — the rise of internet shutdowns worldwide, the prevalence of unlawful surveillance, increases in privatization, and the impact of the COVID-19 pandemic — that we chose to examine the state of the rights to freedom of peaceful assembly and of association from a digital rights perspective. Where have we come from, particularly since Arab Spring? Where are we currently, noting the momentum of Black Lives Matter protests both within and beyond U.S. borders? And finally, where are we heading with the impact of COVID-19?

This paper examines three current issues: (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. It is beyond the scope of this paper to address the nuance of this topic, particularly in a rapidly changing global context. Therefore, the authors would like to make two important caveats. First, in response to the current global context, this paper mainly emphasizes and focuses on the right to freedom of peaceful assembly — with particular attention to collective protests that are protected under international human rights law — noting that more space is needed to fully assess the right to freedom of association. Second, this paper speaks to timely topics, and some information will require further updates and research. We provide an overview of each of the three topics mentioned followed by case studies and specific guidance for states, the private sector, and international institutions, for each topic discussed. Overall, this paper, supported by case studies from regions across the world, aims to provide an overview of the state of the rights to freedom of peaceful assembly and of association in the digital age and a series of tailored recommendations for various stakeholders.

II. INTRODUCTION

The rights to freedom of peaceful assembly and of association are enshrined in Article 20 of the Universal Declaration of Human Rights, and affirmed in the U.N. International Covenant on Civil and Political Rights (ICCPR), under Articles 21 and 22, respectively.[14] The U.N. Human Rights Committee, a body of independent experts that monitors implementation of the ICCPR and interprets the treaty's meaning is currently underway shaping — for the first time — a General Comment No. 37 on Article 21, the right of peaceful assembly.[15] This timely legal instrument will serve to interpret Article 21. More importantly, this General Comment, as it stands, will update the interpretation of Article 21 from when it was originally drafted in 1966. This is a welcomed and necessary update since the nature of assemblies has undergone substantial change since the inception of the ICCPR, particularly regarding the use of digital technologies worldwide. The General Comment will therefore play a significant role in advising state parties and other stakeholders on the right to peaceful assembly in online spaces. Additionally, the General Comment should highlight the potential risks such as the increase in internet shutdowns, barriers to internet access, prevalence of unlawful surveillance, and unaccountable privatization of spaces of assembly, all of which unduly curtail the right to peaceful assembly. This paper assesses these rights through the international human rights legal framework, drawing upon regional and domestic examples in support of its position and to provide recommendations to guide international organizations such as the U.N.

Like all human rights, the rights to freedom of peaceful assembly and of association, are universal, indivisible, interdependent, and interrelated.[16] While the right to freedom of peaceful assembly and the right to freedom of association are often discussed in tandem, it is important to recognize they are two separate rights, often governed by different domestic legislation.[17] For instance, the General Comment narrows in specifically on Article 21 — freedom of peaceful assembly. Nonetheless, association is important, particularly in labor contexts and the formation of online communities of identity and political action.

Freedom of peaceful assembly and of association are fundamental human rights, not only in democratic states, but also authoritarian ones. As captured by the U.N. Special Rapporteur on

[14] General Assembly Res. 217 (III) A, Universal Declaration of Human Rights, (10 December 1948). https://undocs.org/A/RES/217(III); ICCPR, *supra* note 9.
[15] U.N. Human Rights Committee, *Second Reading of Draft 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
[16] World Conference on Human Rights in Vienna, *Vienna Declaration on Programme of Action,* (25 June 1993). https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx;
[17] Maina Kiai, *supra* note 7, at para 4.

freedom of assembly and association, such assemblies and associations can serve as "a barometer for measuring the situation pertaining to, and the enjoyment of, human rights in any given country and a useful proxy for how open or closed countries and their national institutions are."[18] Interference with assemblies and associations serves as an early warning sign that the state is not meeting the needs and interests of the public.[19] Assemblies and associations, and the response they garner, draw attention to the need for state accountability, as well as the accountability of other powerful actors, such as corporations, who heavily influence society and impact fundamental rights and who, under the international human rights framework, are called on to respect human rights.[20]

Such a barometer can lead to action at both the local and international levels. For example, after a request from the African Group — which represents 54 member states from the African continent — the U.N. Human Rights Council hosted an urgent debate on the current racially inspired human rights violations, systemic racism, police brutality against people of African descent, and violence against peaceful protest.[21] States and over 600 civil society organizations worldwide pressured the U.N. to adopt a resolution responding to the police murder of George Floyd and countless other Black Americans. On June 19, 2020 — also known as Juneteenth, the day celebrating emancipation from enslavement in the U.S. — the resolution was adopted by consensus.[22] While a historic move in many respects, the final resolution remained diluted of the original hope of the hundreds of civil society organizations that called for its urgency.[23] Yet, as Gay MacDougall, former U.N. Independent Expert on minority issues, notes, "this is a significant step forward in a continuing struggle."[24]

---

[18] General Assembly Res. 72/135, *Rights to freedom of peaceful assembly and of association*, U.N. Doc. A/72/135 (14 July 2017). https://undocs.org/A/72/135, at para 17.

[19] U.N. Human Rights Committee*. Half-Day General Discussion in preparation for a General Comment on Article 21 (Right of Peaceful Assembly) of the International Covenant on Civil and Political Rights, Palais Wilson, 20 March 2019 - Article 19 written contribution.* https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GC37.aspx, at para 10.

[20] OHCHR, *Guiding Principles on Business and Human Rights*, HR/PUB/11/04 (16 June 2011). https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[21] ACLU, *Coalition Letter - Request for U.N. independent inquiry into escalating situation of police violence and repression of protests in the United States*, 2020. https://www.aclu.org/letter/coalition-letter-request-un-independent-inquiry-escalating-situation-police-violence-and This comes alongside similar advocacy efforts from other civil society organizations and international experts . U.N. Special Procedures. *Statement on the Protests against Systemic Racism in the United States*, 2020. https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25927&LangID=E; and Deutsche Welle, *UN agrees to urgent debate on racism and police violence,* 2020. https://www.dw.com/en/un-agrees-to-urgent-debate-on-racism-and-police-violence/a-53807879

[22] The final resolution calls on the High Commissioner to prepare a comprehensive report on systemic racism, policing practices such as those that led to the killing of George Floyd, violence against protesters, and related incidents globally. UN News. *Human Rights Council calls on top UN rights official to take action on racist violence*, 2020. https://news.un.org/en/story/2020/06/1066722

[23] Human Rights At Home Blog*, The UN Makes Unprecedented Response to George Floyd's Murder*, 2020. https://lawprofessors.typepad.com/human_rights/2020/06/the-un-makes-unprecedented-response-to-george-floyds-murder.html

[24] Ibid.

Indeed, assemblies and associations have historically played a pivotal role in deconstructing systemic forms of racism, decolonization, self-determination, addressing women's inequality, and LGBTQ struggles, among others. For instance, the LGBTQ community has advanced LGBTQ rights by taking to the streets — including at the 1969 Stonewall Riots, when Black trans individuals in Greenwich Village famously stood up to police harassment and the tradition of Pride was born.[25]

As stated previously, while the rights to freedom of peaceful assembly and of association are often used interchangeably, it is important to note that they are also two separate rights.[26] This section therefore briefly examines the rights separately.

THE RIGHT TO FREEDOM OF PEACEFUL ASSEMBLY

Assemblies, most commonly understood as protests, take many forms. Assembly has been defined as "an intentional and temporary gathering in a private or public space for a specific purpose."[27] According to international bodies, freedom of assembly covers a wide range of gatherings, whether static or in motion and whether held on private or public property, including streets and highways.[28] In fact, the Supreme Court of California held that the particular shopping center at issue was treated as a public forum. This case therefore establishes that constitutional speech and petition rights might be protected in a privately owned shopping center.[29] Additionally, in a case brought before the Supreme Court of New Jersey, the court acknowledged that the shopping center had displaced the downtown

[25] Access Now. *Standing together in Pride*, 2020. https://www.accessnow.org/standing-together-in-pride/
[26] Maina Kiai, *supra* note 7, at para 4.
[27] Ibid., at para 24.
[28] Organization for Security and Cooperation in Europe. *Benchmarks for Laws related to Freedom of Assembly and List of International Standards*. https://www.osce.org/files/f/documents/5/d/37907.pdf, at para. 6; see *Rassemblement Jurassien & Unité Jurassienne v Switzerland*, Application No 8191/78 (1979) ECtHR. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-74721&filename=001-74721.pdf; see *Christians against Racism and Fascism v United Kingdom*, Application No 8840/78 (1980) ECtHR. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-74287%22]}; see *Anderson and Nine Others v United Kingdom*, Application No 33689/96, 25 EHRR CD 172 (1997). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-3988%22]}; see *Djavit An v. Turkey*, Application No 20652/92 (2003) ECtHR. http://hudoc.echr.coe.int/eng?i=001-60953; see *Kudrevičius and others v. Lithuania*, Application No 37553/05 (2015) ECtHR. https://hudoc.echr.coe.int/eng#{%22docname%22:[%22Kudrevi%C4%8Dius%20and%20others%20v.%20Lithuania%22],%22itemid%22:[%22001-158200%22]}. Importantly, the ECtHR note that "the practice whereby the authorities allow an assembly to take place, but only at a location which is not within sight and sound of its target audience and where its impact will be muted, is incompatible with the requirements of Article 11 of the Convention"; see *Lashmankin v Russia*, Application No 57818/09 (2017) ECtHR. https://hudoc.echr.coe.int/rus?i=001-170857, at § 426.
[29] *Pruneyard Shopping Ctr v Robins*, 447 U.S. 74 (1980). https://supreme.justia.com/cases/federal/us/447/74/#tab-opinion-1953647 It is important to note that this case, and cases that followed, made it clear that this decision did not apply to all shopping centers. While this decision was appealed, the United States Supreme Court held that "a State … may adopt reasonable restrictions on private property so long as the restrictions do not amount to taking without just compensation or contravene any other federal constitutional provision." In this specific case, the Court further held that petitioning did not amount to a "taking" because the activity did not "unreasonably impair the value or the use of [the] property as a shopping center." Importantly, the U.S. Supreme Court affirmed that, in this situation, compelling the owner to accommodate other speakers did not infringe the owner's constitutional rights.

business area as the center of commercial activity and held the center could not deny the right to use the space as an invited public forum.[30]

International human rights law upholds the right to "peaceful" assembly — an unusual qualifier.[31] As a result, states are prone to narrowly interpret the term "peaceful" to limit the scope of the right.[32] While the term "peaceful" has been applied mainly to offline assemblies, the spectrum between offline and online worlds is increasingly fluid. All stakeholders involved in demonstrations — from press to police and protesters — may use digital technologies. Often, they try to respond to or control the other's use.

Regional courts and existing international standards provide important interpretations of "peaceful" assembly. The European Court of Human Rights (ECtHR) has sought to "avert the risk of a restrictive interpretation" of the right to freedom of peaceful assembly, refraining "from formulating the notion of an assembly … or exhaustively listing the criteria which would define it."[33] Similarly, *The Right to Protest: Principles on the protection of human rights in protests* (*The Right to Protest Principles*), a set of principles established by civil society organization ARTICLE 19, equates "peaceful" with "nonviolent" to counter states' narrow interpretation that could restrict the right.[34] In its written submission to the U.N. Human Rights Committee half-day general discussion in preparing for a General Comment on Article 21 (Right of Peaceful Assembly), ARTICLE 19 maintains that, in determining whether an assembly is "peaceful," this assessment should be conducted on a case-by-case basis, bearing in mind the context, particularly (1) the intent of the organizers and participants and (2) the likelihood of significant violence and/or property damage. This should be considered on a high-threshold scale affording the maximum protection to the right to freedom of

[30] *New Jersey Coalition Against War in the Middle East v. J.M.B. Realty Corp*, A-124/125-93 (NJ 1994). The Court relied on the balancing factors as set out in *State v Schmid*. For information on the international level see e.g. U.N. Human Rights Council, *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*, U.N. Doc. A/HRC/31/66 (4 February 2016) https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/018/13/PDF/G1601813.pdf?OpenElement, at para 84. And regional level see *Appleby v. the United Kingdom*, Application No. 44306/982003) ECtHR. https://hudoc.echr.coe.int/eng#{%22appno%22:[%2244306/98%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-61080%22]}

[31] Note that in the African regional context, the "peaceful" qualifier is not there.

[32] Similar qualifier is noted in regional and domestic legal frameworks, with the exception of the African Charter on Human and People's Rights which under Article 11 guarantees "the right to assemble freely" without reference to "peaceful."

[33] *Navalnyy v Russia*, Application Nos. 29580/12 and four others, [GC] (2018) ECtHR. https://hudoc.echr.coe.int/eng#{%22docname%22:[%22Navalnyy%20v%20Russia%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-187605%22]}, at para 98.

[34] Article 19. *The Right to Protest: Principles on the protection of human rights in protests*, 2016. https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf For more information, see principle 1.2 of the Right to Protest Principles, which elaborates a set of four considerations that should be taken into account when interpreting "peaceful" or "non-violent" to afford the widest possible human rights protection for peaceful assemblies.

peaceful assembly while bearing in mind the conduct within the scope may still be subject to limitations under Article 21.[35]

This twofold assessment is particularly relevant in the digital context. For instance, consider online tactics that can be disruptive, misleading, or potentially vandalizing. A growing range of activities, such as "Zoom-bombing," coined after the Zoom online video platform, may violate either the private platform's terms of use or criminal law.[36] Yet, in some circumstances, could these disruptions be considered a legitimate form of expressive dissent? Depending on the context and nature of the disruption, Zoom-bombing could look more like a flash mob or outburst at a campaign rally or private event, to express dissent and disrupt the power dynamics inherent in certain conversations. Overall, it seems clear that civil disobedience will continue in the digital age, and tactics will evolve constantly as digital technologies also develop. The intention of the organizer — whether to dissent, which may fall within the scope of the right, or rather, simply to disrupt, troll, and impede others — is therefore a key consideration. Similarly, the meaning or likelihood of "significant" damage must also be taken into consideration. Does Zoom-bombing or similar digital disruption amount to "significant" damage? If so, to whom, to what extent, and for how much time? The nuance surrounding such questions requires further research.

Importantly, as ARTICLE 19 further notes, even if those participating "in an assembly engage in acts of violence or property damage, this should not be enough to [automatically] categorize the assembly as 'not peaceful' and therefore deprive all participants their right of peaceful assembly."[37] In fact, in 1980, the European Commission on Human Rights opined that:

> The possibility of violent counter-demonstrations or the possibility of extremists with violent intentions, not members of the organising association, joining the demonstration cannot as such take away the right [to peaceful assembly]. Even if there is a real risk of a public procession resulting in disorder by development outside the control of those organizing it, such procession does not for this reason alone fall outside the scope of Article 11 (1).[38]

Rather, it is the intention to hold a peaceful assembly that is significant in determining whether the assembly falls within the scope of the right, not the likelihood of violence, because of the reactions of other groups or other factors.[39] *The Right to Protest Principles* make a further claim that "states should acknowledge that whenever a protest ended in

[35] U.N. Human Rights Committee, *supra* note 19, at para 16.
[36] For more information, see Lawfare. *Prosecuting Zoom-Bombing*, 2020. https://www.lawfareblog.com/prosecuting-zoom-bombing
[37] U.N. Human Rights Committee, *supra* note 19, at para 18.
[38] *Christians against Racism and Fascism v United Kingdom*, *supra* note 28, at page 148; *Anderson and Nine Others v United Kingdom*, *supra* note 28.
[39] *See* Maina Kiai, *supra* note 7, at para 25.

violence, it was due to the state's failure to effectively facilitate peaceful protest, prevent violence, and engage in conflict resolution with those who were likely or intended to engage in violence."[40] This state responsibility follows online, where cyber attacks on civil society shrink civic space and harm democratic mobilization. Disruption may be used for legitimate protest, but also — and likely more often — to suppress human rights and democratic functioning.

THE RIGHT TO FREEDOM OF ASSOCIATION

According to the U.N. Special Rapporteur on freedom of assembly and association, "association refers, inter alia, to civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, foundations, or even online associations as the [i]nternet has been instrumental, for instance, in 'facilitating active citizen participation in building democratic societies."[41] In particular, associations can be ad hoc, for a specific cause or issue, and over different periods of time. The right to freedom of association equally protects associations that are registered and unregistered.[42]

THE RIGHTS TO FREEDOM OF PEACEFUL ASSEMBLY AND OF ASSOCIATION ONLINE

The U.N. Human Rights Council has declared that the same rights that people have offline must also be protected online.[43] The U.N. General Assembly has further called on states to "ensure that the same rights that individuals have offline … are fully protected online, in accordance with human rights law."[44] The internet, particularly social media, and other ICTs have facilitated the enjoyment of the rights to freedom of peaceful assembly and of association both on and offline. According to the Association for Progressive Communications (APC), association online "refers to the act of forming groups, including informal ones, online, with or without moderators or group leaders."[45] Similarly, peaceful assembly online refers to "an intentional and temporary gathering in a private or public space for a specific purpose that includes the acts of coordinating, organising, gathering, planning,

[40] Article 19. *The Right to Protest: Principles on the protection of human rights in protests*, 2016. https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf, at 1.2 (d).
[41] Maina Kiai, *supra* note 7, at para 52.
[42] Ibid., at para 56.
[43] U.N. Human Rights Council, Res. 38/l.10, *The promotion, protection and enjoyment of human rights on the Internet*, U.N. Doc. A/HRC/38/L.10/Rev.1 (4 July 2018). https://undocs.org/en/A/HRC/38/L.10/REV.1; U.N. Human Rights Council, Res. 24/5, *The rights to freedom of peaceful assembly and association,* U.N. Doc. A/HRC/RES/24/5 (8 October 2013). http://freeassembly.net/wp-content/uploads/2013/08/A-HRC-RES-24-5-ENG.pdf, at para 2.
[44] U.N. General Assembly, Res. 73/173, *Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association*, U.N. Doc. A/HRC/Res/73/173 (8 January 2019) https://undocs.org/en/A/RES/73/173 at para 4. For a notable regional example affirming these rights in the online context, see the African Declaration on Internet Rights and Freedoms at African Declaration Group. *African Declaration on Internet Rights and Freedoms*, 2015. https://africaninternetrights.org/articles/
[45] Venkiteswaran, G., Association for Progressive Communications (APC). *Freedom of assembly and association online in India, Malaysia and Pakistan: Trends, challenges and recommendations*, 2016. https://www.apc.org/sites/default/files/FOAA_online_IndiaMalaysiaPakistan.pdf, at page 13.

or meeting on platforms available online such as instant messaging, voice over internet protocol, chat applications, email groups, and mailing lists, among others."[46]
Various online techniques and tools are used to further enable the rights to freedom of peaceful assembly and of association online.[47] In 2019, the U.N. Special Rapporteur on freedom of assembly and association, Clément Voule, released a timely report on the exercise of the rights to freedom of peaceful assembly and of association in the digital age to the U.N. Human Rights Council.[48] In his report, Voule addressed the intersection of digital technologies and peaceful assembly and association, noting worldwide examples that "demonstrate the power of digital technology in the hands of people looking to come together to advance democracy, peace, and development."[49] For instance, hashtags are commonly used to share information, mobilize individuals, and gather worldwide support.[50] End-to-end encryption technologies, pseudonyms, and other digital security features empower individuals to operate in a safe digital space to connect and mobilize without undue interference.[51] Finally, petitions and crowdfunding platforms are circulated through social media to reach new audiences, enable greater participation, and spread information worldwide.[52] Take, for instance, young people's efforts worldwide to use social media platforms, such as TikTok, to mobilize against injustice. Most recently, fans of South Korea's pop music scene, known as K-pop, engaged in online activism to support the Black Lives Matter movement. In addition to using social media to collect donations — raising $1 million for Black Lives Matter-associated organizations — K-pop fans took action to "foil police operations" aimed at identifying Black Lives Matter protesters "by urging fans to submit their fancam footage to a U.S. police department" and to hijack racist hashtags.[53] These groups' activism gained increasing attention following recent news regarding U.S. President Donald Trump's sparse rally attendance in Tulsa in mid-June. TikTok users and K-pop fans revealed that they "mobilized to request tickets, inflating expectations for turnout."[54] As Marshall McLuhan, a famous Canadian philosopher, claims, "the medium is the message." Access to the internet and digital technologies is therefore key to repurposing digital tools for unique and creative modes of protest and organizing. Overall, these online mobilization efforts highlight the

[46] Ibid., at page 13.
[47] U.N. Human Rights Council, Res. 21/16, *The rights to freedom of peaceful assembly and of association*, U.N. Doc. A/HRC/RES/21/16 (11 October 2012). https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/174/63/PDF/G1217463.pdf?OpenElement
[48] U.N. Human Rights Council, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Voule*, U.N. Doc. A/HRC/41/41 (17 May 2019). https://undocs.org/A/HRC/41/41
[49] Ibid., at para 2.
[50] Ibid., at paras 22-23, 43.
[51] Ibid., at para 24.
[52] Ibid., at para 25.
[53] The Guardian. *Digitally-savvy and passionate, K-pop fans' Trump activism should come as no surprise,* 2020. https://www.theguardian.com/commentisfree/2020/jun/22/digitally-savvy-and-passionate-k-pop-fans-trump-activism-should-come-as-no-surprise
[54] Ibid.

momentum such activism and associations have built by harnessing digital tools to advance the exercise of peaceful assembly and association in the digital age.

PERMISSIBLE RESTRICTIONS UNDER INTERNATIONAL HUMAN RIGHTS LAW

The rights to freedom of peaceful assembly and of association are not absolute rights, and international standards allow for certain restrictions under limited and narrowly defined circumstances.[55] Both Article 21 and Article 22(2) of the ICCPR respectively state "no restriction may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others."[56] Restrictions must not contradict the purpose of the right and must be proportionate and "necessary in a democratic society."[57] Article 22 (2), the right to association, adds an additional caveat that this "shall not prevent the imposition of lawful restrictions on members of the armed forces and of the police in their exercise of" the right to association.[58] The U.N. Special Rapporteur on freedom of assembly and association, Clément Voule, emphasizes that, in the digital context, "the freedom to access and use digital technologies for the exercise of peaceful assembly and association rights should be viewed as the rule, and the limitations as the exception."[59]

At the time of writing, 173 countries have ratified the ICCPR, thereby affirming the rights to freedom of peaceful assembly and of association. Yet state parties to the ICCPR include countries that have unduly restricted the exercise of such rights both on- and offline, including, for instance, the United States, Egypt, Tunisia, Sudan, Iran, Syria, China, Cuba, Ethiopia, and Vietnam.[60] The next section examines specific case studies from these and other domestic contexts to support recommendations to states, companies, and international organizations.

---

[55] American Association for the International Commission of Jurists. *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 1984. https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf
[56] ICCPR, *supra* note 9., Articles 21 and 22; U.N. Human Rights Council, Res. 15/21, *The rights to freedom of peaceful assembly and of association*, U.N. Doc. A/HRC/RES/15/21 (6 October 2010). https://undocs.org/en/A/HRC/RES/15/21
[57] Maina Kiai, *supra* note 7, at para 16.
[58] ICCPR, *supra* note 9, Article 22.
[59] Clément Voule, *supra* note 48, at para. 12.
[60] OHCHR. *Status of Ratification Interactive Dashboard*. https://indicators.ohchr.org/
It is important to note that some of these countries listed, such as the United States, Egypt, Sudan, Syria, China, Ethiopia, and Vietnam have taken no action to sign or ratify the Optional Protocol to the ICCPR.

III. ACCESS, CONNECTIVITY, AND INTERNET SHUTDOWNS

States are increasingly shutting down access to the internet and communications services during public demonstrations. An internet shutdown happens when someone — usually a state — intentionally disrupts the internet or mobile apps to control what people say or do. Internet shutdowns are also sometimes called "blackouts" or "kill switches."[61]

Internet shutdowns are a blatant tool employed by states to quell protests and dissent. According to data collected by Access Now and the #KeepItOn coalition, "in 2019, the most commonly observed cause of internet shutdowns were protests."[62] This data indicates that when a state "says it is cutting access to restore 'public safety,' in reality it could mean the [state] anticipates protests and may be attempting to disrupt people's ability to organize and speak out, online or off."[63] Internet shutdowns restrict access to vital information and harm the fundamental right to freedom of expression. Internet shutdowns also prevent communication between protesters and block them from sharing footage of the demonstrations. For instance, in 2017, Access Now and WITNESS issued a letter to major wireless carriers, outlining concerns that the networks would be overwhelmed and congested as a result of protests during President Trump's inauguration weekend, thereby preventing protesters and journalists from documenting demonstrations.[64] Furthermore, protesters may be prevented from reaching emergency and medical services, accessing life-saving information, and reaching family and friends in the country and abroad.

The free flow of information is essential during times of civil unrest, but internet shutdowns prevent journalists from reporting on the situation on the ground. Media may be blocked from speaking with their sources and sharing the reality of the violence and human rights violations committed by security forces during the protests. Take, for instance, the #IAmTheSudanRevolution demonstrations. In June 2019 — within a week of Sudan's shutting down the internet — 100 people were killed, over 700 injured, and at least 70 raped.[65] The

[61] A more technical definition of internet shutdowns, as developed by experts, explains that "an internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." Access Now, *supra* note 10, at FN 1.
[62] Ibid., at page 13.
[63] Ibid.
[64] The Hill. *Cellphone providers brace for heavy inauguration use*, 2017. https://thehill.com/policy/technology/315187-cellphone-providers-brace-for-heavy-inauguration-use; Access Now. *Re: Ensure internet connectivity for events and demonstrations during weekend of presidential inauguration*, 2016. https://www.accessnow.org/cms/assets/uploads/2017/01/Mobile_Internet_AccessNow_Witness12-21.pdf
[65] Access Now. *#IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan!*, 2019.

shutdown made it extremely difficult for journalists to shed light on the high number of human rights violations committed throughout the week as they occurred.

> Many local and international media houses were unable to speak with their sources and informants, file their stories, and verify the many videos that were posted online. Notably, the alternative forms of communications, SMS and mobile phone calls, were insecure, [putting] journalists, activists, human rights defenders, and even emergency service providers in danger.[66]

Overall, internet shutdowns damage education, as well as economic and health outcomes during times of protest. Internet shutdowns specifically exacerbate these impacts during an unprecedented global health crisis where access to health information is vital to save lives.[67]

State restrictions on the rights to freedom of peaceful assembly and of association, especially internet shutdowns, do not comply with international human rights standards.[68] In fact, in 2015, major U.N. and international human rights experts declared that internet shutdowns are absolutely impermissible under international human rights law, even in times of conflict. [69] Other courts of law, including the ECtHR, have ruled that overbroad restrictions or blocking orders that inhibit access to entire web services or domains cannot be held to be proportionate restrictions to internationally protected fundamental rights under human rights law.[70] These critical court decisions reiterate that states can no longer justify ordering telecommunications companies to shut off mobile or internet services in the face of social unrest or protest, and they have the power to impact the rights of people protesting worldwide.

Related, but distinct from internet shutdowns, is the issue of internet connectivity. Internet connectivity ensures that individuals can communicate and access the information they need to fully exercise their human rights, including their rights to freedom of peaceful assembly and of association. However, the reality is that, as states intentionally disconnect citizens from the internet to stifle dissent and peaceful assembly, they also inadvertently, and at times deliberately, neglect to invest in infrastructure that would enable people to connect to the internet. Similar to other critical infrastructures like healthcare, roads, and more, the infrastructures that enable internet connections are missing in areas that are on the margins.

---

https://www.accessnow.org/iamthesudanrevolution-theres-a-direct-link-between-internet-shutdowns-and-human-rights-violations-in-sudan/

[66] Ibid.

[67] Access Now. *#KeepItOn: Internet shutdowns put lives at risk during COVID-19*, 2020. https://www.accessnow.org/keepiton-internet-shutdowns-put-lives-at-risk-during-covid-19/

[68] Frank La Rue, *supra* note 6, at para 79.

[69] Access Now. *Internet kill switches are a violation of human rights law, declare major UN and rights experts*, 2015. https://www.accessnow.org/internet-kill-switches-are-a-violation-of-human-rights-law-declare-major-un/

[70] Access Now. *#KeepItOn: Keeping the internet open and secure in Hong Kong*, 2019. https://www.accessnow.org/keeping-internet-open-in-hong-kong/

Internet connectivity is essential for economic, social, cultural, political, and civic participation in the digital age. Since more than 3.6 billion people worldwide lack access to the internet, the largest stakeholder group in these efforts remains disconnected, likely marginalized, rarely consulted, and dangerously at risk of being left behind.[71] This is particularly problematic given the disproportionate number of marginalized individuals and groups who remain disconnected. Such individuals and groups therefore cannot use digital technologies to access information and communicate with others about protests and other ways of assembling on- and offline to hold states and other powerful actors accountable for systemic inequalities and injustice. Scientific researchers have found "a strong and persistent political bias in the allocation of Internet coverage across ethnic groups worldwide."[72] In addition to ethnicity, other indicators impacting an individual's access to the internet, including race, must also be considered. For instance, according to the Pew Research Center, in the United States "92% of Whites nationally used the internet in 2019, compared to 85% of Blacks and 86% of Hispanics."[73] Examining individual experience with intersecting digital divides, such as race and ethnicity, therefore challenges "the frequent assumption that the uneven global distribution of digital technology can be mitigated by economic forces and incentives," like competition and smart regulation — or deregulation — of telecommunication companies.[74]

Such analyses are particularly imperative when discussing access to the internet, and the social, economic, and health consequences arising from the COVID-19 pandemic and its aftermath. 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, the internet blackout during protests in Zimbabwe in 2019 cost the country an estimated $5.7 million USD per day.[75] Such costs in many states will likely be compounded during and following the COVID-19 pandemic.

---

[71] Access Now. *The Human Rights Principles for Connectivity and Development*, 2016. https://www.accessnow.org/cms/assets/uploads/2016/10/The-Human-Rights-Principles-for-Connectivity-and-Development.pdf; International Telecommunication Union. *New ITU data reveal growing Internet uptake but a widening digital gender divide*, 2019. https://www.itu.int/en/mediacentre/Pages/2019-PR19.aspx

[72] Nils B. Weidmann, Suso Benitez-Baleato, Philipp Hunziker, Eduard Glatz, Xenofontas Dimitropoulos. *Digital discrimination: Political bias in Internet service provision across ethnic groups*, *Science* 353, no. 6304 (9 September 2016): 1151-1155. https://science.sciencemag.org/content/353/6304/1151

[73] Pew Research Center. Internet/Broadband Fact Sheet, 2019. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/; National Telecommunications and Information Administration. *The State of the Urban/Rural Digital Divide*, 2016. https://www.ntia.gov/blog/2016/state-urbanrural-digital-divide

[74] Nils B. Weidmann, Suso Benitez-Baleato, Philipp Hunziker, Eduard Glatz, Xenofontas Dimitropoulos, *supra* note 72.; Access Now. *We can't reach the U.N. goals for sustainable development without the internet*, 2017. https://www.accessnow.org/cant-reach-u-n-goals-sustainable-development-without-internet/

[75] Exx Africa Business Risk Intelligence. *Special Report: The cost of internet shutdowns in Africa*, 2019. https://exxafrica.com/wp-content/uploads/2019/01/SPECIAL-REPORT_-THE-COST-OF-INTERNET-SHUTDOWNS-IN-AFRICA.pdf

The internet is an essential enabler of human rights in the digital age. Some even suggest that access to the internet is a human right.[76] Nonetheless, the COVID-19 pandemic has amplified the discrepancy between those with and without access to a universal, affordable, open, secure, stable internet connection. The U.N. Sustainable Development Goals (SDGs) are a series of ambitious targets to end extreme poverty and tackle climate change for everyone by 2030. According to the Danish Institute for Human Rights, "over 90 percent of the SDG targets are connected to international human rights and labour standards."[77] The 2030 Agenda is grounded in human rights, and protecting human rights is therefore necessary to reach the SDGs. We believe that extending secure and open access to the internet is essential to the exercise of human rights in the digital age, and, in turn, to reaching the SDGs. The SDGs, particularly SDG 9.C, call on Least Developed Countries (LDCs) to bring everyone online by 2020. In our view, this means extending digital literacy and access to the global, open internet, not simply censored, surveilled, limited, or app-based connectivity. The goal is very ambitious, and, with 2020 more than halfway through and amid a global pandemic, now, more than ever, there is a need to mobilize political will to accelerate SDG targets because the world is well behind — and will miss — the well-intended target of SDG 9.C.

Exercising human rights online is particularly important for the realization of women's human rights. As the Office of the High Commissioner for Human Rights (OHCHR) notes in its report on the gender digital divide, "women activists, including women human rights defenders, increasingly rely on [ICTs] to advocate, communicate, mobilize, protect, access information and gain visibility."[78] OHCHR specifically highlights that "as many women human rights defenders still struggle to gain access to online spaces, the need to share devices, use cybercafes and rely on legacy or 'dumb'[79] mobile telephones may impair their rights to freedom of opinion and expression and further contribute to their digital insecurity."[80]

---

[76] OpenGlobalRights. *COVID-19 exposes why access to the internet is a human right*, 2020. https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/
[77] The Danish Institute for Human Rights. *The sustainable development goals (SDGs)*. https://www.humanrights.dk/learning-hub/sustainable-development-goals-sdgs
[78] U.N. Human Rights Council, *Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective - Report of the United Nations High Commissioner for Human Rights,* U.N. Doc. A/HRC/35/9 (5 May 2017). https://undocs.org/A/HRC/35/9, at para 23.
[79] Usually referred to as "feature phones."
[80] U.N. Human Rights Council, *supra* note 78, at para 23; APC. *What are the digital security concerns and threats facing women human rights defenders?*, 2012. https://www.apc.org/en/news/what-are-digital-security-concerns-and-threats-facing-women-human-rights-defenders; Association for Women's Rights in Development, *Our right to safety: women human rights defenders' holistic approach to protection*, 2014, https://www.awid.org/sites/default/files/atoms/files/Our%20Right%20To%20Safety_FINAL.pdf, at page 19. Point of View. *Free To Be Mobile*. https://sgt-57ed.kxcdn.com/wp-content/uploads/2019/03/FTBM_Web_final.pdf, a not-for-profit organization based in India that aims to equip women, girls, and queer and trans persons to freely inhabit digital domains released a report "Free to Be Mobile," which provides 10 stories to capture online violence through the use of mobile phones.

States have a positive obligation to facilitate the exercise of human rights, including in the digital context.[81] Digital divides represent a significant challenge, particularly in some regions of the world. Yet North and Latin American countries should be commended for their recent efforts to address gender divides. According to Doreen Bogdan-Martin, director of the International Telecommunication Union's Telecommunication Development Bureau, "more men than women use the Internet in every single region of the world except the Americas — and I applaud the efforts of policy-makers in the nations of North and Latin America for their success in promoting digital equality."[82]

CASE STUDIES

Extending secure and open access to the internet is essential to upholding human rights in the digital age and to reaching the SDGs. Nonetheless, populations around the world remain offline — often by malicious design — or are limited to censored and surveilled connections. In assemblies, 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, journalists can report stories and reach their sources, and families and friends can check in with their loved ones.[83] Below we highlight the impact of internet shutdowns and connectivity gaps drawing upon specific domestic examples.

Ecuador	**#decreto883 #Ecuador #ParoNacionalEC** In October 2019, the president of Ecuador published Decree 883 that made substantial changes to the Ecuadorian economy in order to comply with the requirements of the International Monetary Fund's loan. The government eliminated the subsidy for fuel prices, which in turn drastically affected the supply of products and the price of transportation, created a fuel shortage and price speculation, and more. Many indigenous groups in the country traveled to the capital and led the protest against these measures[84] as they

[81] U.N. Human Rights Council, Res. 38/7, *The promotion, protection and enjoyment of human rights on the Internet*, U.N. Doc. A/HRC/Res/38/7 (17 July 2018). https://undocs.org/A/HRC/RES/38/7, at para 5.
[82] International Telecommunication Union. *Measuring digital development: facts & figures 2019*, 2019. https://news.itu.int/measuring-digital-development-facts-figures-2019/
[83] Access Now. *#KeepItOn coalition warns internet shutdowns would further hurt Hong Kong*, 2019. https://www.accessnow.org/internet-shutdowns-will-harm-hong-kong/
[84] BBC. C*risis en Ecuador: continúan las protestas mientras el gobierno y el movimiento indígena se preparan para dialogar este domingo*, 2019. https://www.bbc.com/mundo/noticias-america-latina-50009459

did years ago to fight for other causes.[85] While they were traveling, they experienced disruptions to both internet connection and telephone signal. Due to the protests, the government declared a state of emergency, suspended rights, and set a curfew. In this scenario, users of the state internet and mobile service provider Corporación Nacional de Telecomunicaciones reported on October 6 and 7 that it was impossible to send multimedia content over Facebook and WhatsApp, as it was not possible to access the image, audio, and video servers.[86] Some days later on October 12, reports signaled problems in the Claro network at the moment the curfew started.[87]

Ethiopia

#OromoProtests

On June 29, 2020, prominent Oromo musician and social activist, Haacaaluu Hundeessaa, was shot dead by unknown attackers. In response to the unjust killing, numerous protests sprung up in Addis Ababa and other cities in the Oromia region. The protests demanded justice for Hundeessaa and, as they grew in size, culminated in police clashes and military intervention.[88] At the time of writing, at least 239 people have been killed and 3,500 arrested during the anti-government protests.[89] In response to these protests, the government ordered a nationwide internet blackout to quell unrest.[90] The ongoing internet shutdown is substantially impeding journalists, activists, and other relevant actors from monitoring and properly reporting on the crises in the country. During his final interactive dialogue with the U.N. Human Rights Council, David Kaye, the U.N. Special Rapporteur on freedom of expression, called on the Ethiopian government to "end the practice of shutting down the internet, which reinforces marginalization and limits the

[85] El Espectador. *Movimiento indígena en Ecuador: ¿Por qué continúan las protestas?*, 2019. https://www.youtube.com/watch?v=6H7EU66Cj3A
[86] Access Now. *Disrupciones de internet en Ecuador: cómo ocurrieron y cómo eludirlas*, 2019. https://www.accessnow.org/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas/
[87] APC, Taller de comunicación mujer, Digital Defenders Partnership, and LaLibre.net. *Derechos digitales en el contexto de las protestas y movilización social en Ecuador en octubre de 2019. Aporte para la Visita de Observación al Ecuador por parte del Relator Especial para la Libertad de Expresión, Edison Lanza y del Comisionado Luis Ernesto Vargas de la Comisión Inter Americana de Derechos Humanos (CIDH).* https://www.apc.org/sites/default/files/Ecuador_Informe_bloqueos_e_interrupciones_red_octubre2019_CIDH_1.pdf
[88] Access Now. *#KeepItOn: The Ethiopian government must end the arbitrary use of internet shutdowns to quell protests*, 2020. https://www.accessnow.org/keepiton-ethiopian-government-must-end-arbitrary-internet-shutdowns/
[89] The Washington Post. *Ethiopia's week of unrest sees 239 dead, 3,500 arrested*, 2020. https://www.washingtonpost.com/world/africa/ethiopias-week-of-unrest-sees-239-dead-3500-arrested/2020/07/08/8eb30952-c100-11ea-8908-68a2b9eae9e0_story.html
[90] Access Now. *Back in the dark: Ethiopia shuts down internet once again*, 2020. https://www.accessnow.org/back-in-the-dark-ethiopia-shuts-down-internet-once-again/

	public's access to information at critical moments of public debate, health, and protest."[91]
India	**#CAAProtests #KeepUsOnline #LetTheNetWork** In December 2019, the Indian government suspended broadband and mobile data, as well as voice calling services, in several districts of the national capital of Delhi, in addition to districts across several other Indian states and the entire state of Assam. These rights-harming, inherently disproportionate shutdowns came at a time when individuals took to the streets of Delhi to protest the Citizenship Amendment Act — legislation, controversial for its alleged religious discrimination, that was pushed through the Indian parliament on the urging of the Union Government — and the proposed National Population Registry.[92] The government claims that "the decision to suspend the internet was taken in order to prevent misuse of social media platforms to disturb peace and tranquility, and for maintaining law-and-order."[93] Indian media noted the government's communication order citing "law-and-order" "does not fulfill the test of imminent danger to public tranquility that the [domestic] court insists upon when fundamental rights are curbed."[94] The shutdown in the state of Assam was overturned by the state high court.[95] Research from the Cellular Operators Association of India, found that "Indian mobile operators [were] losing around 24.5 million rupees ($350,000) in revenue every hour they are forced to suspend internet services

[91] Freedex. *David Kaye (United Nations Special Rapporteur on Freedom of Expression) - Final reports to Human Rights Council*, 2020. https://freedex.org/2020/07/09/final-reports-to-human-rights-council/
[92] Quartz India. *Over 4,000 hours of internet shutdowns cost India more than $1.3 billion in 2019*, 2020. https://qz.com/india/1781178/internet-shutdowns-over-caa-article-370-cost-india-1-3-billion/; Access Now. *With shutdowns in major cities to silence protests, India tries to black out democracy*, 2019. https://www.accessnow.org/with-shutdowns-in-major-cities-to-silence-protests-india-tries-to-black-out-democracy/; Reuters. *India widens internet shutdown to parts of Delhi to curb protests*, 2019. https://www.reuters.com/article/us-india-citizenship-mobile-services/india-widens-internet-shutdown-to-parts-of-delhi-to-curb-protests-idUSKBN1YN0MX?il=0
[93] Hindustan Times. *Internet shutdown in many parts including Mangaluru following CAA protests*, 2019. https://www.hindustantimes.com/india-news/internet-shutdown-continues-in-several-parts-including-mangaluru-ghaziabad-following-anti-citizenship-protests/story-hnPSSj9oGh2AtZw8TQoxaM.html
[94] Scroll.in. *Internet shutdowns now reach India's capital - but was the Delhi Police order legal?*, 2019. https://scroll.in/article/947336/internet-shutdowns-now-reach-indias-capital-but-was-the-delhi-police-order-legal
[95] Deccan Herald. *CAA stir: Mobile internet back in Assam after 9 days*, 2019. https://www.deccanherald.com/national/east-and-northeast/caa-stir-mobile-internet-back-in-assam-after-9-days-787128.html; Huffpost. *Internet Shutdown: Why Gauhati HC's Order To Restore Mobile Internet In Assam Is Significant*, 2019. https://www.huffingtonpost.in/entry/internet-shutdown-why-gauhati-hcs-order-to-restore-mobile-internet-in-assam-is-significant_in_5dfbd493e4b01834791dbd47

	on government orders to control protests."[96] It has also been estimated that, from 2012 to 2017, the 16,315 hours of internet shutdown in India cost the country's economy approximately $3.04 billion.[97]
Iraq	**#IraqProtests #INSM_IQ** As mass anti-government protests began in Iraq in 2019, thousands protested rising unemployment, failing public services including long power outages, and government corruption.[98] The security forces responded by killing 100 people and injuring more than 800 protesters, according to international media.[99] The wave of protests broke out in Baghdad's Tahrir Square and spread nationwide, taking place in at least seven other provinces. Within just a few hours of the initial protests, Iraqi authorities blocked Facebook, Twitter, WhatsApp, Instagram, and other social and messaging apps multiple times. As the situation escalated, Iraqi authorities imposed a near-total internet shutdown. They also shut down government offices, introduced a curfew in several cities, deployed thousands of heavily armed security forces, arrested hundreds of people, and engaged in conflict for an extended period of time, reportedly resulting in protester deaths.[100]
Sudan	**#IAmtheSudanRevolution** While states claim that internet shutdowns increase public safety,[101] they in fact enable human rights violations to take place in the dark. In June 2019, the internet was shut down for over a week in Sudan. This was not the first time Sudan had shut down the internet, but this round was different: this time, the shutdown was evidently introduced to deter protesters from livestreaming the reported systematic and organized killings and looting by the Transitional Military Council (TMC). Just before mobile internet was shut

[96] Access Now, *supra* note 92; India Today. *Telecoms burnt in CAA, Article 370 fire; lose Rs 24.5 million per hour of internet shutdown*, 2019. https://www.indiatoday.in/business/story/telecoms-burnt-in-caa-art-370-fire-lose-rs-24-5-million-in-revenue-per-hour-of-internet-shutdown-1632107-2019-12-28
[97] Indian Council for Research on International Economic Relations (ICRIER). *The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India*, 2018. https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout_ppt.pdf
[98] BBC News. *Iraq protests: What's behind the anger?*, 2019. https://www.bbc.com/news/world-middle-east-49960677
[99] CNN. *Death toll rises to 93 in Iraq amid ongoing protests*, 2019. https://edition.cnn.com/2019/10/03/middleeast/iraq-economic-protests-intl/
[100] The Guardian. *Internet blackout in Iraq as death toll from violent protests rises*, 2019. https://www.theguardian.com/world/2019/oct/03/internet-down-across-iraq-third-day-protests
[101] Africa News. *Ethiopia will cut internet as and when, 'it's neither water nor air' - PM Abiy*, 2019. https://www.africanews.com/2019/08/02/ethiopia-will-cut-internet-as-and-when-it-s-neither-water-nor-air-pm-abiy//

	down, the TMC, which had been negotiating with opposition groups to set up a transitional civilian government, withdrew from the negotiations and sent in the Janjaweed militia in a reported murderous attack on peaceful protesters.[102]
Togo	**#TogoDebout, #TogoEnMarche** In September 2017, Togo united in protests to demand reforms from president Faure Gnassingbe, whose regime killed hundreds when he came to power in 2005, following his father's four-decade reign. While Gnassingbe first disrupted the internet during an election in 2015, under his leadership, the Togo government continued to use internet shutdowns in an effort to stop protest organizers from mobilizing marches.[103] On June 25, 2020, the Economic Community of West African States (ECOWAS) Community Court of Justice ruled that the September 2017 internet shutdown ordered by the Togolese government during protests was illegal and an affront to the applicants' right to freedom of expression. The court ordered the government of Togo to pay two million CAF to the plaintiffs as compensation, and to take all the necessary measures to guarantee the implementation of safeguards with respect to the right to freedom of expression of the Togolese people.[104]

[102] The Guardian. *Sudanese doctors say dozens of people raped during sit-in attack*, 2019. https://www.theguardian.com/world/2019/jun/11/sudan-troops-protesters-attack-sit-in-rape-khartoum-doctors-report
[103] Access Now. *Dispatches from an internet shutdown--Togo*, 2017. https://www.accessnow.org/dispatches-internet-shutdown-togo/
[104] Access Now. *ECOWAS Court upholds digital rights, rules 2017 internet shutdowns in Togo illegal,* 2020. https://www.accessnow.org/internet-shutdowns-in-togo-illegal/; *See* also Access Now. *ECOWAS Togo court decision: Internet access is a right that requires protection of the law*, 2020. https://www.accessnow.org/ecowas-togo-court-decision/

IV. SURVEILLANCE AND THE RIGHT TO PRIVACY

Privacy creates a zone of freedom necessary to foster community organizing and enables the exercise of the rights to freedom of peaceful assembly and of association. Importantly, privacy is key to building the trust of vulnerable and marginalized individuals and communities when they come online, particularly to exercise their right to protest. As we have seen in situations around the world, surveillance technologies have the potential to violate privacy and other human rights of millions of individuals and communities. These human rights are more likely to be violated where there are not adequate control mechanisms for the acquisition and use of surveillance technologies and remedies for their abuse.[105]

As noted by the U.N. Special Rapporteur on freedom of expression, David Kaye, "anonymous speech has been necessary for activists and protesters, but States have regularly attempted to ban or intercept anonymous communications in times of protest."[106] From facial recognition technologies (FRT) to the interception of mobile devices, protesters' right to privacy and anonymity is increasingly infringed during protests. For instance, "[FRTs] in public spaces can be abused very easily to violate people's fundamental privacy rights, in ways that are very difficult to remedy."[107] Unlike other sensitive personal information like passwords or security PINs, a person cannot change their face if the data captured is abused or compromised. Without proper safeguards in place, public surveillance tools can be used to track people's movements in a way that inhibits the right to strike in labor contexts, freely associate, express, and enjoy public space in sporting and cultural events, among others.

Protesters have nonetheless inspired creative ways to circumvent FRT. For instance, protesters in Hong Kong have worn face masks, including Guy Fawkes masks, in case photos or FRT are used to identify them.[108] Yet recent trends indicate that it is still relatively easy for digital systems to adapt to most methods individuals use to circumvent surveillance. In fact, with many individuals wearing face masks to prevent the spread of COVID-19, "facial recognition developers are adapting, building datasets of images featuring masked faces to develop and train facial identification and recognition algorithms, and upgrading existing

[105] Access Now. *Argentina province in talks with Huawei over acquiring facial recognition surveillance technology*, 2018. https://www.accessnow.org/mendoza-surveillance-tech/
[106] U.N. Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, U.N. Doc. A/HRC/29/32 (22 May 2015). https://undocs.org/A/HRC/29/32, at para 53.
[107] Access Now, *supra* note 105.
[108] The Guardian. *Hong Kong's digital battle: tech that helped protestors now used against them*, 2019. https://www.theguardian.com/world/2019/jun/14/hong-kongs-digital-battle-technology-that-helped-protesters-now-used-against-them

solutions."[109] Even when face masks are used, digital systems can arguably use other indicators, such as gait, to identify individuals. These protesters are therefore reverting to these creative techniques partially as a result of fears over how authorities are working to identify them through facial recognition and surveillance technologies.[110]

Communications tools are essential to enable the safe and effective exercise of the right to protest. Digital communication services, including new technologies, therefore must remain open and secure for all to exercise their rights to freedom of expression, peaceful assembly and association. The vast amount of personally identifiable information on individuals that is available online may also be used to track and identify individuals and may lead to the automatic sorting out of certain individuals or groups from calls for assemblies, which could have a significant negative impact on the freedom of peaceful assembly and association. Strong end-to-end encryption is therefore essential to defend against unlawful access to data and to protect users, particularly marginalized communities at greater risk of unwarranted surveillance.[111]

Nonetheless, online communications can be easily intercepted by third parties from corporations, states, and non-state actors. Surveillance technologies can be deployed to enable the bulk interception of communications. For instance, international mobile subscriber identity-catchers, also known as "IMSI catchers," "stingrays," or "cell site simulators," are invasive cell phone surveillance devices that "mimic cell phone towers and send out signals to trick cell phones into transmitting their locations and identifying information."[112] Some IMSI catchers are also able to intercept text messages and record cell phone conversations. In the context of assemblies and associations, social media monitoring can be deployed as a form of blanket surveillance — without adhering to the necessity or proportionality principles under international human rights law — to curb dissent, anticipate protests, and justify arbitrary measures such as detentions, fines, etc. States must ensure that

[109] GCN. *Facial recognition adapts to a mask-wearing public*, 2020.
https://gcn.com/articles/2020/06/03/facial-recognition-masks.aspx
[110] BuzzFeed News. *Hong Kong Protesters are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched*, 2019.
https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers; The New York Times. *His Face is Unmistakable. It Is the Face of Protest*, 2019.
https://www.nytimes.com/2019/11/05/opinion/guy-fawkes-day-v-for-vendetta.html
[111] Access Now. *195 companies, organizations, and individuals from 42 countries ask world leaders to support strong encryption*, 2016.
https://www.accessnow.org/195-companies-organizations-and-individuals-from-42-countries-ask-world-leaders-to-support-strong-encryption/; Access Now. *Access Now joins open letter on Facebook's end-to-end encryption plans*, 2019.
https://www.accessnow.org/open-letter-facebooks-end-to-end-encryption-plans/
Access Now. *Lawful Access to Encrypted Data Act would cripple digital security*, 2020.
https://www.accessnow.org/lawful-access-to-encrypted-data-act-would-cripple-digital-security/;
[112] ACLU. *Stingray Tracking Devices.*
https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices;
Access Now. *Brazil's Olympic surveillance legacy*, 2016. https://www.accessnow.org/brazils-olympic-surveillance-legacy/

laws, regulations, activities, and authorities related to communications surveillance adhere to international human rights law and standards. In 2013, following a global multi-stakeholder consultation, a coalition of NGOs, including Access Now, developed the Necessary and Proportionate Principles on the Application of Human Rights to Communications Surveillance.[113] The Necessary and Proportionate Principles serve as a framework for various stakeholders to evaluate whether current or proposed surveillance laws and practices are consistent with human rights. States nonetheless put in place measures to address illegal activities that are often broad and unnecessary and have the effect to disincentivize expression, assembly, and association. Examples of such measures include the proposed creation of wide data-retention mandates for traceability of private massages or the requirement of state-issued IDs to use social media services.[114]

Moreover, third parties can collect and store data on associations and those assembling online and off. Social media platforms may sell or share this information to other third parties, including police authorities. For a recent example, see reporting on artificial intelligence startup company Dataminr, which enjoys real-time access to all tweets on Twitter. This "firehose" of content includes tweets and location data from protest organizers and participants, who use Twitter to coordinate and publicize actions. Recently, Dataminr was found to have sold to U.S. law enforcement agencies access to data regarding Black Lives Matter protests following the police murder of George Floyd, including the location data of peaceful demonstrators.[115] This is not the first instance of police buying privately held data without a warrant, which violates international human rights law and norms.[116]

In addition to malware-based phishing attacks, there are many other examples of attacks designed to hack protesters' — 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.[117] Our Digital Security Helpline has also found instances of doxxing — maliciously

[113] Electronic Frontier Foundation. *Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance*, 2014. https://necessaryandproportionate.org/principles/
[114] Coalizão Diretos na Rede. *Nota da Coalizão Direitos na Rede sobre Aprovação do PL 2630/20 no Senado*, 2020. http://plfakenews.direitosnarede.org.br/nota-da-coalizao-sobre-aprovacao-do-pl-2630-20/
[115] The Intercept. *Police Surveilled George Floyd protests with help from Twitter-affiliated startup Dataminr*, 2020. https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/
[116] *See* The Daily Beast. *AT&T is spying on Americans for profit*, 2017. https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit; and previous revelations of Dataminr collaboration with intelligence activities, at The Wall Street Journal. *Twitter Bars Intelligence Agencies From Using Analytics Service*, 2016. https://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682
[117] Access Now. *New Facebook phishing attack taking Vietnamese opposition voices online*, 2018. https://www.accessnow.org/vietnam-facebook-phishing-attack-take-opposition-voices-offline/

publishing one's personal information, such as a phone number or addresses — to encourage physical harm to protesters and community organizers.[118] Furthermore, according to research conducted by the Citizen Lab, NSO Group's Pegasus spyware has been used in 45 countries, with at least six countries with significant Pegasus operations having been previously linked to the abusive use of spyware to target civil society, human rights defenders, and those engaging in protests.[119]

Digital identity programs also undermine individuals' rights to freedom of peaceful assembly and of association by facilitating state surveillance through the massive collection of personal data, including biometric data. For instance, more than 140 countries worldwide require people to provide personal information as a condition to acquire a SIM card.[120] Through this mandatory SIM card registration, states are able to identify the owner of a SIM card and attribute communications to specific persons. Due to the lack of anonymity, protesters fear that authorities may trace the identity of individuals who use their mobiles to speak up against state practices or engage in or organize protests and demonstrations.[121] In addition to FRTs, mandatory SIM card registration may negatively impact the willingness of protesters to engage in activism, therefore triggering a chilling effect on the exercise of freedom of expression, peaceful assembly, and association, as it facilitates the monitoring of protesters and reprisals against them. Hence, deploying FRT or relying on data collected from digital identity programs must meet an even higher threshold of the necessity and proportionality test.[122]

---

[118] Access Now. *New wave of online attacks in Nicaragua puts opposition voices at risk of physical violence*, 2018. https://www.accessnow.org/new-wave-of-online-attacks-in-nicaragua-puts-opposition-voices-at-risk-of-physical-violence/

[119] The Citizen Lab. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[120] GSMA. *Access to Mobile Services and Proof-of-Identity: Global policy trends, dependencies and risks*, 2018. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf, at page 39.

[121] GSMA. *The Mandatory Registration of Prepaid SIM Card Users - A White Paper*, 2013. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf, at page 13. EFF argues that freedom of association can be burdened by a "chilling effect" when an association engaged in protected expression is forced to disclose the names of its members. Acorn Investments, Inc. v. City of Seattle, 887 F.2d 219, 225 (9th Cir. 1989); and that "[c]onstitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights." Laird v. Tatum, 408 U.S. 1, 11 (1972). The Ninth Circuit has also stated plaintiffs may establish a prima facie case of infringement on First Amendment rights by showing "other factors suggesting a 'chilling' of members' associational rights." Brock v. Local 375, Plumbers Int'l Union of Am., AFL-CIO, 860 F.2d 346, 350 n.1. (9th Cir. 1988). EFF provided specific examples in the brief of the government's mass collection program resulting in a decreased number of calls and associations between the organizations and their constituents as evidence of the chilling effect the government program had on freedom of Association. See *First Unitarian Church v NSA* at https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa.

[122] *See* e.g. Pete Fussey, Daragh Murray. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. 'The Human Rights, Big Data and Technology Project', University of Essex, Human Rights Centre, 2019. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

Amid the COVID-19 pandemic, as cities, regions, and countries reopen, authorities are designing strategies to prevent new waves of contamination. Among these strategies is the processing of health data from individuals to enable the identification of those who may or may not move around and access different spaces, including public ones, through digital health certificates.[123] Digital health certificates consist of the administration and authentication of digital certificates or passes to allow the movement of people according to their health history. Regardless of the motives behind the development of digital health certificates, great concern exists that states may use these certificates to hinder the exercise of individuals' rights.[124] Data associated with digital health certificates may be used as pretext to prevent people from accessing public spaces and thereby exercising the right to freedom of peaceful assembly and of association.

The use of surveillance technologies by police forces raises concerns for protesters. In cases of police brutality and claims of impunity, authorities have used and consider the use of body-worn cameras as a tool to deter police violence, promote accountability, and enhance public trust. However, body-worn cameras may also work as a deterrent against protests and demonstrations, due to the fear of being identified and monitored by police forces.[125]

Community control over police surveillance is growing. The New York City Council recently passed the Public Oversight of Surveillance Technology (POST) Act,[126] legislation that requires the New York City Police Department (NYPD) to disclose the surveillance technologies it procures and uses and the data they collect, and to develop policies around the use and impact of such technologies.[127] It also puts NYPD's use of surveillance technologies under civilian oversight.[128] The POST Act follows a trend of legislative and policy efforts to control law enforcement use of surveillance tech.[129]

---

[123] WHO, *"Immunity passports" in the context of COVID-19,* 2020.
https://www.who.int/publications/i/item/immunity-passports-in-the-context-of-covid-19
[124] EFF. *Immunity Passports Are a Threat to Our Privacy and Information Security*, 2020.
https://www.eff.org/deeplinks/2020/05/immunity-passports-are-threat-our-privacy-and-information-security; ACLU. *Coronavirus 'Immunity Passports' are not the Answer*, 2020.
https://www.aclu.org/news/privacy-technology/coronavirus-immunity-passports-are-not-the-answer/
[125] ACLU. *Body Cameras and the George Floyd Protests*
https://www.aclu.org/news/privacy-technology/body-cameras-and-the-george-floyd-protests/
[126] Venture Beat. *NYC passes POST Act, requiring police department to reveal surveillance technologies*, 2020.
https://venturebeat.com/2020/06/18/new-york-city-council-passes-law-requiring-nypd-to-reveal-its-surveillance-technologies/
[127] New York City Council. *Creating Civilian Oversight of Police Surveillance*, 2020.
https://council.nyc.gov/press/2020/06/16/1984/; New York Times. *Council Forces N.Y.P.D. to Disclose Use of Drones and Other Spy Tech*, 2020. https://www.nytimes.com/2020/06/18/nyregion/nypd-police-surveillance-technology-vote.html
[128] Surveillance Technology Oversight Project (STOP), *Post Act*. https://www.stopspying.org/post-act
[129] *See* ACLU, *Community Control over Police Surveillance*.
https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance

Surveillance and censorship risks are compounded for those who face marginalization through intersecting identities, whether on the grounds of race, ethnicity, sexual orientation, religion, or otherwise. As noted by the Association for Progressive Communications (APC), "surveillance has historically functioned as a tool of patriarchy, used to control and restrict women's bodies, speech, and activism."[130] APC further explains that "participating in queer or feminist activism online [or] navigating social media as a member of a sexual minority, particularly when additionally racialized, can come at great cost, ranging from involuntary 'outing' of one's identity, to harassment, social stigma, violence and persecution."[131] For instance, LGBTQ people are more likely to be attacked using online harassment and violence, victimized through online censorship, intimidated by outing and doxxing, and targeted by law enforcement.[132] As U.N. Special Rapporteur on freedom of expression David Kaye notes, "AI-driven newsfeeds may perpetuate and reinforce discriminatory attitudes, while AI profiling and advertising systems have demonstrably facilitated discrimination along racial, religious and gender lines."[133] For instance, automated gender recognition (AGR) as a part of FRT violates the rights of trans and non-binary people. Specifically, "AGR systems … either fail to classify trans and non-binary people as either male or female (they are thus excluded), or they misgender them by assigning them a gender which does not match what they themselves haven chosen as their gender."[134] These instances of discrimination are particularly concerning if FRT is used for access to buildings or facilities such as bathrooms or changing rooms, as it outs and misgenders individuals by default.

CASE STUDIES

While the internet has created a new space for individuals to mobilize worldwide, the internet is also considered "the greatest spying machine the world has ever seen."[135] Third parties, including states, corporations, and non-state actors, can monitor and collect information on associations and individuals assembling worldwide. Such spying techniques not only undermine individuals' rights to privacy, freedom of expression, peaceful assembly, and association, but also threaten the trust individuals and associations have in using digital

[130] APC. *Feminist Principles of the Internet 2.0*, 2016. https://www.apc.org/en/pubs/feminist-principles-internet-version-20
[131] APC. *Providing a gender lens in the digital age: APC Submission to the Office of the High Commissioner for Human Rights Working Group on Business and Human Rights*, 2018. https://www.ohchr.org/Documents/Issues/Business/Gender/APC.pdf, at page 12.
[132] Access Now, *supra* note 25.
[133] General Assembly, *Promotion and protection of the right to freedom of opinion and expression - Note by the Secretary-General*, U.N. Doc. A/73/348 (29 August 2018). https://undocs.org/pdf?symbol=en/A/73/348, at para 37.
[134] Access Now. *Facial recognition on trial: emotion and gender 'detection' under scrutiny in a court case in Brazil*, 2020. https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brazil/
[135] The Hindu. *World's greatest spying machine*, 2011. https://www.thehindu.com/opinion/editorial/lsquoWorlds-greatest-spying-machine/article14672829.ece

technologies to further enable their human rights. The following domestic case studies highlight a few concerning issues regarding surveillance and the right to privacy.

Azerbaijan

#etiraz

Azerbaijan's government has been systematically suppressing dissent and protest activities through violence, detentions, arrests, and intimidation of civil society.[136] In 2016, after an initial case received by our Digital Security Helpline, Amnesty International, along with other organizations, unveiled a sustained spear-phishing campaign — using a custom malware agent — targeting Azerbaijani human rights defenders, activists, and journalists for over 13 months. The spear-phishing tactics impersonated well-known human rights defenders and comprised their online accounts. Human rights defenders, activists, and journalists in Azerbaijan often face online harassment, such as "abusive comments and threats on social media and website comments, and through a government weaponization of trolling."[137] Research by the Citizen Lab and others indicates that "Azerbaijan has sought to acquire intrusion software from the Italian company Hacking Team."[138]

Brazil

#SemFakeNewsComDireitos

In June 2020, the Federal Senate of Brazil passed a bill that mandates the retention of private-messaging communications data at scale, with the intention of enabling message traceability.[139] This dangerous measure, if finally approved by the house of representatives, would endanger any group of users who communicate to organize peacefully or engage in political participation. Moreover, the first drafts of the bill included a mandatory identification using national ID and cell phone number for all social media users.[140] After a lot of criticism, the actual text limits the identification requirement to accounts subject to complaints by other users, in cases of evidence of a non-authentic account, and upon court order. The problem

[136] Human Rights Watch. *Azerbaijan's Not-So-Subtle Campaign to Stifle Protest*, 2016. https://www.hrw.org/news/2019/10/22/azerbaijan-peaceful-rallies-dispersed-violently; Human Rights Watch. *Azerbaijan: Peaceful Rallies Dispersed Violently*, 2019. https://www.hrw.org/news/2019/10/22/azerbaijan-peaceful-rallies-dispersed-violently.
[137] Medium/Amnesty Global Insights. *False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan*, 2017. https://medium.com/amnesty-insights/false-friends-how-fake-accounts-and-crude-malware-targeted-dissidents-in-azerbaijan-9b6594cafe60
[138] Ibid.; The Citizen Lab. *Mapping Hacking Team's 'Untraceable' Spyware*, 2014. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/
[139] Coalizão Direitos na Rede, *supra* note 114.
[140] Access Now. *Coalition letter: Brazilian disinformation bill threatens freedom of expression and privacy online*, 2020. https://www.accessnow.org/coalition-letter-brazilian-disinformation-bill-threatens-freedom-of-expression-and-privacy-online/

	with this new disposition is that anyone can file a complaint to the platform.[141] This method can be used to silence demonstration leaders, who might want to be anonymous. At the time of publication, the bill awaits its second and final vote in the House of Representatives of Brazil.[142]
France	**#technolopolice** In May 2020, top judges in France banned the use of surveillance drones by police to monitor compliance with COVID-19-related restrictions, citing privacy issues.[143] Civil liberties groups claimed that "people were being filmed without their knowledge, and with no limits on how long footage could be kept."[144] The judges ruled that "drones with cameras can no longer be used until the concerns are addressed, either via a privacy-friendly law or by equipping the drones with technology that makes it impossible to identify the people filmed."[145]
Hong Kong	**#FightForHongKong and #HongKongProtest** On October 4, 2019, amid the ongoing and escalating city-wide protest, Chief Executive of the Hong Kong Special Administrative Region (HKSAR) Carrie Lam invoked a colonial-era ruling, which authorized sweeping powers to quell social unrest, including banning face masks. Hong Kong law enforcement has long had access to FRT and other wide-ranging surveillance tools to identify and track the public. These moves from the authority put the identity and security of Hong Kong citizens under greater risk. In response, protesters in Hong Kong have used creative techniques to limit their exposure to government surveillance and censorship. Accordingly, protesters in Hong Kong have kept "a low profile on social media, communicating only via secure messaging apps, deleting conversations related to the protests and using pre-paid SIM cards not linked to their personal information."[146] They are also "wearing face masks in case photos are used to identify them and declining to give out their

[141] Coalizão Direitos na Rede, *supra* note 114.
[142] See *e.g.* Senado Federal. *Lei Brasileira de Responsabilidade e Transparência na Internet*, 2020. https://legis.senado.leg.br/sdleg-getter/documento?dm=8128670&ts=1594325280670&disposition=inline
[143] Bloomberg. *French Covid-19 Drones Grounded After Privacy Complaint*, 2020. https://www.bloomberg.com/news/articles/2020-05-18/paris-police-drones-banned-from-spying-on-virus-violators
[144] Ibid.
[145] Ibid.
[146] The Guardian, *supra* note 108.

phone numbers or contacts to reporters."[147] These protesters are reverting to these techniques, in part, as a result of fears over how authorities are working to identify them through facial recognition and surveillance technologies.[148] Even though the strong resistance and the later COVID-19 pandemic made the anti-mask law implausible, the Hong Kong government and the central government of China took aggressive moves in 2020 to crack down on protests and the pro-democracy movement. The National Security Law in Hong Kong, in 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.[149]

India

#CAAProtests #SaveOurPrivacy #NCRB

In December 2019, activists in India raised concerns over illegal acts of mass surveillance by Delhi law enforcement authorities during the protests against the Citizenship Amendment Act and proposed National Register of Citizens.[150] Many protesters have reportedly been under mass surveillance through drones and video cameras. The Delhi Police have allegedly purchased facial recognition software from Innefu Labs, a startup funded by IndiaNivesh Venture Capital Fund.[151] The National Crimes Records Bureau and Union Ministry for Home Affairs have been pushing ahead with a national "automated facial recognition system" (AFRS) project despite repeated concerns about its overbreadth and lack of clarity on safeguards and legal oversight.[152] Local lawyers, who express concerns regarding the increased use of surveillance technology by Indian authorities and mandatory data localization, suggest that "the use of facial recognition tech to profile citizens could be illegal, as it does not pass the test laid out by the Supreme Court's privacy judgment."[153] A proposed privacy and data

[147] Ibid.
[148] BuzzFeed News, *supra* note 110.
[149] Access Now. *New police powers in Hong Kong threaten human rights online*, 2020. https://www.accessnow.org/new-police-powers-in-hong-kong-threaten-human-rights-online/
[150] The Economic Times. *Activists rally against 'illegal' surveillance of CAA protests*, 2019. https://m.economictimes.com/news/politics-and-nation/activists-rally-against-illegal-surveillance-of-caa-protests/articleshow/73039535.cms
[151] Ibid.
[152] The Quint. *Govt Planning Facial Recognition System; Raises Privacy Concerns*, 2019. https://www.thequint.com/news/india/ncrb-automated-facial-recognition-system-ministry-of-home-affairs-data-protection-bill-privacy-pending
[153] Ibid.

protection bill is delayed and still pending before a parliamentary committee; the failure of its current text to regulate government surveillance and data collection has led to the bill's original advising author — a retired Supreme Court judge — to criticize it as failing to uphold privacy standards and enabling chilling government surveillance.[154] India's rapidly expanding use of new technologies to surveil protesters, public interest groups, and others has led to concerns that the world's largest democracy is a growing surveillance state.[155]

Russia

#Москва #Протест #Выборы

In July 2019, thousands of people came out in the Russian capital to protest a rejection of the independent candidates to participate in the 2019 Moscow City Duma election. The authorities responded with violence and detained at least 1,373 people.[156] In response, on September 27, 2019, around 20,000 people came out to demand the release of arrested protesters, making it the largest political rally in Russia since the 2011-12 protests.[157] According to the activists, there were CCTV cameras with a facial recognition system installed at the entrance to the protest site. Opposition politician Vladimir Milov and lawyer Alena Popova challenged the use of the cameras against protesters in Moscow court, citing the right to privacy under the Russian constitution and the Personal Data Protection Law, which forbids processing of biometrical data without consent.[158] The court rejected the case, relying on a previous decision that ruled the use of facial recognition cameras during another protest lawful.[159] In July 2020, Popova and Milov took their case to the ECtHR.[160]

[154] The Wire. *Interview | Dilution of Privacy Bill Makes Govt Surveillance a Cakewalk: Justice Srikrishna,* 2019. https://thewire.in/government/interview-justice-srikrishna-privacy
[155] Foreign Affairs. *India's Growing Surveillance State: New Technologies Threaten Freedoms in the World's Largest Democracy*, 2020. https://www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state
[156] Radio Free Europe/Radio Liberty. *Blood, Broken Legs, And Mass Detentions: 2019's Moscow Protests*, 2019. https://www.rferl.org/a/moscow-protests-2019-photos-detentions-blood-broken-legs/30330552.html
[157] BBC News. *Thousands demand protesters freed in Moscow rally*, 2019. https://www.bbc.com/news/world-europe-49871901
[158] Коммерсантъ. *Милов подал иск к московским властям и ГУВД из-за технологии распознавания лиц*, 2020. https://www.kommersant.ru/doc/4227471
[159] Роскомсвобода. *Иск о незаконном использовании технологии распознавания лиц в Москве отклонён судом*, 2020. https://roskomsvoboda.org/55974/
[160] Human Rights Watch. *Moscow's Use of Facial Recognition Technology Challenged*, 2020. https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged

United States	**#BlackLivesMatter and Standing Rock #NoDAPL** 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." Barr warned that alleged violence carried out by Antifa and other movements will be treated as domestic terrorism. On June 19, 2020, U.N. Independent Experts expressed profound concern over such statements, saying they undermine the rights to freedom of expression and of peaceful assembly in the country.[161] From local police to the federal government, the recent round of Black Lives Matter protests exposed the use of surveillance tools to monitor lawful political activity. Examples show the repurposing of tools intended for other ends: the Department of Homeland Security's use of drones, airplanes, and helicopters purchased for its customs and border enforcement to instead monitor Black Lives Matter protests in more than 15 cities;[162] and video footage captured by "smart streetlights" in San Diego, installed to monitor traffic and environmental conditions,[163] to aid law enforcement persecution of protesters.[164] Similarly, when indigenous communities were protesting against installation of the Dakota Access Pipeline (DAPL), which threatened both sacred lands and the water supply to the Standing Rock reservation, they were met with helicopter flyovers and over forms of direct surveillance. When word spread that local police were monitoring the "check in" feature on Facebook to identify individuals participating in the protest, more than a million people around the world "checked in" to express their solidarity and potentially help defend protesters' safety.[165]

[161] OHCHR. *UN experts decry US rhetoric on designation of terrorist groups*, 2020. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25980&LangID=E
[162] The New York Times. *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, 2020. https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html
[163] The City of San Diego. *San Diego to Deploy World's Largest City-Based 'Internet of Things' Platform Using Smart Streetlights*, 2017. https://www.sandiego.gov/mayor/news/releases/san-diego-deploy-world%E2%80%99s-largest-city-based-%E2%80%98internet-things%E2%80%99-platform-using-smart
[164] Mashable. *Police used 'smart streetlights' to surveil protesters, just as privacy groups warned*, 2020. https://mashable.com/article/police-surveil-black-lives-matter-protesters-smart-streetlights/; Access Now. *Standing with #BlackLivesMatter -- for human rights, for justice, and for democracy*, 2020. https://www.accessnow.org/standing-with-black-lives-matter/
[165] The Guardian. *A million people 'check in' at Standing Rock on Facebook to support Dakota pipeline protesters*, 2016. https://www.theguardian.com/us-news/2016/oct/31/north-dakota-access-pipeline-protest-mass-facebook-check-in

V. THE INFLUENCE OF THE PRIVATE SECTOR IN ONLINE CIVIC SPACE

The private sector plays a significant role in respecting and promoting the rights to freedom of peaceful assembly and of association in the digital age. From telcos to online platforms, technology companies control where individuals exercise their rights. Private sector firms build on and benefit from the protocols and infrastructure laid through decades of public sector investment and academic development. But even public services and educational systems have been forced online during the COVID-19 pandemic in an acceleration toward "mass digitalization," often meaning mass privatization. The tech sector welcomes these new user bases, but also frequently inhibits the rights to freedom of peaceful assembly and of association in the interests of profit, monopolistic tendencies, and discriminatory policies — without redress or oversight — among other factors that tend to accompany privatization.

States too willingly hand over the keys to the kingdom through deregulation, corruption, or even good intentions. Human rights experts decry "efforts to 'privatise' control measures by pressuring intermediaries to take action," where states cede traditional public functions to private actors.[166] Additionally, as holders of a wealth of information, technology companies frequently receive informal requests and pressure from states to access user data, remove or restrict user accounts, or undertake a series of actions to serve state interests. Such companies are also confronted with competing domestic and international legal obligations "that threaten their compliance with human rights as well as their ability to operate in certain jurisdictions."[167] This often leads to the infringement of users' rights, including the rights to freedom of peaceful assembly and of association, in order to meet the pressing demands of states.

These corporate practices lacking accountability are compounded by the failure of corporations to disclose adequate information on their human rights impacts. Though, under certain jurisdictions, companies may be legally restricted or prevented from disclosing details about states' requests, in many cases, companies can still provide a basic level of disclosure through "transparency reporting."[168] As the U.N. Special Rapporteur on freedom of peaceful assembly and association Clément Voule notes, "companies around the world often fail to

[166] OAS, IACHR. *Joint Declaration on Freedom of Expression and 'Fake News,' Disinformation and Propaganda*, 2017. http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1056&lID=1
[167] Clément Voule, *supra* note 48, para 58.
[168] Access Now. *Transparency Reporting Index*. https://www.accessnow.org/transparency-reporting-index/

adequately disclose information about data collection and Governments' requests," therefore raising questions regarding corporate transparency and accountability.[169]

THE CAMPAIGN TO #SAVEDOTORG

The lack of corporate transparency and accountability is precisely why hundreds of civil society organizations worldwide came together to save their ".ORG" home from profit-seeking hands. In November 2019, civil society rallied together both online and off — principally in an impromptu town hall meeting at the 2019 Internet Governance Forum[170] — to call on the leaders of the Internet Society (ISOC) and the Internet Corporation for Assigned Names and Numbers (ICANN) to stop the sale of the .ORG top-level domain to private equity firm Ethos Capital. The .ORG domain is the place where civil society and NGOs reside in the digital environment. The .ORG domain is an essential "assembly hall" for civil society and NGOs, as both the physical and virtual world have become increasingly inhospitable and risky for organizations who face constant surveillance, online censorship, and even more physical risks and legal restrictions on their operations and personnel. The proposed sale — which was quashed — presented an additional danger that undermined the safety and stability of digital space for countless NGOs, their partners, and their broader communities.[171] U.N. Special Rapporteurs David Kaye and Clément Voule echoed civil society's concerns regarding the proposed sale of .ORG in a joint letter to ICANN.[172] The U.N. Special Rapporteurs drew attention to the human rights implications of the proposed sale, including how important it is "for civil society organizations to have a place online that is not subject to the pressures of a commercial environment that could very well silence them."[173]

On April 30, 2020, the ICANN Board of Directors responded to the groundswell of opposition by rejecting the change of control of the .ORG domain.[174] While civil society was very pleased that .ORG was not sold to Ethos Capital, concerns remained over "the unilateral decision-making that led to the ISOC Board of Directors deciding in secrecy over a matter of weeks to sell the .ORG domain."[175] In a recent follow-up letter to ISOC and Public Interest Registry leadership, civil society issued a statement reiterating a twofold request to (1)

---

[169] Clément Voule, *supra* note 48, para 58.
[170] Access Now. *Access Now calls on Internet Society to halt the sale of .ORG*, 2019. https://www.accessnow.org/access-now-calls-on-icann-and-internet-society-to-halt-the-sale-of-org/
[171] Access Now. *Letter to ISOC and ICANN*, 2020. https://www.accessnow.org/dot-org-civil-society-letter/; BuzzFeed News. *A Private Equity Firm Is Trying to Buy the .Org Domain. Now, Greenpeace, the ACLU, and Color of Change Are Protesting*, 2020. https://www.buzzfeednews.com/article/alexkantrowitz/a-private-equity-firm-is-trying-to-buy-the-org-domain-now
[172] David Kaye (U.N. Special Rapporteur on freedom of expression), Clément Voule (U.N. Special Rapporteur on freedom of assembly and association). *Letter to ICANN - Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, 2019. https://www.icann.org/en/system/files/correspondence/kaye-voule-to-marby-20dec19-en.pdf
[173] Ibid.
[174] ICANN. *Approved Board Resolutions | Special Meeting of the ICANN Board*, 2020. https://www.icann.org/resources/board-material/resolutions-2020-04-30-en
[175] Save Dot Org. *Letter to the Internet Society and Public Interest Registry leadership*, 2020. https://savedotorg.org/

amend the .ORG registry agreement to include vital protections for human rights and the public interest, and (2) take concrete action to restore trust in .ORG's existing ownership and prevent these kinds of threats from actualizing in the future.[176]

TRANSPARENCY REPORTING

Regularly issuing transparency reports is one of the best ways for companies to communicate to their users and the public about the steps they take to respect human rights. Transparency reports serve three main functions: (1) reviewing company operations that specifically impact privacy or freedom of expression, (2) detailing enforcement of internal rules such as community guidelines and terms of service, and (3) disclosing original stats on state and third-party requests for user data and content and account restrictions.[177] Transparency reports are essential for several reasons. First, they are a powerful mechanism for companies to disclose threats to user privacy and free expression. Second, transparency reports serve as an essential resource to guide investors' decision-making and to support their human rights advocacy. Transparency reports are a crucial indicator in "security and risk analysis for states, companies, organizations, and individuals seeking to adopt or switch tools, services, or platforms."[178] Indeed, as the COVID-19 pandemic pushed operations and the global community online, the U.N. was faced with the need to assess its own private-public partnerships after much criticism around the lack of transparency in the procurement process and the risk certain private sector partners pose to digital rights.[179] This was a huge wake-up call to the U.N., an international organization largely behind in ensuring digitally secure platforms for online operation, but making more strides to address this lag through initiatives such as the U.N. Secretary-General's Data Strategy.[180] As a result of a global crisis during which nearly every aspect of our lives is now conducted online, technology companies have seen a huge growth in their user base.[181] The necessity and rising popularity of online services and platforms gives these companies outsized influence over the way we live our lives. Such influence is more apparent given the pandemic, as assemblies and associations have sought to redefine and repurpose their movements during COVID-19. With this power comes the responsibility to respect human rights.

[176] Ibid. The Public Interest Registry is the organization tasked with management and operation of the .ORG domain and is wholly owned by ISOC.
[177] Access Now. *The what, why, and who of transparency reporting*, 2020. https://www.accessnow.org/the-what-why-and-who-of-transparency-reporting/
[178] Ibid.
[179] Access Now. *U.N. backs down on partnership with Tencent*, 2020. https://www.accessnow.org/un-backs-down-on-partnership-with-tencent/
[180] United Nations. *Secretary-General's Data Strategy*. https://www.un.org/en/content/datastrategy/index.shtml
[181] Access Now, *supra* note 177; Apptopia. *Top iOS Apps: Free app store rank data for iTunes Connect,* 2020. https://apptopia.com/store-insights/top-charts/itunes-connect/top-overall/united-states

REGULATING SPEECH

Under international law, recalling the U.N. Guiding Principles on Business and Human Rights (UNGPs), companies have a specific responsibility to respect all human rights, including the right to non-discrimination.[182] More importantly, these companies may face even stricter international obligations with the U.N.'s proposed legally binding treaty on transnational corporations and mandatory human rights due diligence regimes currently underway.[183] Overall, these policies and practices of technology companies, including their power to decide whose voices are amplified and silenced, have a direct impact on rights to freedom of peaceful assembly and of association. For instance, as feminist organizer Nadine Moawad highlights, "when Google chose a rainbow-colored doodle for the Sochi Olympics, they were expressing a corporate interest in LGBT[Q] rights ... However, unlike a rainbow flag, other forms of sexual speech remain less welcome, such as ... Facebook's ban of women's nipples during the Black Lives Matter nude protest in San Francisco."[184] Social media and other tech platforms must address systemic barriers in order to meaningfully meet the needs and interests of all their users. As technology researcher Maya Indira Ganesh rightfully questions, "how can we rethink the role of these platforms and companies when they take credit for supporting popular uprisings around the world, yet have no accountability to their users in the regulation of speech?"[185]

Social media platforms are commonly referred to as the new "public square," a simplification that belies a more nuanced and changing reality. Back in 2011, during the Arab Spring, this function of social media companies served their public relations and overall image very well. However, many activists now cannot trust these platforms for documenting human rights violations, organizing, and campaigning, as a result of their content moderation policies.[186] Facebook and its family of companies — Instagram, Messenger, and WhatsApp — undeniably

[182] Further noting the 2018 United Nations Human Rights Council Internet Resolution "encourages business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law." *See* U.N. Human Rights Council, *supra* note 43.
[183] Access Now. *Revised draft U.N. treaty on business and human rights: a few steps forward, a few unanswered questions*, 2019. https://www.accessnow.org/revised-draft-u-n-treaty-on-business-and-human-rights-a-few-steps-forward-a-few-unanswered-questions/
[184] Nadine Moawad. *One and the Other: Fighting Online Misogyny, Fighting a Corporatised Internet*, ARROW for Change: Sexuality, Sexual and Reproductive Health and Rights, and the Internet 22, No 1 (2016): 8. https://www.apc.org/sites/default/files/AFC22.1-2016_0.pdf, at page 8.
[185] Maya Indira Ganesh. *The New Green: The Landscapes of Digital Activism*, ARROW for Change: Sexuality, Sexual and Reproductive Health and Rights, and the Internet 22, No 1 (2016): 8. https://www.apc.org/sites/default/files/AFC22.1-2016_0.pdf , at page 4.
[186] See e.g. Pete Fussey, Daragh Murray, *supra* note 122; NBC News. *'Facebook doesn't care': Activists say accounts removed despite Zuckerberg's free-speech stance*, 2020. https://www.nbcnews.com/tech/tech-news/facebook-doesn-t-care-activists-say-accounts-removed-despite-zuckerberg-n1231110

dominate the discourse of groups of all shapes and sizes, from friends and families to corporate, religious, sports, entertainment, and other interest groups. Quantifying its reach depends on data provided by the company; in the past 18 months, Facebook reported housing more than 10 million Groups, "with 1.4B people using them every month," and nearly three billion active users.[187] The firm's centrality to the exercise of peaceful assembly and association must not be ignored.

Despite the company's centralized governance, of which Mark Zuckerberg is the dominant shareholder, board chair, and CEO, Facebook's impact and approach has not been consistent. Facebook has previously responded to the Business & Human Rights Resource Centre regarding the civil society allegations raised about the platform's role in amplifying hate speech and facilitating violence in Sri Lanka.[188] The company reiterated its commitments to tackling these challenges and implementing and improving their policies through engaging with partners. They also released a report on their human rights impact assessments in Sri Lanka, Indonesia, and Cambodia.[189] However, Facebook has made little progress in addressing these same concerns in other parts of the world. In May 2020, U.S. senators wrote to Facebook CEO Mark Zuckerberg, expressing concerns over the company's policy on disinformation, particularly in light of the upcoming U.S. presidential elections.[190] Shareholders have raised similar salient risks with the company, most recently during Facebook's 2020 Annual General Meeting.[191] Increasing the dialogue between social media platforms and civil society groups across regions is an opportunity to better understand and tackle the manifestations of violence in the digital space, but structural change may be necessary to make real progress among the group of Facebook companies toward respecting human rights.

[187] Facebook for Business. *Gen Z: Getting to Know the 'Me Is We' Generation*, 2019. https://www.facebook.com/business/news/insights/generation-z; VentureBeat. *Facebook apps now used monthly by more than 3 billion people*, 2020. https://venturebeat.com/2020/04/29/facebook-earnings-q1-2020/
[188] Business and Human Rights Resource Centre. *Facebook response re allegations regarding Facebook's role in amplifying hate speech and facilitating violence in Sri Lanka, as well as its role generally with exacerbating the spread of false information*, 2018. https://www.business-humanrights.org/sites/default/files/documents/Facebook%20response_19%20Nov%202018.pdf
[189] Facebook. *An Update on Facebook's Human Rights Work in Asia and Around the World*, 2020. https://about.fb.com/news/2020/05/human-rights-work-in-asia/
[190] Bob Menendez Senate. *Menendez, Harris, Blumenthal, Blast Facebook's Continued Failure to Protect Users from Hate Speech and Misinformation*, 2020. https://www.menendez.senate.gov/news-and-events/press/menendez-harris-blumenthal-blast-facebooks-continued-failure-to-protect-users-from-hate-speech-and-misinformation
[191] OpenMIC. *Senators ask Facebook's Zuckerberg to address civil and human rights concerns ahead of 2020 election*, 2020. https://www.openmic.org/news/facebook-civil-rights-letter-from-senators-menendez-harris-blumenthal

CASE STUDIES

Profit motives and the corporate tendencies surrounding privatization have come at a great cost to those exercising their rights to freedom of peaceful assembly and of association. The following domestic case studies highlight some of tech companies' dealings with human rights defenders, activists, labor movements, and general dissent online and off.

Activision Blizzard ***Hong Kong***	In October 2019, the gaming company Activision Blizzard penalized a professional player in Hong Kong for expressing support for the Hong Kong protests during a live online broadcast.[192] Though the company later reduced the penalties, the incident demonstrated the wide variety of online spaces where the right to protest could be at risk.
Whole Foods (Amazon) ***United States***	Internal documents revealed that Amazon-owned supermarket Whole Foods employs interactive heat maps to monitor its stores nationwide.[193] The chain also assigns each store a unionization risk score based on employee demographics and the community's broader socioeconomic wellbeing. These anti-union surveillance efforts could negatively impact Whole Foods' approximately 95,000 employees by allowing their employer to predict what races and classes of workers are more likely to unionize, increasing the likelihood of discrimination in the hiring process as a result.

[192] Access Now. *Blizzard must demonstrate its commitment to respecting the human rights of its users*, 2019. https://www.accessnow.org/blizzard-must-demonstrate-its-commitment-to-respecting-the-human-rights-of-its-users/
[193] Observer. *Whole Foods Secretly Upgrades Tech to Target and Squash Unionizing Efforts*, 2020. https://observer.com/2020/04/amazon-whole-foods-anti-union-technology-heat-map/

Twitter ***Egypt***	In September 2019, demonstrations against Egyptian President Abdel Fattah el-Sisi broke out throughout the country.[194] Egyptians used Twitter, Facebook, and other social media platforms to comment on the protests. The government responded with arrests and blockings of independent media and websites.[195] In addition, Twitter also started suspending accounts that were publicly critical of the government. Over 100 activists had their accounts suspended, including human rights activist Hend Nafea, artist Ganzeer, and journalist Ahmad Hasan al-Sharqawi.[196] Twitter has apologized for temporarily suspending the accounts.[197] Many of the suspended accounts tweeted specific words in Arabic used in a sociopolitical context critical of President Sisi; Twitter's algorithm picked them up as "manipulative."[198] Activists claim that this incident shows that either Twitter does not have enough human moderators overseeing Arabic-language networks or there may have been intentional mass reporting of certain accounts to suppress dissenting voices during the protests.[199]

[194] The New York Times. *Rare Protests Against Egypt's Leader Erupt in Cairo and Elsewhere*, 2019. https://www.nytimes.com/2019/09/20/world/middleeast/anti-government-protests-egypt.html
[195] The New York Times. *In Egypt, Scattered Protests Break Out for Second Week*, 2019. https://www.nytimes.com/2019/09/27/world/middleeast/egypt-protests.html
[196] Middle East Eye. *Egyptian activists sound alarm over Twitter account suspensions*, 2019. https://www.middleeasteye.net/news/egyptian-activists-sound-alarm-over-twitter-account-suspensions
[197] BuzzFeed News. *Twitter "Silenced" Dissenting Voices During Anti-Government Protests In Egypt*, 2019. https://www.buzzfeednews.com/article/meghara/twitter-egypt-protests-accounts-suspended
[198] Middle East Eye, *supra* note 196.
[199] Ibid.

VI. POLICY RECOMMENDATIONS

Now, more than ever, the current global context is calling for all stakeholders to recommit to their pledge to fulfill, protect, respect, and remedy the rights to freedom of peaceful assembly and of association, both online and off. Based on the analysis above, it is evident that these rights, in particular, have not been sufficiently developed to account for the vastly changing digital context. Nonetheless, various international human rights experts, such as several U.N. Special Rapporteurs and those at the OHCHR, are increasingly examining and assessing the intersection of human rights and digital technologies, including the rights to freedom of peaceful assembly and of association.[200] The following recommendations build upon such efforts to further echo the multi-stakeholder call to action to uphold these rights in the digital age.

RECOMMENDATIONS FOR STATES

General

1. Protect and promote the rights to freedom of peaceful assembly and of association, even amid crises.
2. Ensure universal access to ICTs, which are essential to the exercise of the rights to freedom of peaceful assembly and of association in the digital age.
3. Recognize and protect the right to protest as it extends online and into digital spaces, which may be publicly or privately owned and operated.

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 that uses biometric analysis to identify those peacefully participating in an assembly, including, but not limited to, facial, gait, or voice recognition.

[200] See e.g. OHCHR. *New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States*, 2020. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E

2. Dedicate attention to the impact that use of artificial intelligence and machine learning systems in content moderation and content curation can have on the rights to freedom of peaceful assembly and of association, especially in contexts where these freedoms are difficult to exercise offline.
3. Strictly regulate the use of facial recognition technology. In particular, set out clear limitations for its use and require public transparency to protect the effective exercise of the right to freedom of peaceful assembly.
4. Prohibit the use of surveillance technologies, particularly mass surveillance of biometric identifiers, for the indiscriminate and untargeted surveillance of individuals exercising their right of peaceful assembly.
5. 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.
6. Protect the rule of law and ensure that data-sharing agreements between states and companies are based in law.
7. Apply data protection and privacy law and principles, ensuring in particular that law enforcement do not access personal data held by public or private actors without a valid warrant or court order. Comply with the 13 "Necessary and Proportionate" Principles applying human rights law to communications surveillance.
8. Protect and promote privacy-enhancing technologies, and safeguard people's use of encryption, pseudonymity, and anonymity, essential enablers of human rights.
9. Ensure compliance with data protection and privacy rights in the case of abuses from private parties.
10. Conduct timely, accessible, and public mandatory human rights impact assessments and due diligence processes for every public-private partnership and public procurement.
11. Promptly investigate any incidents of police or other forms of brutality or use of excessive force with a view to disseminate the results, including any surveillance footage, and bring those responsible to justice in accordance with international standards.
12. Prevent and prosecute reprisals against those documenting protests, demonstrations, and other assemblies and disseminating such information through digital means.
13. Refrain from integrating digital identity programs, including digital health certificates, in unlawful and repressive surveillance strategies, especially targeting those exercising their rights to freedom of peaceful assembly and of association.

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. Require human rights impact assessments that are (a) conducted regularly, prior to public procurement, during development, at regular milestones, and throughout their context-specific use, (b) include an evaluation of the possible transformations that they may bring upon existing social, institutional, or governance structures, (c) in consultation with

affected communities, and (d) made available to the public in an easily accessible and machine-readable format.
3. Ensure that all human rights defenders and media are able to operate without restrictions, including judicial harassment.

RECOMMENDATIONS FOR THE PRIVATE SECTOR

General

1. Fulfill international obligations to respect the rights to freedoms of peaceful assembly and of association.

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. Apply privacy and data protection laws and principles.
2. 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.
3. Treat all data traffic on an equitable basis no matter its origin, type, destination, or content.
4. Make a public commitment not to reuse or monetize data, and set clear limitations on secondary uses or further processing of data.
5. Condemn the reuse of third-party data without prior authorization.
6. Conduct timely, accessible human rights impact assessments prior to engaging in any public-private partnership and public procurement involving surveillance technologies.

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. Insist that any restrictions on users' rights strictly comply with international human rights laws and standards and the rule of law, and are necessary and proportionate to achieve a clearly defined and legitimate public purpose.
3. Issue transparency reports at least once annually, and ensure that such reports are easily accessible to all users. This includes, at minimum, ensuring that the reports (a) are

consistently easy to find on the company's website, (b) use an intuitive user interface, (c) are formatted to allow users with disabilities to access, and (d) include glossaries or explanations of terms when necessary, in appropriate languages.
4. 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.
5. Sign onto and actively participate in meaningful multi-stakeholder mechanisms, including those offering expert, third-party assessments like the Global Network Initiative and others.
6. 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.
7. 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.
8. Enable independent stakeholders, such as civil society organizations or human rights experts, to regularly check content-moderation and content-distribution systems and to ensure that platforms' policies are in line with international human rights legal standards to mitigate the risk imposed by algorithmic decision making on users' human rights.

RECOMMENDATIONS FOR INTERNATIONAL INSTITUTIONS

General

1. Prioritize and develop, through multi-stakeholder engagement, interpretations on the right to freedom of association in the digital age, such as a General Comment on the Right to Freedom of Association (Article 22) at the U.N. Human Rights Committee.

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.
4. Establish a global fund to increase internet access in LDCs in light of SDG 9.C. This fund should include the full participation of local communities and civil society in technical skill transfer and digital literacy programming, especially with gender focus (building on the Global Connect Initiative and EQUALS projects) to ensure digital inclusion.

Surveillance and the Right to Privacy

1. Prohibit the indiscriminate and untargeted surveillance of individuals exercising their right of freedom of peaceful assembly.
2. Establish a global registry of private sector firms developing and selling targeted surveillance technologies for use by state agencies, in their crises responses, including COVID-19 responses.
3. 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.
4. 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. Investigate the commitments undertaken by states and the private sector under the UNGPs, as well as their application to the development, trade, and use of technology that infringes on human rights, including contact-tracing technologies. Further, consider the introduction of a monitoring body to report back to the U.N. on the status of such.
4. Ensure protection for the public interest, human rights, and civic space in internet governance bodies and forums.
5. 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.

VII. CONCLUSION

The current global context, particularly amid the COVID-19 pandemic, is vastly changing the landscape of assemblies online and off. For instance, individuals used to wear face masks to defy state and corporate power (noting Guy Fawkes masks in particular), and now face coverings are used in assemblies, in part, to comply with state policy and prevent the spread of the COVID-19 virus. In fact, at the time of writing, statistics indicate that there was no evidence of a spike in COVID-19 cases following mass protests in cities across the U.S., including New York City.[201] Moreover, individuals and groups, as evidenced in the youth-led movement on TikTok regarding Trump's rally in Tulsa, are moving quickly to repurpose digital tools to seize the power and utility of such mediums. People are adapting to continue exercising their rights.

At the same time, states and the private sector are quickly deploying tactics to adjust to these new protest norms. For instance, as discussed in this paper, developers are training facial recognition tech to recognize masked faces.[202] Moreover, social media monitoring is being deployed as a form of blanket surveillance — without adhering to the necessity or proportionality principles under international human rights law — to curb dissent, anticipate protests, and justify arbitrary measures such as detentions and fines.

While advocacy at international, regional, and national fora has countered the closing of digital space for communities at risk — most recently, in the U.N. Human Rights Council resolution led by the African Group, judicial decisions against internet shutdowns in Indonesia and ECOWAS, and laws on police use of surveillance tech as enacted by the New York City Council — more must be done to tackle nuanced questions surrounding the rights to freedom of peaceful assembly and of association, and specifically within the digital context.

First, prior to the COVID-19 pandemic, the world was already set to miss the hopeful promise of SDG target 9.C. The economic impact of the COVID-19 pandemic will inevitably exacerbate the economic struggle of individuals — particularly from marginalized communities — and therefore also strain access to the internet. Consequently, all stakeholders must work to address various digital divides, particularly in relation to social, economic, and cultural rights, as well as civil and political rights.

[201] *See* e.g., National Bureau Of Economic Research. *Black Lives Matter Protests, Social Distancing, and Covid-19*, 2020. http://www.nber.org/papers/w27408
[202] GCN, *supra* note 109.

Second, again, prior to the COVID-19 pandemic, states worldwide were already collecting personal data, including biometric data, through the growing use of digital identity programs — in many cases to the detriment of privacy and other fundamental rights.[203] As the COVID-19 pandemic prompts discussions on collection of personal data for health purposes, such as digital health certificates, states and the private sector must affirm their commitment to human rights and ensure that such data is not used as a pretext to prevent critical voices from accessing public spaces and challenging authorities. Multilateral institutions like U.N. treaty bodies, regional bodies like the Association of Southeast Asian Nations (ASEAN) and the Organisation for Economic Cooperation and Development (OECD), and technical standards associations must update their guidance on protecting the rights to protest and assemble online.

Finally, the tech sector must step up to the plate and stop inhibiting the rights to freedom of peaceful assembly and of association in the interests of profit motives, monopolist tendencies, and discriminatory policies. The tech sector must specifically establish effective remedy mechanisms and significant oversight to safeguard these rights.

In conclusion, we call on all stakeholders to monitor, protect, and promote the rights to peaceful assembly and of association, a relatively unheralded and undeveloped set of freedoms that speak urgently to the changing spaces and bodies we inhabit and build in the digital age.

For more information contact:

Laura O'Brien | UN Advocacy Officer, Access Now | laura@accessnow.org

Peter Micek | General Counsel & UN Policy Manager, Access Now | peter@accessnow.org

[203] *See* #WhyID. *An open letter to the leaders of international development banks, the United Nations, international aid organisations, funding agencies, and national governments,* 2019. https://www.accessnow.org/whyid/