A Cross Regional Case Study

Reflections on Successes in Digital Rights & Security

POLLICY

Authors: Mardiya Siba Yahaya, Phillip Ayazika, Meital Kupfer, Jason Muyumba, Favour Borokini, and Soledad Magnone

March 2023

contents

introduction

We are proud to share our new brief on success stories which explores relevant case studies within digital rights and security. We defined successes within this paper as different forms of advocacy, campaigns, programmes, and initiative for policy, anti-surveillance, censorship, safety, and awareness raising initiatives that have been able to achieve their purpose by design or through international solidarity. Success also means that initiatives and interventions whose work has enabled us take one step forward towards creating inclusive, accessible, secure, safe and an open internet. The case studies were also based on stories whose goals were to make digital societies, services and technology more just for minoritized communities. We also chose to use words such as 'minoritized' because to paraphrase D'Ignazio and Klien in Data Feminism, we believe using the word 'minoritized' allows us to acknowledge that marginalization is an active socio-political design through matrices of domination that "positions groups of people in opposition to a more powerful social group."[1]

These cases were also selected from Eastern Europe, Asia-Pacific, Central Asia, Africa, Latin America, and the Middle East and North Africa. We also assessed how the stories aligned with our five thematic areas, and how the processes and tactics of the cases achieve their goals and results. Through our broader research project, we identified what digital rights and security activists, networks and practitioners defined as an 'ideal internet.' While there was no single definition, most people defined it as an accessible, free, safe, secure, operable, inclusive, consented space not managed by a few global North companies. As such, we bring together various case studies and campaigns that contribute to one or more of these factors. In addition, one of the problems that framed our research and is identified through this section is the reactive nature of the digital rights and security ecosystem that does not allow reflection and introspection.

[1] D'ignazio, Catherine, and Lauren F. Klein. Data feminism. MIT press, 2020.

Meanwhile, it is important to note some of the limitations in relation to our definition and criteria for selection. Although a campaign, program, or intervention may be designed to address certain harms of technology and digital societies against minoritized groups, most of them may not have been spearheaded by the groups. However, we make an attempt to represent more stories of successes designed and headed by people who are marginalized by race, location, gender, ethnicity, and sexuality. Similarly, while our ultimate goal is to ensure the liberation of digital societies along the stated margins, some of the case studies only achieve success in pushing for just designs and democratic policy. Thus, why we refer to successes as "a step forward."

In the first white paper, we expanded key terms and definitions used in the internet freedom, digital rights and security space. As the world becomes increasingly automated, the need to take a step back and evaluate the ways in which technology intersects with society in ways that reinforce and perpetuate systems of oppression, exclusion, and discrimination manifests. It is critical to remain cognizant of technology's limitations in addressing deeply rooted and highly complex problems within society. Technology should therefore not be presented as a neutral panacea to problems of crime and safety nor should the inequalities and injustices that predate its adoption be overlooked. Hence, digital rights, safety and security activists, organizations and practitioners continuously work to address some of these issues at the intersection of society and technology while contributing to building our ideal internet , and ultimately an ideal society.

Documenting success stories is also a chance for us as a community to reflect, learn from the practices within the digital rights field, and provide opportunities for collaboration as folks see similarities across regions. The case studies represented within this report may not be exhaustive of all successful work within the digital rights ecosystem. However, through our strides towards a digital society that is privacy-preserving, safe, secure, accessible, does not further exacerbate harm, and allows minoritized communities to use it at its fullest potential, the report with its few examples attempts to put an inclusive internet for all into a closer view. In other words, by documenting the successes and best practices within the digital rights and security field, we are collectively contributing to conceptualizing what a more liberated, equitable and inclusive society is through grassroots advocacy, research and policy reform worldwide. This paper summarizes success stories of and by practitioners working on creating their ideal interpretation of the internet and digital spaces between 2018 and 2022.

Learning from campaigns against surveillance, data protection & facial recognition

Figure 1: Article 19

Biometric facial recognition surveillance in Serbia[2]

In 2021, Serbia's Minister of Interior announced an initiative to install 1,000 cameras with facial and license plate recognition capacity over a period of two years in Belgrade,[3] as part of Serbia's "Safe Society" initiative in collaboration with Chinese telecommunication company, Huawei.[4] The plan was proposed despite biometric mass surveillance being illegal in Serbia, in line with European Union Data protection laws and protocols. However, these plans remain highly contested. The Serbian data protection commissioner rejected the plans of the Ministry of Interior, citing a failure to provide adequate files and evidence for how they will protect the privacy, freedoms and rights of citizens should biometric surveillance systems be implemented.[5]

[2] Perkov, Bojan, "A City with a Thousand Eyes: Mass Surveillance in Belgrade - about:Intel," about intel, January 4, 2021, https://aboutintel.eu/mass-surveillance-serbia/

[3] Share Foundation, "new surveillance cameras in Belgrade: location and human rights impact analysis – "withheld", March 29, 2019 https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location- and-human-rights-impact-analysis-withheld/

[4] Krivokapić, Danilo, Bajić, Mila and Bojan Perkov, "Biometrics in Belgrade: Serbia's Path Shows Broader Dangers of Surveillance State: Heinrich Böll Stiftung: Brussels Office - European Union," Heinrich-Böll-Stiftung, May 19, 2021, https://eu.boell.org/en/2021/05/19/biometrics-belgrade-serbias-path-shows-broader-dangers-surveillance-state.

[5] Ibid

Civil society organizations spearheaded and participated in regional campaigns such as Hiljadekamera and ReclaimYourFace to ensure that the biometric surveillance systems are not implemented. They continue to also engage in policy dialogues and advocacy to address legal loopholes which may allow the Serbian government to deploy the AI cameras. According to the activist community, such AI technologies should not be introduced at all, given the risks they pose to privacy and freedom. Subsequently, activists favor an outright ban on automated video surveillance in public spaces by arguing that mass surveillance goes against the ideals that a just and fair society should endeavor to uphold.[6]

The two largest community-led campaigns, Hiljadekamera and the European Digital Rights (EDRi), advocate against biometric surveillance while promoting the responsible use of AI technologies in Serbia.[7] Their work includes educational resources that teach the public about the risks and harms that may occur when these technologies are deployed. All existing cameras have been mapped, showing that the number of surveillance cameras in the city exceeds official statistics.[8] Hiljadekamera and EDRi also launched a public petition with more than 16,000 signatures requesting the opposition of surveillance systems in Serbia and across Europe. They also engaged in policy advocacy with key European and Serbian data protection authorities.

Civil society pushed back on the deployment of surveillance technologies through advocacy, public petitions and accessible knowledge creation. Public and legal pressure slowed down the expansion process of the surveillance cameras in Serbia. While the need for regulatory and legal frameworks to protect the public from the misuse of AI remains, the work of civil society organizations, communities and individuals secured time to stall, and hopefully in the long run, address this issue.

Actions towards misuse of facial recognition technology on trains in Brazil

In March 2022, civil society groups in Brazil successfully legally challenged the use of facial recognition technology on the metro system, run under the administration of Companhia do Metropolitano de São Paulo.[9] Citing risks to fundamental human rights as

[6] Perkov, 2021.

[7] Krivokapić, Danilo "Biometrics in Belgrade: Serbia's Path Shows Broader Dangers of Surveillance State." Heinrich-Böll-Stiftung, May 19, 2021. https://eu.boell.org/en/2021/05/19/biometrics-belgrade-serbias-path-shows-broader-dangers-surveillance-state

[8] Ibid

[9] Mari, Angelica. 2022. "São Paulo subway ordered to suspend use of facial recognition." ZDNET, March 23, 2022. https://www.zdnet.com/article/sao-paulo-subway-ordered-to-suspend-use-of-facial-recognition/

well as insufficient explanation regarding how it intends to protect user data, Judge Cynthia Thome at the São Paulo State Court ruled for the immediate suspension of the use of the system with a daily fine set in the event of failure to comply.

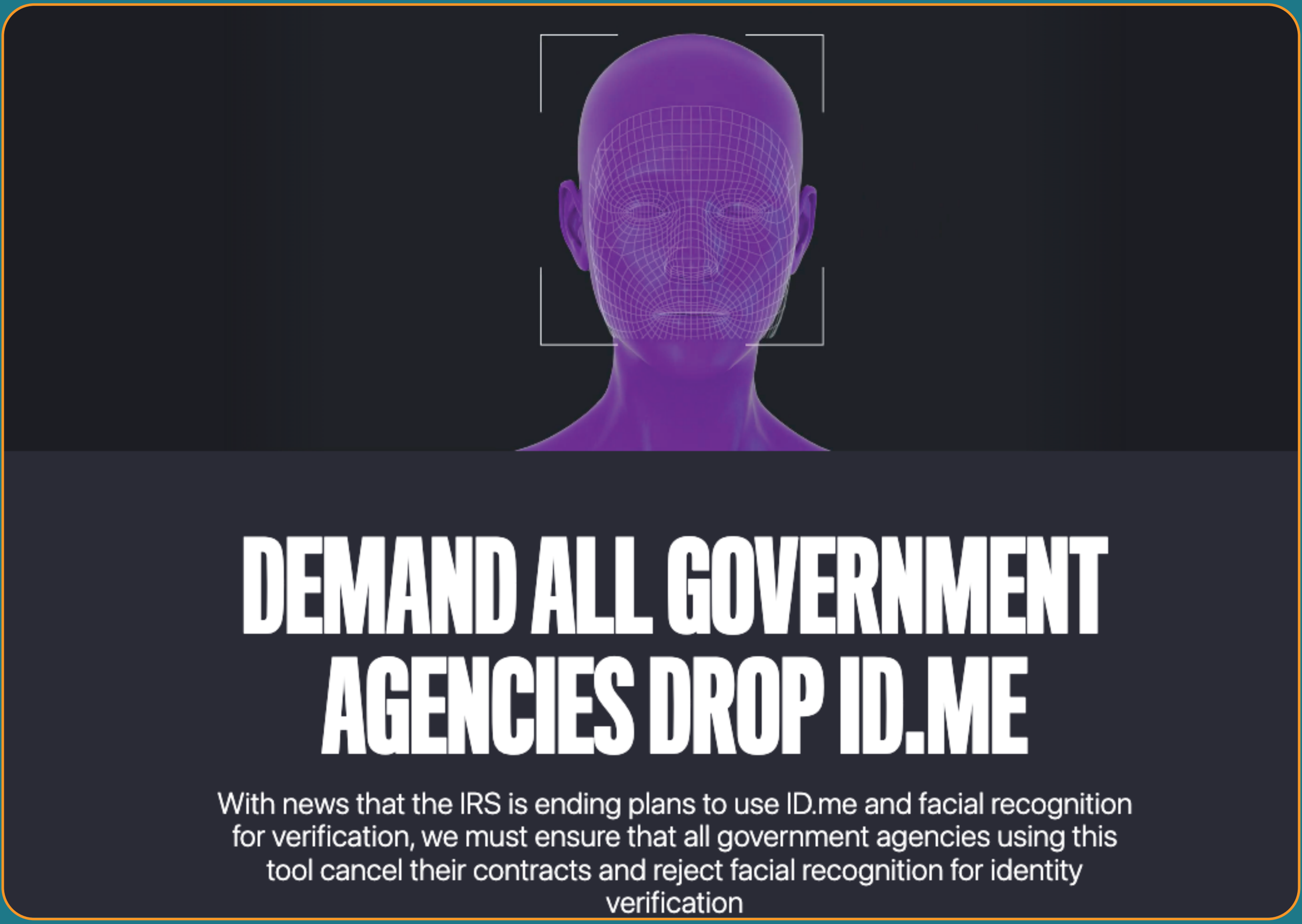
The use of facial recognition technology in surveillance is described as a threat to individual and collective human rights by civil society organizations in Latin America.[10] In Brazil, while public and private users rely on these technologies for "public safety, fraud detection, and tracking school attendance," no evidence exists to back these claims. In fact, using facial recognition on the metro was described by the civil society groups as invasive. The propagation of similar systems throughout the country supposedly normalized the government's unrestricted access to the personal data of citizens in public spaces.[11] Civil society organizations such as Article 19 view this as a failure to recognize that privacy rights exist beyond the confines of the home.

Furthermore, inaccuracies in the use of the facial recognition system results in discrimination against Black and non-binary people, who are uniquely affected by this technology through inaccurate or harmful classification. Furthermore, constant surveillance results in self-censorship, which negatively impacts the individual's ability to participate in demonstrations and protests due to fear of recognition. The success of the action taken against the metro underscores the importance of civil society in the protection of fundamental human rights in digital spaces. It further sets precedence for a people-centered approach that is cognizant of the sanctity of human rights. Similar projects in the future should clearly articulate the impact of surveillance technologies on citizens within a human rights framework.

[10] Access Now, Surveillance Tech in Latin America; Made Abroad, Deployed at Home, (New York: Access Now, 2021), 4 - 5, https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.

[11] ARTICLE 19. 2022. "Brazil: Civil society blocks facial recognition tech on São Paulo Metro." Last modified May 09, 2022. https://www.article19.org/resources/brazil-civil-society-blocks-facial-recognition-tech-on-sao-paulo-metro/.

DUMPID.ME: Campaigns against the US government’s contract with id.me



DEMAND ALL GOVERNMENT AGENCIES DROP ID.ME

With news that the IRS is ending plans to use ID.me and facial recognition for verification, we must ensure that all government agencies using this tool cancel their contracts and reject facial recognition for identity verification

Figure 2: DUMPID.me

DUMP.ID.me is an advocacy campaign led by the Algorithmic Justice League (ALJ) together with Fight for the Future and other organizations against the United States Internal Revenue Services’ (IRS) use of a third-party service called ID.me. The service helped the IRS authenticate taxpayers using facial recognition[12] which required people who created online accounts to take pictures of themselves. The IRS claimed that ID.me was supporting the secure collection and storage of taxpayers’ data, which became the basis for criticism and campaigns.[13]

Through the campaign, Algorithmic Justice League and Fight for the Future detailed significant issues with the IRS’s use of ID.me through reports and urged legislators to “DUMPID.me.” In various op-eds, letters and social media awareness campaigns, they

[12] Rappeport, Alan and Hill, Alan. 2022. “I.R.S. to End Use of Facial Recognition for Identity Verification.” The New York Times, February 7, 2022. https://www.nytimes.com/2022/02/07/us/politics/irs-idme-facial-recognition.html.

[13] IRS, 2021. “IRS unveils new online identity verification process for accessing self-help tools.” Internal Revenue Services, 17 November 2021.
URL: https://www.irs.gov/newsroom/irs-unveils-new-online-identity-verification-process-for-accessing-self-help-tools

highlighted that the IRS's system would have destructive results especially against minoritized communities at the margins of race, gender, class and sexuality. As such, ALJ and Fight for the Future demonstrated how facial recognition technologies such as ID.me's have been used by police to track protesters, make wrongful arrests and administer manipulative marketing.

The organizations who came together to challenge the use of the facial recognition system also created an interactive and informative website that garnered signatures in the form of a public petition. They won. As of February 2022, the IRS committed to move away from third-party services, including ID.me. However, their fight against using facial recognition to authenticate taxpayers' information had only begun. While the IRS is transitioning to a single sign-on government authentication service which does not use facial recognition technology, the agency is still intent on using AI technology to verify the identities of people who create accounts online.[14]

This commitment by the IRS represents a significant win for AJL, Fight for the Future and other AI, digital and data rights organizations, activists, and researchers who were a part of the campaign. First, it demonstrates that meaningful collaboration across different digital rights and security groups and institutions significantly contributes to developing a resilient ecosystem. Similarly, just as activists in Serbia leveraged various tactics such as public campaigns, educational awareness, and petitions, the DUMP.ID.me campaign has also proven that through similar complementary forms of advocacy they were able to steer conversation with the public and legislators. Ultimately showing that we might be able to regulate and stop the questionable use and deployment of certain technologies within the public domain.

[14] Ferris, Gabe. 2022. "IRS rolls out artificial intelligence to help callers make payments, resolve simple tasks." ABC News, 18 June 2022. URL: https://abcnews.go.com/Politics/irs-rolls-artificial-intelligence-callers-make-payments-resolve/story?id=85467107

Gender digital divides, technology-facilitated violence in the Global South

Gender digital divides in adolescent populations in Peru

> ***Español: Estudio exploratorio sobre brechas digitales de género en población adolescente en Perú***

For the last two decades,[15] the United Nations has increasingly referenced the interconnection between digital technologies and a wide array of human rights.[16] In light of the ongoing pandemic, this interconnection particularly with regards to minoritized groups became more evident. Similarly, the gender digital divide has been addressed by different organizations globally. According to a report from the Web Foundation, internet access is skewed in favor of men. Globally, this disparity sits at 21%, rising to 52% in low-income countries.[17] To address this situation, studies and recommendations are becoming more common to focus on the rights of women and LGBTQIA+ individuals in the digital age.

In Latin America, the digital gap reinforces and is fueled by acute social inequalities. Women are less able to afford digital tech and have less free time to use it, due to domestic and care responsibilities. Furthermore, their participation is often disrupted by pervasive online gender-based violence. To shed light on some of these issues in Peru, Hiperderecho and UNICEF conducted a study in 2021[18] to specifically understand the barriers that adolescent women encounter when accessing and using the internet. Hiperderecho is a Peruvian civil society organization dedicated to research and promotion of rights and freedoms in digital environments.

[15] UNDP. Human development Report 2001. (New York: UNDP, 2001), https://hdr.undp.org/content/human-development-report-2001

[16] UN OHCHR. A/74/493: Digital welfare states and human rights - Report of the Special Rapporteur on extreme poverty and human rights. (Geneva: United Nations Human Rights Office of the High Commissioner, 2019), https://www.ohchr.org/en/documents/thematic-reports/a74493-digital-welfare-states-and-human-rights-report-special-rapporteur

[17] World Wide Web Foundation. 2020. "Women's Rights Online: closing the digital gender gap for a more equal world". Last Modified October 12, 2020. https://webfoundation.org/research/womens-rights-online-2020/

[18] UNICEF. Estudio exploratorio sobre brechas digitales de género en población adolescente de Perú. (Peru: UNICEF, 2022), https://www.unicef.org/peru/informes/estudio-exploratorio-sobre-brechas-digitales-de-genero-en-poblacion-adolescente-en-peru

Figure 3: People protest marching in the central Andean city of Ayacucho, Peru, on December 17, 2022. (Source: JAVIER ALDEMAR—AFP/Getty Images)

In Peru only 54.5% of women use the internet, compared to 59.7% of men. This gap increases in the rural sector, where only 18.7% of women use it, compared to 26% of men. Hiperderecho's and UNICEF's study stands out for its special focus on adolescents, in a country where 9 million people are between 12 and 17 years old and from which 92.9 % use the internet. The study which was designed by UNICEF and Global Kids Online was conducted by Hiperderechos using mixed methods. It was composed of interviews with experts and online surveys amongst adolescents. It is a first of its kind in Peru and combines a national outlook analyzing individual, social and gender factors. Initiatives such as this study have a fundamental role in providing inputs for the public and private sectors to develop strategies, projects and laws for children and adolescents to benefit from digital technologies.

Studies on online gender-based violence

Internet connectivity has been lauded for its ability to close the gender gap in Africa.[19] Digital tools help marginalized groups produce and access new knowledge and counter-discourses across gender, race, sex, class, religion, ability, and nationality.[20] However, the internet, once considered a potential utopia for equality, is proving to be an embodiment of the old oppressive and violent systems.[21] If Twitter or the blogosphere resemble a virtual street (and Facebook a private party), then the comparisons to street sexual harassment are appropriate. Thus, ignoring street sexual harassment contributes to the perception that city streets are a masculine space and that women's presence must be aggressively policed. Women continue to face several internet-related risks and difficulties such as image-based sexual assault, nonconsensual photo sharing, online scams, and hacks, prompting many women to self-censor and avoid the internet. Pollicy and various organizations have spent the last few years conducting research to uncover how gendered threats manifest online and how they have evolved over time with the intention to advocate for policies and designs that make the digital space safer for women.

Body and Data’s campaigns against online gender-based violence in Nepal

In 2020, Body and Data identified that the pandemic increased online violence in Nepal. In response, they launched a campaign called “Campaign Against Online Violence” with a series of activities to educate people on technology-facilitated violence. Through their campaign, Body and Data highlighted that access and free expression online relies on people’s safety, security and autonomy. They used creative illustrations, and modes of communication such as informative posters (see Figure 4) to share information on online gender-based violence.

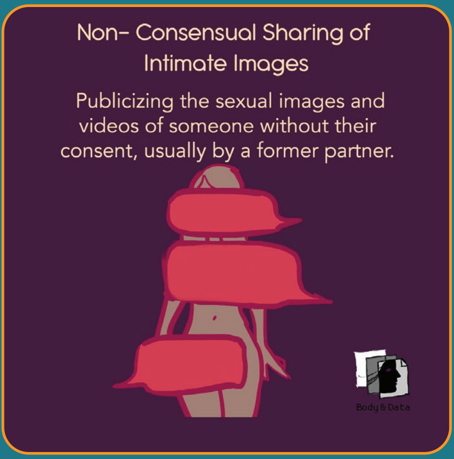

Non- Consensual Sharing of Intimate Images
Publicizing the sexual images and videos of someone without their consent, usually by a former partner.
Body & Data

Figure 4: Body and Data

[19] World Wide Web Foundation (2020). Women’s Rights Online: Closing the digital gender gap for a more equal world. Web Foundation.

[20] Shaw, Adrienne. 2014. “The internet Is Full of Jerks, Because the World Is Full of Jerks: What Feminist Theory Teaches Us About the internet .” Communication and Critical/Cultural Studies 11, no. 3: 273-277. DOI: 10.1080/14791420.2014.926245

[21] Kovacs, Anja, Richa Kaul, and Padte Shobha SV. Don’t Let It Stand!’ an Exploratory Study of Women and Verbal Online Abuse in India (New Delhi: internet Democracy Project, 2013),
https://internet democracy.in/reports/women-and-verbal-online-abuse-in-india.

Body and Data also used an action approach throughout their campaign by sharing prevention resources, reporting mechanisms and a webinar that supported their audience with more context and information on online violence in Nepal, which also included critical assessments of media laws and their limitations.

The action and capacity building approaches used by Body and Data throughout this campaign provided spaces and opportunities for people to safely learn and grow their digital literacy skills. In an ecosystem where people are unaware of media laws and their shortcomings, using creative knowledge creation facilitates access to information for minoritized communities.

Amplified Abuse: mapping violence against women politicians in Uganda

Online violence spikes during political and election seasons, and it is typically directed at women in political discourse, exemplifying violence against women in politics (VAW-P).[22] Gendered mis/disinformation and hate speech are weaponized against women leaders during this period, including In Uganda.[23] Yet, there was a knowledge gap to the extent, context and landscape of violence against women politicians in Africa.

Pollicy conducted research to identify and analyze the scope of online violence directed at women political candidates and high-profile individuals during Uganda's general election in January 2021. The study also sought to discover how this type of online harassment might influence women leaders' use of social media during elections. By monitoring 152 Facebook and Twitter accounts belonging to nominated political candidates and 50 high-profile individuals during the campaign and election period in Uganda, the study found that women candidates were more likely to experience trolling, sexual violence, and body shaming compared to their men counterparts. Yet, men candidates were more likely to experience hate speech and satirical speech as compared to women candidates.

Through this study, Pollicy designed recommendations for political organizations, the Uganda Electoral Commission (EC), parliamentary bodies such as the Uganda Parliamentary Women's Association (UWOPA), women's groups, the media, and civil society to implement. The study also emphasized on the need for safety and security skills development, in addition to structural transformation. Hence, Pollicy's project 'Vote Women' which is a

[22] Inter-Parliamentary Union, 2016. Sexism, harassment and violence against women parliamentarians," Issues Brief, November 2016. URL: https://www.ipu.org/resources/publications/issue-briefs/2016-10/sexism-harassment-and-violence-against-women-parliamentarians

[23] Daily Monitor, 2020. One in three women harassed online - survey. Daily Monitor, 31 August 2020. URL: https://www.monitor.co.ug/uganda/special-reports/one-in-three-women-harrased-online-survey-1922924

hybrid (synchronous and asynchronous) digital skills course was specifically designed to support women leaders with digital literacy skills that centers on safety, and security. What both Body and Data, and Pollicy's tactics to knowledge creation, capacity building and access facilitation teach us is that by using action-oriented approaches to creating more accessible and safer internets for minority groups, we move a step closer to achieving inclusive digital spaces.

African Commission of Human and People's Rights Resolution to protect women from technology-facilitated violence in Africa

For a long time, African feminist technologists contributed significantly to contextualizing the issue of online gender-based violence (OGBV). Their work provided a view into how different communities in Africa uniquely experience OGBV and specified ways to address the issue. The goal was to ensure that OGBV was brought into the limelight of our global and regional internet governance agenda, which eventually led to the African Commission's resolution to protect women online.

On August 2, 2022, the African Commission adopted a resolution to protect women from what they term as 'digital violence,' which falls under standard conceptions of online violence. The resolution draws the correlation between offline and online violence and acknowledges the need to protect rights online as they are protected offline through policy, legislation, increased research and awareness programs for men and boys on the effects of their actions online, to name a few.

For a space that has contested the importance of digital rights and security in relation to other human rights, the African Commission's resolution and acknowledgement represents an important step. In the past, online gender-based violence has been relegated to the sidelines because policy formulation relies on certain forms of evidence and credible acknowledgement from other bodies, a counterintuitive process which requires the problem to get out of hand before it can be resolved. Hence, the Commission's resolution is a collective win for all African feminist technology organizations, activists, individuals, and researchers who committed their time and resources to addressing OGBV. Besides research and theorization of the problem, African feminists also engaged in poli cy advocacy through governance forums. Thus, the Commission's resolution signifies an advocacy-level success.

Digital security helplines

Digital Rights Foundation Pakistan’s cyber harassment helpline and security resource book

Digital Rights Foundation’s (DRF) launched its Cyber Harassment Helpline in 2016 during the foundation's Hamara internet Project. The creation of the Helpline was in response to the continuous and increasing number of queries DRF responded to in relation to online harassment, and digital security measures. The DRF supported many groups , including women and young people with their questions on situations they faced online, which soon became a popular space for social media support. During the same year, Qandeel Baloch was murdered for her online activism. The murder of Qandeel Baloch was important in highlighting the transcendence of online violence to offline and physical harm.

The Helpline was designed to be a “dedicated bridge between the increasing number of online harassment cases, and a digital and legal solution available to the public, especially women.” As the region's first dedicated services to addressing online harassment and gender-based violence; they recorded 4,441 new cases in 2021 alone. The Cyber Harassment Helpline provides specialized needs and services through Helpline associates, digital security experts and a legal team. DRF’s Helpline also provides a series of resources to their callers, some of which are publicly accessible in their Security Resource Book.

The Helpline is especially important for addressing issues and harm at the intersection of gender, religion, and technology. By providing specialized needs and in-person legal services to people in DRF’s location, the helpline demonstrates how digital security and legal support can be embedded in social context. DRF’s work provides an intersectional solution to addressing online violence which we can learn from and collaborate as practitioners, creatives, designers and activists on how to implement a successful intervention that centers on people's social contexts.

Access Now’s Digital Security Helpline

Access Now's Digital Security Helpline is a free resource for civil society around the world that provides real-time, direct technical assistance and advice to civil society groups and activists, media organizations, journalists and bloggers, and human rights defenders. The Helpline, created in 2009, recorded its first case on August 23, 2013. It was officially launched later that year and marked 10,000 cases in 2021.[24] The Helpline makes knowledge open and accessible by documenting and openly publishing all procedures for addressing digital security threats and incidents. This has enabled digital security help desks and rapid responders to find tested workflows tailored to the various languages spoken at the helpline, including English, Spanish, French, German, Portuguese, Russian, Tagalog, Arabic, and Italian.[25]

The 24/7/365 Helpline serves individuals, groups, and organizations from 161 countries and has a global mandate to provide real-time direct technical support to civil society groups, activists, and human rights defenders. Since their inception, the number of requests for assistance has steadily increased, from 152 in 2013 to 2,111 in 2021, representing a 1,288.8% increase in the number of cases.[26] The growing popularity of the Helpline is promising. However, it suggests that threats to members of civil society, activists, human rights defenders and journalists have increased.

[24] Bedoya, Daniel , Michael Carbone, and Sage Cheng. “Strengthening Civil Society’s Defenses: What Access Now’s Digital Security Helpline Has Learned from Its First 10,000 Cases.” Access Now, June 7, 2021. https://www.accessnow.org/helpline-10k-cases-report.

[25] Access Now 2022. “Digital Security Helpline Community Documentation | Access Now Digital Security Helpline Public Documentation.” Accessed September 15, 2022. https://accessnowhelpline.gitlab.io/community-documentation/index.html.

[26] Access Now, 2021. What Access Now’s Digital Security Helpline has learned from its first 10,000 cases. Access Now, 7 June 2021. URL: https://www.accessnow.org/cms/assets/uploads/2021/06/Helpline-10000-cases-report.pdf

To better respond to and combat threats to civil society, the Helpline was a founding initiative of CiviCERT, a network of computer emergency rapid response teams and independent internet content and service providers. The success of the helpline has enabled them to gain and build trusting partnerships such as being a part of FIRST, a leading global incident response initiative, allowing them to provide instant and long-term assistance to at-risk communities.

The Helpline has progressed from an isolated support approach to one that includes a comprehensive assessment of group and organizational security. This assessment is frequently conducted over a longer period of time and with the assistance of partners. They employ more professional security assessment methods, such as the SAFETAG[27] framework in their work, which helps them improve their skills and processes, thus, providing better results to the groups they work with and support.[28] Over the years, the Helpline's work has exposed some of the threats that civil society groups face around the world. Some of the most common threats to civil society that have been documented via the helpline over the years include account takeovers, malware, censorship, denial-of-service attacks on websites, harassment, and communication spying.[29] Altogether, Digital Rights Foundation and Access Now's Helplines, exemplify that through increased capacity and long and short term routes, we are able to build and sustain access to resources and support.

[27] SAFETAG. n.d. "Safetag." Accessed August 30, 2022, https://safetag.org/

[28] Bedoya, Daniel , Michael Carbone, and Sage Cheng. "Strengthening Civil Society's Defenses: What Access Now's Digital Security Helpline Has Learned from Its First 10,000 Cases." Access Now, June 7, 2021. https://www.accessnow.org/helpline-10k-cases-report.

[29] Ibid, 59

Advocacy for freedom of expression, inclusive access to the internet and digital services

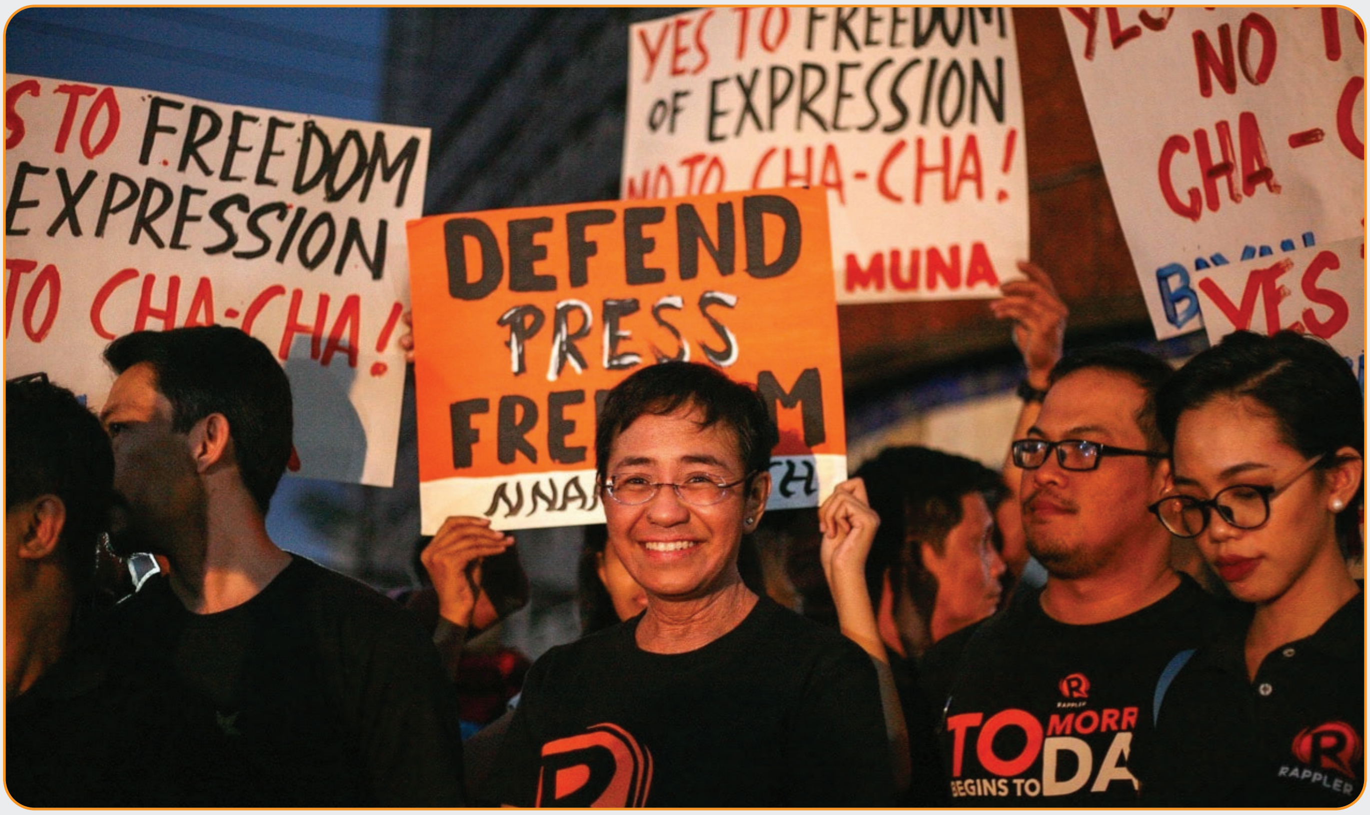


Figure 5: IFEX

Fighting for freedom of expression in the Philippines

In 2020, Maria Ressa and Rappler's former researcher and writer, Reynaldo Santos, were found guilty of cybercrime libel under Philippines' cybercrime act.[30] The verdict was viewed as a direct statement against the journalism community and the state of free expression in the Philippines.[31] To Rappler, this was the government's attempt to restrict critical research and dissenting journalism. Thus, freedom of expression in this sense

[30] "Philippines: Rappler Verdict a Blow to Media Freedom." Human Rights Watch, October 28, 2020, https://www.hrw.org/news/2020/06/15/philippines-rappler-verdict-blow-media-freedom.
[31] "Philippines: SEC Order to Shut down Rappler Violates Freedom of Expression." International Commission of Jurists, July 8, 2022, https://www.icj.org/philippines-sec-order-to-shut-down-rappler-violates-freedom-of-expression/

considers the power relations between the people, journalists, and the government, and who has the power to control what is said or reported.

Maria Ressa was awarded the 2021 Nobel Peace Prize in recognition for her work. Such recognition also served to bring these struggles to light beyond the borders of the Philippines, encouraging others within Southeast Asia and globally.

The case of Rappler's fight for freedom of expression in the Philippines highlights a continuous pushback against repression and a shrinking civic environment.[32] In this case, we argue that success may not be a destination however, a journey to creating a just civic society where people freely access information and are able to express themselves. Rappler has committed its work to shedding light on the state of democracy, press freedom, and targeting of social media in the Philippines despite the hostile environment in which it exists.[33] Rappler is a beacon of hope in the Philippines where a hostile government remains committed to undermining freedom of expression.

To date, media freedom and freedom of expression remains highly contested in the Philippines. This is evidenced by the Philippines Securities and Exchange Commission (SEC) decision in 2018 and 2022 to revoke the publication's certificate of incorporation for a supposed violation of the 'foreign ownership restriction.'[34] However, Rappler's efforts serve to expose attacks on media freedom, free expression within digital media space, human rights and the abuse of power within the Philippines that may otherwise remain concealed while strengthening which deserves acknowledgement, support, and solidarity. The journey to creating free, operable, safe, accessible and secure digital media does not exist without constantly fighting powerful institutions. As with most of the stories highlighted throughout this paper, there were visible, hidden, and invisible powers the organizations and activists had to navigate to achieve their goal.

[32] Gavilan, Jodesz. 2018. "Freedom of Expression Now 'Battlefield' in Fight for Human Rights – Amnesty Int'l." Rappler, February 22, 2018), https://www.rappler.com/nation/196654-freedom-expression-battlefield-fight-human-rights-amnesty-international/

[33] "Philippines: UN Expert Slams Court Decision Upholding Criminal Conviction of Maria Ressa and Shutdown of Media Outlets." OHCHR, July 14, 2022, https://www.ohchr.org/en/press-releases/2022/07/philippines-un-expert-slams-court-decision- upholding-criminal-conviction

[34] Ibid.

Don't tax my megabytes

> ***"We wish to denounce by this petition this decree which is a backpedal in the fight against the digital divide and the promotion of the digital economy (sic)."***

The above quote was taken from an online petition to revoke the tax on Over-The-Top (OTT) services proposed by the government of Benin in July 2018, adding a five percent tax on the pre-tax price for voice, SMS and internet services and a fee per MB for data used to access social media, including video or streaming platforms.[35] According to the establishing decree, internet users were charged an additional 5 West African Francs (FCFAs) per megabyte (an average of $1.50 USD additional cost per gigabyte) in addition to a 5% levy.

The new policy was seen by some as a growing pattern of state-sanctioned efforts to suppress freedom of expression through taxing social media on the continent.[36] This was especially pertinent in the context of increased use of social media in Benin, sitting at 13% of the population as of January 2021.[37] Not only did the proposed tax threaten people's access to a free and open internet by pricing users out, these actions were seen as a deliberate attack on the principle of net neutrality given its target of internet activities deemed 'recreational,' as opposed to 'productive.'[38] More broadly, this proposed tax was forming part of a growing trend across Africa, in which governments were increasingly resorting to the adoption of social media taxes in order to dissuade politicking.[39,40]

As such, in August 2018, the #TaxePasMeMo (#DontTaxMyMegabytes) campaign was launched following the formal introduction of the internet tax at the Benin Investment Forum.[41] Young Beninese were at the forefront of the campaign against the internet tax which had both an online and offline presence. Civil society organizations raised alarm

[35] Over-The-Top (OTT) services are streaming services provided on the internet , different from traditional distribution channels. Examples include: Whatsapp, Twitter, Facebook etc. Referenced from https://www.itu.int/en/ITU-T/Workshops-and-Seminars/bsg/201609/Documents/OTT%20Services%20in%20Korea_BSG_HJP.pd

[36] Ogundeji, Olusegun. 2018. "Benin to tax social media." ItWeb, August 31, 2018. https://itweb.africa/content/JN1gPvOYxbYMjL6m

[37] Ibid.

[38] Bergere, Clovis. 2020. "internet Shutdowns in Africa|"Don't Tax My Megabytes": Digital Infrastructure and the Regulation of Citizenship in Africa." International Journal of Communication 14 (2020): 18.

[39] Boxell, Levi, and Zachary Steinert-Threlkeld. 2022. "Taxing dissent: The impact of a social media tax in Uganda." World Development Vol. 158. 105950.

[40] Fadare, Titilope. 2018. "Group condemns Social Media Tax trend in Africa." Orderpaper, August 30, 2018. https://orderpaper.ng/group-condemns-social-media-tax-trend-in-africa/

[41] Alliance for Affordable internet . 2019. "When The People Talk: Understanding the impact of taxation in the ICT sector in Benin." Last modified March 25, 2019. https://a4ai.org/news/the-impact-of-taxation-on-internet -affordability-the-case-of-benin/

bells signaling concerns over the introduction of the tax in question. Two days later activists created a Change.org petition.[42] The petition gathered over 14,000 signatures in days, becoming part of a fierce and widespread campaign under the #TaxePasMeMo. It included calls to boycott government social media accounts. Following the traction both on the ground and on social media, alongside growing international scrutiny from interest groups, the tax was repealed in September 2018, less than a week after it was instituted.

Thousands of youths across the country weighed in on the decision by voicing their discontentment using the hashtag. Off the back of this widespread support, attempts by activists to stage sit-in protests in the country's capital were thwarted by the mayor who cited a lack of law enforcement capacity as a determinant for the decision.[43] In the face of this pushback, online protests were reinforced, and an online sit-in was staged in which calls were made to boycott government social media accounts and the comment sections of government officials' social media profiles were inundated with commentary on the issue.

While the government never formally acknowledged the extensive backlash as one of the reasons for the repulsion of the tax, the protests were universally regarded as the catalyst.[44] This victory illustrates the ways in which social media can be used as a powerful force particularly in the face of offline censorship. Using social media, the people of Benin were able to bring awareness to their cause and to galvanize international support.
The government's ability to prevent in-person protests was curtailed by the decision to accelerate the movement online.

#DataMustFall

The telecommunications sector in Southern Africa is dominated by a handful of oligopolies.[45] The market also has weak regulatory enforcement, ineffective and outdated legislation. Relative to other emerging markets and African countries, the cost of data in South Africa is high and is considered anti-poor and lacks transparency.[46]

[42] Dahir, Latif Abdi. 2018. “Benin is the latest African nation taxing the internet .” Quartz Africa, September 4, (2018. Modified July 21, 2022. https://qz.com/africa/1377582/benin-is-taxing-use-of-social-media-apps-like-facebook-whatsapp/

[43] “Anger mounts in Benin as new data tax drives up internet costs.” New Vision, September 24, (2018. https://www.newvision.-co.ug/news/1486290/anger-mounts-benin-tax-drives-internet -costs

[44] Ibid.

[45] Sutherland, Ewan. "Data Must Fall the Politics of Mobile Telecommunications Tariffs in South Africa." In South African Association of Political Studies (SAAPS) 15th Biennial Conference, Rhodes University, pp. 26-28. 2021.
https://dx.doi.org/10.2139/ssrn.2154165

[46] Chinembiri, T. (2020). Despite reduction in mobile data tariffs, data is still expensive in South Africa (Policy Brief No. 2). Cape Town: Research ICT Africa. Retrieved from
https://researchictafrica.net/publication/despite-reduction-in-mobile-data-tariffs-data-is-still-expensive-in-south-africa/

In September 2016, a popular local DJ and radio personality used Twitter to call out mobile network operators (MNOs) for their oppressive data charges.[47] In hours, the tweets amassed hundreds of retweets and triggered robust discourse on the digital platform as respondents relayed the effects of high data costs on them. Mainstream media outlets picked up on the conversation with the hashtag #DataMustFall, leading it to trend nationwide. Representatives from two of the country's largest opposition parties echoed the call for operators to reduce costs and pledged support to the movement.[48] As the movement gained traction, young people vocalized their discontent with the high price of data, perceived by many as unaffordable and exclusionary.[49] This was the first time citizens publicly galvanized in large numbers to hold MNOs accountable. As discourse intensified on social media, diverse stakeholders such as political parties, civil society and interest groups weighed in, leading to the issue gaining national prominence. This led the government to force operators to reduce data costs and engaged in processes to address the structural factors inhibiting accessible and affordable data in the country.

In response, the government tasked the relevant parliamentary committee to explore ways to structurally reform the sector to reduce data costs and enable competitiveness within the market. The President also reaffirmed the government's commitment to ensure affordable data in the annual state of the nation address in early 2017.[50] However, MNOs remained steadfast in their justification of data prices in the country and fierce debate marred the interaction between the state, regulator, and MNOs. By July of that year, a regulation review and inquiry had been launched by the regulator and competition commission respectively.[51] Between February and December of 2019 unprecedented gains had been achieved. Following the findings of the regulatory review, operators agreed to scrap the loss of unused data which was flagged as a key issue amongst users.[52] By December 2019, the competition commission had recommended that major

[47] "Datamustfall, warns Tbo Touch." Enca, September 15, 2016. https://www.enca.com/south-africa/datamustfall-demands-cellular-providers-to-lower-their-prices

[48] Smith, Bryan. "The EFF Becomes the First Political Party To Pledge Support For #Datamustfall" Bandwidths (blog) n.b, https://bandwidthblog.co.za/2016/09/16/eff-pledges-support-datamustfall/

[49] Moyo, Dumisani, and Allen Munoriyarwa. 2021 "'Data must fall': mobile data pricing, regulatory paralysis and citizen action in South Africa." Information, Communication & Society 24 (3): 365-380. DOI: 10.1080/1369118X.2020.1864003

[50] Mzekandaba, Simnikiwe. 2017. "Government admits data costs must fall." ItWeb, February 16, 2017. https://www.itweb.co.za/content/2j5alrMQl9O7pYQk

[51] Mothobi, Onkokame, 2018. Competition Commission Data service Market Inquiry, 2018. Research ICT Africa. URL: https://researchictafrica.net/wp/wp-content/uploads/2018/11/Competition-Commission-Data-Service-Market-Inquiry-2018.-.pdf

[52] Alt.Advisory. n.d. "Amendments to the End-User and Subscriber Service Charter." Accessed September 15, 2022. https://altadvisory.africa/2019/02/13/amendments-to-the-end-user-and-subscriber-service-charter/

players –MTN and Vodacom – reduce their data costs by 30 to 50 per cent.[53] This recommendation was instituted by operators in March 2020.

However, the movement was seen as being elitist, with discourse limited to individuals perceived to be of a privileged class background.[54] There was a failure to sustainably address solutions and interventions through a clear plan of action and the roles of the government, the regulator, and MNOs. Instead, stakeholders took actions in silos and the resulting policy changes were characterized as reactionary – particularly from regulators and MNOs. Lastly, the nature of the movement meant that initial efforts were neither sustained nor reinforced towards establishing a network or committing resources to ensure the continued efforts to realize the movement's objectives. The movement signified the need for online movements to set out clear actions and plans for sustainable change beyond the short-lived momentum of hashtags.

[53] "South Africa's Vodacom and MTN told to lower data prices." Reuters, December 2, 2019. https://www.reuters.com/article/safrica-telecoms-idUSL8N28C3JW

[54] Moyo, D., & Munoriyarwa, A. (2021). 'Data must fall': mobile data pricing, regulatory paralysis and citizen action in South Africa. Information, Communication & Society, 24(3), 365-380.

MTN's human rights record

The MTN Group is one of the largest telecommunication providers in Sub-Saharan Africa. In markets in Uganda, South Africa, Ghana and Nigeria, MTN provides cellular services, mobile money, and internet access. MTN is known for allying with authoritarian regimes to censor content, shut down the internet, collect metadata and commit human rights violations.[55] During the 2019 uprising in Sudan, MTN Sudan and other telecommunications companies blocked access to the internet. The shutdown persisted for more than five weeks shortly after the Transitional Military Council (TMC) ordered the Janjaweed militia to attack hundreds of peaceful protesters.[56] Twenty-three civil society groups accused MTN of aiding and abetting this violence in a public letter. Between 2019 and 2020, MTN also complied with other network shutdown orders, including in Benin[57] and Guinea.[58] Shutdowns and censorship not only put freedom of expression and organizing at risk, but also block businesses and individuals from financial activities, particularly mobile money, and e-finance. MTN has also complied with government requests (such as in Nigeria,[59] Ghana,[60] and Uganda[61]) to require ID cards for SIM card registration, often denying people who cannot produce a valid ID card access to basic services.

[55] Sutherland, Ewan. 2015. "MTN: A South African Mobile Telecommunications Group In Africa And Asia". Communicatio 41 (4): 471-505. doi:10.1080/02500167.2015.1100645.

[56] "MTN Contributed To Human Rights Violations In Sudan, Say 23 Civil Society Groups - Business & Human Rights Resource Centre." 2022. Business & Human Rights Resource Centre. https://www.business-humanrights.org/en/latest-news/mtn-contributed-to-human-rights-violations-in-sudan-say-23-civil-society-groups/

[57] Fanou, Roderick, Padmanabhan, Ramakrishna, Filastò, Arturo and Xynou, Maria, 2019. Benin: Social media blocking and internet blackout amid 2019 elections. Open Observatory of Network Interference (OONI). URL: https://ooni.org/post/2019-benin-social-media-blocking/

[58] Netblocks, 2020. internet disrupted in Guinea ahead of presidential election result announcement. Netblocks, 23 October 2020. URL: https://netblocks.org/reports/internet-disrupted-in-guinea-ahead-of-presidential-election-result-announcement-DA3lQ3BW

[59] Kolawole, Oluwanifemi, 2020. Nigerians should prepare for another SIM card registration exercise in 2020, this time with new requirements. Techpoint Africa, 6 February 2020. URL: https://techpoint.africa/2020/02/06/nigeria-sim-registration-2020

[60] Senyo, PK, 2021. Ghana's new mobile money rule could derail financial inclusion. But there are answers. The Conversation, 18 April 2021. URL: https://theconversation.com/ghanas-new-mobile-money-rule-could-derail-financial-inclusion-but-there-are-answers-158770#:~:text=It%20requires%20proof%20of%20identity,Ghana%20card%20(national%20ID

[61] Busuulwa, Bernard, 2019. Uganda SIM card registration woes. The East African, 4 June 2019. URL: https://www.theeastafrican.co.ke/tea/business/uganda-sim-card-registration-woes-1419422

In September 2020, civil society organizations[62] that focus on technology, human rights, and democratic governance submitted an open letter[63] to MTN's newly appointed Chief Executive Officer, Ralph Mupita. The letter accused MTN of failing to disclose instances when its policies affect users' human rights and a lack of commitment to transparency and customer privacy. The open letter urges MTN to take more concrete steps to commit to protecting customers' human and digital rights. This included the recommendation to collaborate with more civil society organizations to advance human rights across the continent. The letter provided the CEO with four key recommendations, including:

- To publish regular transparency reports concerning policies and actions taken in response to external requests, including governments;
- Disclose MTN policies for handling government internet shutdown orders;
- Disclose policies and practices that affect user privacy; and
- Expand partnership with civil society stakeholders.

In response, in 2020, MTN published a bevy of policies and statements outlining its approach to various human rights topics and also released the first transparency report in its company history. The report details legal frameworks that govern its interactions with governments and authorities, particularly those focusing on freedom of expression, data privacy and information security. At the time, MTN was only the second Africa-based company to release such a report. MTN has since released a report for 2021.

Since then, MTN has also released position statements affirming its commitment to human rights and their internal implementation. MTN publicly declared the "rights of all people to communicate, access, and share information freely and responsibly, and to enjoy privacy and security regarding their data and their use of digital communications."[64] In 2022, MTN publicly joined the Global Network Initiative to strengthen and innovate digital human rights efforts.[65] This represented a win as one of the major asks from the civil society organizations that wrote the letter to the CEO back in 2020.

[62] Signed organizations: Access Now, Article 19, African Declaration on internet Rights and Freedoms Coalition, Association for Progressive Communications, Centre for Human Rights in Iran, Centre for Human Rights, University of Pretoria, Collaboration on International ICT Policy for East and Southern Africa (CIPESA), Paradigm Initiative (PIN), The B Team.

[63] Letter to the CEO, MTN Group. September 2020.
URL: https://www.article19.org/wp-content/uploads/2020/09/Open-Letter-MTN-September-2020.pdf

[64] MTN Group Limited. 2022. "Human Rights - MTN Group." Accessed September 15, 2022.
https://group.mtn.com/sustainability/sustainable-societies/human-rights/

[65] MTN Group Limited. 2022. "MTN advances its digital human rights efforts by joining the Global Network Initiative." MTN, 24 May 2022. URL: https://www.mtn.com/mtn-advances-its-digital-human-rights-efforts-by-joining-the-global-network-initiative/

While the new transparency report and other measures (including the Position on Digital Human Rights and Approach to Digital Human Rights) are commendable, there are still ongoing issues across the continent that undercut the promises in previous responses, such as their response to human rights violations in 2017.[66] MTN is similarly bound to two foundational frameworks: the UN Guiding Principles on Business & Human Rights[67] and the OECD Guidelines for Multinational Entities.[68] The question remains whether MTN will continue to aid the suppression of human rights. However, MTN complied with a government request to shut down internet service providers (ISP) to disrupt access during pro-democracy protests in 2021 in eSwatini, continuing this legacy.[69]

MTN should improve transparency on network shutdown requests, disclose more about its due diligence to human rights and enforce its policies on human rights and transparency more closely. Civil society organizations in the technology and governance space have kept their commitments to keep large telecommunication companies such as MTN accountable. Public accountability processes that manifest in the form of calling out companies publicly and loudly often serve to bring national and global attention to otherwise unheard issues.

[66] MTN Group Limited. RE: Letter to MTN Group, dated 12 September 2018. URL: https://media.business-humanrights.org/media/documents/files/MTN_Group_response_AN_RDR_2018.pdf

[67] Addo, Michael K. "The reality of the United Nations guiding principles on business and human rights." Human Rights Law Review 14, no. 1 (2014): 133-147.

[68] Organisation for Economic Cooperation and Development (OECD), OECD Guidelines for Multinational Enterprises, 27 June 2000, available at: https://www.refworld.org/docid/425bd34c4.html

[69] "Eswatini: ICJ Urges Multinational Mobile Telecommunications Company MTN To Immediately Restore internet Access In Eswatini." 2022. International Commission of Jurists, September 15, 2022, https://www.icj.org/eswatini-icj-urges-multinational-mobile-telecommunications-company-mtn-to-immediately-restore-internet -access-in-eswatini/.

conclusion

This paper presents a counter-narrative by collating, recognizing, and reflecting on the often disparate efforts of activists, organizations, and movements to reign in the enthusiasm with which technology is adopted and used. While the fast-changing world of technology tends to leave civil society scrambling to respond to events after they have happened, the passionate individuals and organizations covered in this paper demonstrate a relentless commitment to the fight for a just and fair society and the protection of human rights which must be commended.

While they do not offer conclusive recommendations applicable to every single threat to internet freedom, these cases recognize the value and power that civil society, mass organizing, and advocacy can have for ensuring that stakeholders, including governments and private companies, are able to listen and act towards maintaining and upholding basic human rights in the adoption and use of technology. The internet represents an invaluable resource for civil society and activist organizations to fight to bring an imagined, collective, and ideal future into view.