WHAT IS AN IDEAL INTERNET TO YOU?

A Global Exploration of Digital Rights Trends

Published by

POLLICY

Authors: Mardiya Siba Yahaya, Favour Borokini, Meital Kupfer, Neema Iyer, Phillip Ayazika and Phyllis Njoki Macharia

Date: July 2022

Suggested Citation: Siba Yahaya, M., Borokini, F., Kupfer, M., Iyer, N., Ayazika, P., and Macharia, P.N. (2022). *What is An Ideal Internet? A Global Exploration of Digital Rights Trends*. Pollicy.

Funded Under the Greater Internet Freedom Project

Foreword from the Team

All of us at Pollicy are proud to share our first publication of a body of work under the Greater Internet Freedom (GIF) Project, in collaboration with Internews and funded by USAID. Through this project, Pollicy seeks to explore the issues, challenges and opportunities within internet freedom by collaborating with decision makers, thought leaders and change agents across the globe.

Our goal is to promote critical and thought-provoking conversations and action at the intersection of technology, data and society. We are interested in understanding the current state and capacity of practitioners working on creating their ideal interpretation of the internet and digital spaces. We do so by mapping out organisations, bodies of work, resources, funders and by investigating the long-term and sustainable support needed for actors to further their work, especially in the Global South and among grassroots communities.

This paper, the first in an upcoming series of white papers, was inspired by our work on the first iteration of an annotated bibliography that we categorised by regions of interest and across pre-defined thematic areas within the digital rights and digital ecosystem globally. At Pollicy, we are always questioning how to make our research and tools more accessible, and this white paper is a step towards this goal.

In the paper, we look at topics and issues pertaining to access and inclusion, security, safety and protection, privacy and anonymity in the digital age, freedom of expression, communication and information, and data governance. While the initial work is not exhaustive of each topic and trends within the existing literature on internet freedom, we hope that forthcoming publications under this project will address these gaps adequately. In this regard, Pollicy calls on digital rights and security colleagues, defenders, advocates, and organisations to share their work by contributing to the accompanying literature and organisational mapping documents.

We also welcome your feedback, collaboration and support. Onwards!

Mardiya, Neema, Phillip and the entire Pollicy Team

Table of Contents

Introduction

Digital rights, as a field, is relatively new. The personal computer industry began in the late 1970s, but issues surrounding digital rights largely emerged after the meteoric rise in mobile phone ownership in the 2000s. In the 2010s, the Arab Spring, Occupy Movement and Snowden's whistleblowing highlighted the power of social media mobilisation and has since led to deep discourse about online censorship, privacy and surveillance. Digital rights has come to encompass a wide range of issues concerned with the health of the Internet, one that is constantly changing and moulding to emerging global technological, socio-political and economic trends.

This white paper seeks to provide an overview of the core thematic issues around digital rights and digital safety across the world. The content builds off a global mapping exercise of organisations and knowledge, predominantly focused on Africa and the Middle East, Latin America, Asia-Pacific, Eastern Europe and Central Asia. This document is intended to serve as a primer for practitioners and newcomers into the field of digital rights to gain a broad understanding of key issues within this ecosystem. There may be certain areas of study and practice that have been left unexplored, which may be considered in future iterations.

Digital Security, Safety and Protection

Gender-based violence online

Gendered violence is any form of violence against a person based on or due to their gender, and forms the basis of online violence.[1] Interactions and engagements within digital spaces are not free from gendered social norms that police and control people's lives and bodies. Gender is a site for surveillance and control, and implications of 'control' of non-cis-hetero-masculine bodies happens in the form of violence, where women, queer people, and gender-nonconforming people are harrassed and bullied through hate speech, misinformation, brigading, and many more.

While online violence affects people everywhere, the experiences of people differ based on their race, ethnicity, location, class and caste. Similarly, responses to gendered violence online vary based on people's social statuses and signifiers. For instance, countries in the global North receive significant safety and security support, and policies, whereas those in the global South continue to struggle to address violence at the platform and legislative level. The race and locational disparities in addressing violence does not assume that online violence has been holistically addressed.

Still, how people experience violence is contextual, and researchers identified that certain comments and posts are not considered violating within technology platforms' code of conduct, because these forms of violence are embedded in cultural references that predictive algorithms or the already strained content moderators may not be able to identify.

With that established, this section of the white paper explores the intersection of digital safety and security across issues of cybersecurity, gendered violence, surveillance, data protection and algorithmic harms. The paper also provides a view into the definitions of key issues raised, how they affect different groups of people and how digital right defenders and organisations are addressing these harms and moving for more secure, protected and safe digital futures.

1 Ott, Megan. "Series: What Does That Mean? Gender-Based Violence." Women for Women International. Accessed May 17, 2022. https://www.womenforwomen.org/blogs/series-what-does-mean-gender-based-violence.

What is digital, safety, security and protection in the context of digital rights?

Digital security, safety and protection are practices used to protect individual online identity, data, and other assets. They are often used to protect Human Rights Defenders (HRDs) and activists and are rights-centred. In other words, digital security is a fundamental human right that emphasises the protection and security of all people using technology and digital services.

Feminist technologists and digital rights defenders conceptualise safety and protection as a response to online violence. Violence online includes, misogynistic speech, cyberstalking,[2] misinformation, targeted abuse and threats against digital right defenders, hacking, the non-consensual sharing of intimate images, doxxing, limiting access to digital technologies and other online controlling behaviours. Thus safety, protection and security happens as a direct, indirect, intentional policy, strategy and action that safeguard people from experiencing the harms that are facilitated and amplified by digital services and technologies. Meanwhile, digital technologies here do not only refer to the use of the internet's technology or media, but include analogue technologies such as the television and the radio which also facilitate violence and put vulnerable communities at risk.

2 Perera, Sachini. Review of WHITE PAPER on FEMINIST INTERNET RESEARCH. APC. https://www.apc.org/sites/default/files/firn-whitepaper-2022.pdf

Defining Cybersecurity: A Policy, Context and Technical Perspective

Cyber Security is the virtual protection of organisational property, personnel, information, and economic assets. Meanwhile, **holistic security** considers an intersectional approach to security. It looks at the general response to online violence against vulnerable people and communities, their self-care, gender justice and the practical and legal approaches. As such while cybersecurity may only consider technical measures such as CCTV cameras, and protecting organisations' information systems, holistic security relies on social context, and approaches digital security from a social justice perspective.

In India, CCTV cameras and AI emotion mapping technology are being used to address violence in public spaces.[3] This approach represents the use of cyber security techniques to address gendered social issues. Yet, given that most of these technologies are abstracted from the social context of women, and the continuous imbalance in power within workspaces, women continue to be harrassed and violated. Whats more, such measures have been found to be reactionary and not effective enough to address the structural and hegemonic design of violence against women, queer people and gender-nonconforming people.

In addition to this, researchers continue to explore ways to address cyberattacks including hacking, misinformation, astroturfing, data and surveillance (*dataveillance*), and protecting women online. Through their work, digital rights and feminsit research emphasises on the need for a more structural way to address the harms amplified and facilitated through technology, rather than the multiple highly technical safety tools created that women are unable to make use of because they do not consider the contexts of women.[4] For instance, the move for panic buttons to be embedded in phones in India did not achieve the expected holistic security because its features did not include options for women to contact their close networks and families when in danger. In addition, these panic buttons could be triggered mistakenly, and there were no options to identify an accidental trigger from ones that required protective action.[5]

Meanwhile, when digital security and safety is holistic and nuanced, feminist technologists and researchers have identified that it may be able to address the concerns of vulnerable communities and the risks they face.

3 Nishtha Shanti, "'Smile! UP Police Is Watching': On Distress, Surveillance and Emotion Mapping," Feminism In India, February 10, 2021, https://feminisminindia.com/2021/02/11/up-police-watching-surveillance-emotion-mapping/.
4 Nayantara Ranganathan, "A Handy Guide to Decide How Safe That Safety App Will Really Keep You," genderingsurveillance.internetdemocracy.in, 2017, https://genderingsurveillance.internetdemocracy.in/safety-app/.
5 Karusala, Naveena, and Neha Kumar. "Women's safety in public spaces: Examining the efficacy of panic buttons in New Delhi." In Proceedings of the 2017 CHI conference on human factors in computing systems, pp. 3340-3351. 2017.

The importance of policy as demonstrated through various findings show that laws could impact or benefit women and marginalised communities when they face online violence. Many argue that removing abusers from digital spaces may not be enough but a recognition of online violence through policies and programmes by organisations and governments would promote freedom and expression and opinion which online violence threatens. Notions that the cyber world is 'less real' according to Kryss Network validates the trivialisation of violence, thus deeming it less physical and ignoring the importance of laws to protect women and gender-nonconforming groups online.[6]

On the other hand, the Malawian government[7] uses 'computer-misuse' and digital security and safety laws to target opposition and repress freedom of expression. The weaponization of laws that are supposedly designed to protect people online present another issue that requires better implementation and governing bodies to clearly define and facilitate the internet governance process. An example of such institutions include the Australian e-safety commissioner.[8]

In essence what feminist technologists, researchers and digital rights defenders argue is that cybersecurity should not be considered through a single perspective of the 'technical,' but acknowledging the social aspects of it through programmes, design innovations and policy, would contribute to holistically addressing security issues as a social justice problem. Collectively, approaching digital security and safety as a social justice issue, with transparency from technology companies and states is the first step towards addressing the harms of technology adequately.

6 Kryss Network. "Online Gender-Based Violence: Issues and Policy Implications." Kryss Network. 2022 https://kryssnetworkgroup.files.wordpress.com/2022/02/online-gender-based-violence_-issues-and-policy-implications_policy-brief_eng-version.pdf.

7 Abdulateef Ahmed. "Mainje: Malawian Nurse Arrested by Police for Cyber Harassment." News Central TV | Latest Breaking News across Africa, Daily News in Nigeria, South Africa, Ghana, Kenya and Egypt Today. May 3, 2022. https://newscentral.africa/2022/05/03/malawian-nurse-arrested-by-police-for-disrespecting-president-online/?utm_source=newsletter&utm_medium=email&utm_campaign=a_troubling_whatsapp_update&utm_term=2022-05-07.

8 https://www.esafety.gov.au/

Feminist Approaches and Frameworks to Achieving Digital Safety and Security

Feminist Approaches and Frameworks to Achieving Digital Safety and Security

1. **Pleasure as a resistance strategy:** Digital technologies and services are rarely associated with women's pleasure, especially when women are continuously being eliminated from online spaces. Assessing online spaces and digital services as a source of pleasure for women, and LGBTQ+ persons forces us to reimagine the ideal internet as a space where more vulnerable communities deserve and are equally entitled to happiness and freedom. Centering pleasure also means "rendering languages and cultures of violence and fear as a way to remind women and LGBTQ+ persons they cannot freely engage in public life, as abnormal".[9] Thus, by encouraging non-binary, trans-gender and queer persons to reclaim public spaces and enjoy the benefits of being in public, we engage in a form of resistance.

2. **Digital Safety and Security as Design Justice**: Digital security as design justice recognizes that at the technology platform level, services should be designed or created with the social contexts and levels of vulnerability of people in mind. Feminist researchers recommend that digital innovations should replace "social identity" with "system identity," and there should be more transparency and accountability in these systems.[10]

3. **Education:** Capacity building and education on digital hygiene, security, and the impact of technology on society is also important in teaching people and law makers ways they can address online violence and digital security holistically. For instance, curriculums, toolkits and helpline such as that of *cybersegura,*[11] Electronic Freedom Frontier[12] curriculums, Pollicy's *Digital Safetea*,[13] and Coalition Against Online Violence[14] helpline and toolkits, provide learning materials to help raise awareness, teach people how to protect themselves and provide support where needed.

4. **Legislature to Protect Vulnerable People Online:** While toolkits help people take personal measures to protect themselves, digital rights defenders point out the importance of legislature recognizing online violence, and security not as a weapon against HRDs, but as a nuanced approach to creating policies and programmes to address the issue of violence at all levels.

---

9 Gqola, Pumla Dineo. Female Fear Factory: Gender and Patriarchy under Racial Capitalism. Melinda Ferguson Books, 2021.

10 Peña, Paz, and Joana Varon. "Decolonising AI: A transfeminist approach to data and social justice." Artificial intelligence: Human rights, social justice and development. Global Information Society Watch. Association for Progressive Communications (2019).

11 https://ciberseguras-org.translate.goog/materiales/the-holistic-security-manual/?_x_tr_sl=es&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

12 https://ssd.eff.org/en/module/seven-steps-digital-security

13 https://digitalsafetea.com/

14 https://onlineviolenceresponsehub.org/resources

Protecting Minors

The COVID-19 pandemic accelerated online learning for 1.6 billion learners[15] (including children for whom remote learning was intended for but did not reach) globally, thus increasing children's exposure to the internet.[1617] Online, children are exposed to different forms of predatory behaviour, and social media continuously used to promote child trafficking, and pornography without adequate protection and prevention policies in place[18]. Most research and policy efforts do little to protect children from the harms and risks they may experience while engaging in contemporary digital life. Children have a lower ability to consent or fully grasp the dangers they face, yet remain the most abused, and ignored when it comes to protection, and security policies.

Researchers have also uncovered numerous cases where A.I 'deepnude' bots were used to undress underage girls across the world.[19] Yet, undressing and posting deepfake porn images of girls and young women is one of many instances where minors have been victims of child pornography facilitated by digital services and technologies.

15 The World Bank, "How Countries Are Using Edtech (Including Online Learning, Radio, Television, Texting) to Support Access to Remote Learning during the COVID-19 Pandemic," World Bank, 2020, https://www.worldbank.org/en/topic/edutech/brief/how-countries-are-using-edtech-to-support-remote-learning-during-the-covid-19-pandemic.

16 Unicef, "Children at Increased Risk of Harm Online during Global COVID-19 Pandemic - UNICEF," www.unicef.org, 2020, https://www.unicef.org/southafrica/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic-unicef.

17 Colleen McClain, "How Parents' Views of Their Kids' Screen Time, Social Media Use Changed during COVID-19," Pew Research Centre, 2022, https://www.pewresearch.org/fact-tank/2022/04/28/how-parents-views-of-their-kids-screen-time-social-media-use-changed-during-covid-19/#:~:text=Among%20parents%20with%20a%20young.

18 BBC. "Telegram: Why Won't You Take My Nudes Down?" Www.youtube.com. February 16, 2022. https://www.youtube.com/watch?v=M-arIpw9fVw.

19 Karen Hao, "A Deepfake Bot Is Being Used to 'Undress' Underage Girls," MIT Technology Review, 2020, https://www.technologyreview.com/2020/10/20/1010789/ai-deepfake-bot-undresses-women-and-underage-girls/.

How can we protect minors?

1. Digital training and security for guardians and parents to learn how to protect their children online.

2. Specific research that map out the harms minors face online and practical recommendations on ways technology companies can design products that centre the safety and security of minors.

3. Contextual safety design online that proactively identifies content, and posts that target children and identify when they are being harmed.

4. Digital policies that especially address and govern the use of technology products by children.

5. Policy, and safety designs and guidelines that proactively address and identify potential child trafficking on digital platforms.

Anonymous has a name: Privacy in the digital age

What is privacy, anonymity and identification?

The concept of privacy has drastically evolved as society enters a digitalized age. Information is stored in databases that are vulnerable to breaches, and information is commodified and transferred in faster ways than ever before. The right to privacy is upheld in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), but becomes complicated when intertwined with the realities of privacy in digital communication practice.

Privacy in the digital and technological context relates to users' rights to not have companies or other entities use and collect their individual data.[20] Many of these concepts fall under the individuals' right to determine how their information is collected and used. Individuals should also have the right to share information digitally knowing that the information is secure.[21] This also relates to an individuals' right to exist freely on the Internet with the choice of the information they are exposed to. In varying contexts, this is not always guaranteed or possible.

Anonymity enables individuals or groups to carry out activities in a public space without being identified. In the digital landscape where the lines between reality and fiction are blurred, anonymity means an individual or groups' identity is hidden, or unable to be determined.[22] Anonymity is a key marker of a free society, including a thriving civic space without fear of retaliation or exposure. It plays a key role in the freedom of expression that is defined on the Internet and digital platforms by free, unfettered information that is not censored or restricted.

Similarly, identification in the digital age is a key concept that plays a major role in governance and society. Identification ties information to an individual or group that dictates many aspects of their life.[23] People's senses of identity ties directly into their interactions in the digital space, and the control over public and private is reduced.[24] Identification is also a key facet of accessing goods and services; in an increasingly connected world, some form of digital ID or record is necessary to pay for goods, travel and receive healthcare.

20 TEDx Talks, "Privacy in the Digital Age | Nicholas Martino | TEDxFSCJ," (2016-01-21) URL: https://www.youtube.com/watch?v=PuhifEL5VsU
21 UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32.
22 Evgeni Moyakine. "Online Anonymity in the Modern Digital Age: Quest for a Legal Right." Journal of Information Rights, Policy and Practice 1, no. 1 (2016).
23 Viktor B Naumov. "Information security in identification in the digital age: information law aspect." Gosudarstvo i pravo 9 (2019): 117-130.
24 Bridgette Wessels. "Identification and the practices of identity and privacy in everyday digital communication." New media & society 14, no. 8 (2012): 1251-1268.

Definitions and sub-topics

Surveillance refers to a third party monitoring and logging an individual's online data, stored locally or transmitted over different networks. Governments, companies and other actors conduct surveillance on individuals, groups and other governments. Surveillance is a tool to crack down on dissidents, freedom of speech, material deemed indecent or inappropriate, or to enforce censorship.

The **Right to Anonymity** is the right of an individual to communicate ideas (political, social, etc.) anonymously online without fear of retribution.[25] This is not a universally held ideal; some countries legally require Internet users to register accounts with their real names and ISP address.

The **Right to be Forgotten (RTBF)**, as outlined by the EU Court of Justice in 2014[26] and in the General Data and Protection Regulation (GDPR)[27] gives individuals the right to have their personal data erased under particular circumstances. The RTBF has primarily been enshrined in the European Union, effective under the GDPR, which has a broad reach across the entire region. The RTBF illustrates a renewed examination at the rights which govern our online lives and the endangerment of privacy in the digital age.[28] It has yet to be complemented by more substantial, national legal instruments to protect individuals' right to this action.

The **Right to Identity**, particularly online, focuses on the idea that if people have access to the Internet, they should also have access to an online identity. It also covers the idea that individuals living in a given context also have the right to register and receive services from a government or civil entity. Identity technology emphasises services that are 'digital by default' and require authentication for users to access particular services. This, in turn, necessitates that an individual have a verifiable online "identity." There is an added level of complexity; many argue whether online identity should or should not parallel lived reality. It is more complex than attaching an online avatar or identification to a real person.[29] The information associated with this digital identity is not static and may not be accurate.

25 Martin, Jason A., and Anthony L. Fargo. "Anonymity as a legal right: Where and why it matters." NCJL & Tech. 16 (2014): 311.
26 https://epic.org/privacy/right-to-be-forgotten/
27 https://gdpr.eu/article-17-right-to-be-forgotten/
28 Weber, Rolf H. "The right to be forgotten: More than a Pandora's box." J. Intell. Prop. Info. Tech. & Elec. Com. L. 2 (2011): 120.
29 Bernal, Paul A. "The right to online identity." Available at SSRN 2143138 (2012).

Facial recognition technology (FRT)[30] and **biometric technology** represent an additional layer to the right to identity. FRT uses artificial intelligence to quantify identifiers of individual faces; this information may be used to identify criminals, fraud or enforce protection mechanisms. FRT algorithms depend on accumulating people's faces in databases, which are derived from a variety of sources.[31] FRT is used for mundane tasks, such as unlocking the home screen of your iPhone. Privacy issues emerge when corporations sell this data to governments or foreign bodies without the consent or knowledge of the people whose photos are sold. It often includes identifiable information that may be easily hacked. Similarly, biometric systems measure physiological characteristics such as irises, fingerprints or faces to identify individuals for security or registration reasons. Biometric data has a range of uses: from facility security to coordinating aid delivery for displaced persons.[32] Biometric data can be extracted from vulnerable populations and sold or given to governments without people's consent.

Encryption is when individuals or groups use mechanisms to secure sensitive data from malicious actors. Encryption shields transactions, personal data, photos and sensitive communication from governments and private sector actors. This includes the concept of "crypto," to encrypt information illegible to anyone but intended recipients.[33] A central component is encryption software, which conceals information from any third party trying to access it. Human rights actors recognize encryption and its software as necessary for free and open Internet, and resultantly, civic space.[3435] Encryption maintains individual freedoms of expression, privacy and anonymity in an Internet world that is increasingly public and dangerous.

30 Lewis, James A. and William Crumpler. "Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape." Center for Strategic and International Studies (2021 September). URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY

31 https://theprivacyissue.com/ai-and-biometrics/facial-recognition-privacy-crisis

32 https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid

33 Hellegren, Z. Isadora. "A history of crypto-discourse: Encryption as a site of struggles to define internet freedom." Internet Histories 1, no. 4 (2017): 285-311.

34 Schulz, Wolfgang, and Joris van Hoboken. Human rights and encryption. UNESCO Publishing, 2016.

35 Hildebrandt, Mireille. "Balance or trade-off? Online security technologies and fundamental rights." Philosophy & Technology 26, no. 4 (2013): 357-379.

Contextual implications

Privacy online has varying implications by context. In the global South, emergent civil society, particularly vulnerable groups, are under increasingly high risk of attack due to weak protection mechanisms and privacy measures online. The rapid pace of digitalization means that regulations and legal protections have not caught up to the millions of people already using the Internet in varying contexts. Shortcomings in mechanisms, awareness and public knowledge and skills are a widening gap and must be addressed.[36] Given that cyberspace has no borders, rules, and encourages free flowing information, challenges proliferate in regards to the protection of individuals worldwide. There is a distinct lack of awareness in the global South on these risks in the expanding Internet. Women and human rights defenders face unique threats online that are exacerbated by a lack of protection regarding their privacy. Gender has an important consideration in online privacy research due to the vastly different experiences men, women and non-binary folk have online.[37]

As a result, growing numbers of users in civic and activist groups encourage increased anonymity on the Internet. In Nigeria, users uphold the ideal of anonymity to allow them to express and take action freely online when physical spaces are dangerous.[38] In contrast, there is a growing group of individuals who believe that abolishing anonymity would make the Internet safer. This includes Eugene Kaspersky, of the eponymous antivirus company. He believes that there should be certain parts of the Internet where access is conditional on linkage to your "real-world" identity, removing the liminality between the digital and physical.[39]

Civic space is threatened by who controls the Internet, which can come under fire from government or private entities.[40] In sub-Saharan Africa for example, if civic space that may flourish online in the context of closed spaces in reality, repressive governments take measures to close both digital and real civic spaces, often with impunity. A recent report documents over 100 techniques used by governments on the continent to close online civic spaces.[41] It represents the need to recognize that digital rights are human rights, but online. Movements of repressive regimes towards 'digital authoritarianism' is dangerous for civic space, individual freedom and general well-being.

36 Schia, Niels Nagelhus. "The cyber frontier and digital pitfalls in the Global South." Third World Quarterly 39, no. 5 (2018): 821-837.
37 Frener, Regine, and Sabine Trepte. "Theorizing Gender in Online Privacy Research." Journal of Media Psychology (2022).
38 Agwuegbo, Chioma. "Reclaiming Nigeria's Shrinking Online Civic Space." (2021).
39 Kaspersky, Eugene. "The cybercrime arms race." (2008).
40 Dahlgren, Peter. "The internet as a civic space." In Handbook of digital politics. Edward Elgar Publishing, 2015.
41 Roberts, Tony, Abrar Mohamed Ali, George Karekwaivanane, Natasha Msonza, Sam Phiri, Juliet Nanfuka, Tanja Bosch et al. "Digital rights in closing civic space: Lessons from ten African countries." (2021).

Vulnerable people similarly have their information exposed or put at risk. FRT and biometric technology has been a compelling example of this. For example, companies who owned the identity information of thousands of Rohingya refugees in Bangladesh sold this data to the Burmese government.[42] Biometric data was collected from refugees with the idea of aid delivery efficiency and protection, yet ultimately ended up in the hands of the regime people had fled from.

Finally, privacy studies have been centred on primarily white, Western experiences. The demographics from which most studies are drawn do not reflect the user base of the Internet that is increasingly based in the global South.[43] More privacy studies need to be conducted in relevant contexts. Privacy harms cannot be avoided for vulnerable populations if the study and recognition of said harms do not encapsulate the lived realities of the majority of the world.

42 Holloway, Kerrie, and Oliver Lough. "Although Shocking, the Rohingya Biometrics Scandal Is Not Surprising and Could Have Been Prevented." ODI. Accessed May 17, 2022. https://odi.org/en/insights/although-shocking-the-rohingya-biometrics-scandal-is-not-surprising-and-could-have-been-prevented/.

43 Arora, Payal. "Decolonizing privacy studies." Television & New Media 20, no. 4 (2019): 366-378.

Overall conclusions and thoughts

The Internet and associated digital spaces have become a playing field for information to be exchanged, withheld and exploited at the risk of individual and group safety. As public and private lives become more intertwined with the Internet, privacy and the right to maintain information is paramount. The digital security of individuals is at risk due to increased surveillance by governments and civil bodies, with the right to be truly unidentifiable on the Internet diminishing. Understanding the current state and definitions of these ideas is key towards addressing policy gaps and issues for future work. Particularly in the global South, a series of questions remain:

1. How can digital rights, such as anonymity and privacy, be enshrined and upheld in spaces with weak governance?

2. How can individuals in countries with monitored or restricted Internet have the right to privacy or anonymity?

3. How can displaced persons better access goods and services even if they lack identification digitally?

Freedom of Expression, Communication and Information

Freedom of Expression, Communication and Information

Freedom of expression, communication and information is the right to express oneself and disseminate information, ideas, and opinions in the same way, it is the right to receive and seek information.[44] Furthermore, freedom of expression is a way for people to participate in political processes and strengthen democracy as it enables free exchange of ideas, opinions and information allowing members of society to form opinions around public policy.[45] In this regard, freedom of expression, communication and information is one of the most fundamental political rights.

Censorship

Censorship has various meanings depending on the context it is viewed. Generally, censorship is the suppression of communication that may be valuable or harmful to the censor, the individual or group censored, or the intended recipient of the communication.[46] In the digital rights context, censorship is considered a state-imposed action, focusing on control of the Internet. State-imposed censorship is control imposed by a group of people in power over the general public.[47] Threats or penalties usually accompany state-imposed censorship to instil fear in the subject to not communicate any information against them. This form of censorship forces people to censor themselves due to fear of the recurpassion they may face when they express themselves.

44 Marcelino Bisbal, "FROM FREEDOM of EXPRESSION to the RIGHT to COMMUNICATION: Scope and Boundaries," 2013, https://media.sipiapa.org/adjuntos/186/documentos/001/839/0001839740.pdf.
45 Cube, "Human Rights Guide," Human Rights Guide, April 13, 2022, https://www.cilvektiesibugids.lv/en/themes/freedom-of-expression-media#:~:text=Freedom%20of%20expression%20%26%20Democracy
46 Michael S. Sweeney, Nicholas G. Evans, and Barney Warf, "Censorship - an Overview | ScienceDirect Topics," Sciencedirect.com, 2017, https://www.sciencedirect.com/topics/social-sciences/censorship.
47 Johnston, Donald H., ed. Encyclopaedia of international media and communications. Vol. 3. San Diego, Calif.: Academic Press, 2003.

Internet censorship is the control or suppression of what can be accessed, viewed or published on the internet.[48] It includes control over Internet access, functionality and content. The government is the main controller of the Internet in state-imposed censorship by limiting access to some websites and content. For example, in 2013 China cracked down on the Internet and media; using the Great Firewall they blocked many foreign websites including Twitter, the New York Times, the Guardian and the Wall Street Journal.[49] Despite this, people in China would circumvent the censorship by using virtual private networks (VPNs) to access blocked websites. However, this was short-lived; in 2015, China introduced the Great Cannon, which has the capacity to block traffic as it enters and exits China. It primarily focused on blocking VPNs to limit access to foreign websites by Chinese citizens.[50]

Repressive governments attempt to control the Internet since they perceive it as an emancipatory tool that promotes democracy by giving voices to those with no political power. In doing so, it undermines authoritarian and repressive governments. In return, due to the fear they have of the emancipatory potential of the internet that allows people to circumvent the tightly controlled internet spaces by using tools like VPNs. Repressive governments have developed numerous methods to better control the Internet. These methods include: filtering content based on keywords, redirecting users to proxy servers' websites, blocking a list of internet protocol addresses (IP), tapping and surveillance. At times, governments may proceed to shutting down the Internet completely. In Belarus, after the 2020 election of President Alexander Lukashenko, people protested and accused him online of rigging the election. As a result, the Internet was shut down, leaving protesters and protests in the dark. The Telegram platform that enabled them to circumvent the government become so slow that it crippled the potential of their anti-government actions.[51]

48 Richie Koch, "What Is Internet Censorship, and How Does It Work?," ProtonVPN Blog, March 16, 2022, https://protonvpn.com/blog/how-does-internet-censorship-work/.
49 Yaqiu Wang, "In China, the 'Great Firewall' Is Changing a Generation," POLITICO, September 1, 2020, https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385.
50 Elizabeth C Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown," the Guardian (The Guardian, July 4, 2018), https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.
51 Andrei Makhovsky Balmforth Tom, "Internet Blackout in Belarus Leaves Protesters in the Dark," Reuters, August 11, 2020, https://www.reuters.com/article/us-belarus-election-internet-idUSKCN2571Q4.

At the moment, there are no concrete recommendations to evade internet censorship that limits digital human rights. However, due to the widespread internet usage and rapid technological change it can overwhelm the government's capacity to control the internet, as it is hard for them to keep up with the updated ever changing technologies[52]. Most of the time, the government acquires foreign tools like website denial of Service (DOS) attacks that disrupt the normal functioning of the website by overloading it with external communication requests in order to control the internet.[53]

The government further faces challenges with the outgrowth of the old/ traditional media regulatory regime that governs the newspapers, radio, and television, usually acting as their mouthpiece. This is because many activists and journalists no longer need a media house to spread information. Thanks to the Internet, they only need a smartphone and a good Internet connection to release their news to the public. Internet censorship is a more complex aspect of contested relationships in cyberspace. The Internet is not only a tool used by the government to control, but it is used for numerous positive purposes, such as a platform for human rights groups, ethnic groups, and anti-government groups.

52 Barney Warf, "4 - Southeast Asia," ed. Barney Warf, ScienceDirect (Chandos Publishing, January 1, 2017), https://www.sciencedirect.com/science/article/pii/B9780081008737000040.

53 Danny O'Brien, "The 10 Tools of Online Oppressors," Committee to Protect Journalists, May 2, 2011, https://cpj.org/reports/2011/05/the-10-tools-of-online-oppressors/.

Mis/dis/mal-information

Misinformation is the unintentional spread of wrong information where the spreader believes the information they are spreading to be true.[54] On the other hand, disinformation is the deliberate spread of false information to mislead or promote an agenda.[55] Social and online media have become a major platform where people are circulating fake news. One of the major challenges society faces daily is the rapid spread of propaganda through social media. According to the MOT research report,[56] false news spreads faster than true news, revealing that false information is seventy percent more likely to be retweeted on Twitter while true information takes up to six times longer before it reaches people.

Social media is a great tool for promoting freedom of speech and expression. However, the inability to fact check the information posted on the platforms has catalysed the spread of incorrect information as users who come across it may actively spread it by sharing or engaging with it.[57] In the pursuit of finding solutions to tackle the spread of false information by states and institutions, the right to freedom of expression and communication is at stake. Their efforts face major obstacles as there is a thin line between spreading fake news and freedom of speech.

The use of anti-fake news policies to control the spread of false information have not been fruitful because these policies threaten the right to freedom of expression by criminalising false news. In Malaysia in 2018, an anti-fake news bill was denounced for targeting freedom of expression after the arrest of a Danish citizen that criticised their police on social media. This action could lead to censorship and suppression of freedom of speech and dissenting voices as people in power may target people who are not supporting their agenda.

54 Storyful, "Misinformation vs. Disinformation: What's the Difference?," Storyful, September 24, 2018, https://storyful.com/thought-leadership/misinformation-and-disinformation/.
55 Holly Latham, "Fake News and Its Implications for Human Rights," Human Rights Pulse, December 14, 2020, https://www.humanrightspulse.com/mastercontentblog/fake-news-and-its-implications-for-human-rights.
56 Peter Dizikes, "Study: On Twitter, False News Travels Faster than True Stories," MIT News | Massachusetts Institute of Technology, March 8, 2018, https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.
57 Tom Buchanan, "Why Do People Spread False Information Online? The Effects of Message and Viewer Characteristics on Self-Reported Likelihood of Sharing Social Media Disinformation," ed. Jichang Zhao, PLOS ONE 15, no. 10 (October 7, 2020): e0239666, https://doi.org/10.1371/journal.pone.0239666.

The spread of false information through media platforms also affects other human rights, namely the right to health information, non-discrimination and the right to free and fair election. Health rights are often affected by the spread of fake news, which most of the time contradicts information about health care and disease; approximately forty percent of health news shared online is false, especially with COVID-19 vaccines.[58] People circulated incorrect information during the release of COVID-19 vaccines to discourage people from taking it. Political figures such as former President Trump, Venezuela's president, Nicolas Maduro and Brazil's president Jair Bolsonaro wrongly promoted the use of home remedies, unapproved drugs or bleach as a means to cure coronavirus. Such false information costs people's lives.[59]

The right to free and fair elections is also affected by false information. Before Uganda's January 2021 election, a lot of incorrect information was circulated through a network of inauthentic social media accounts on Facebook, Instagram and Twitter to spread coordinated disinformation. The disinformation was primarily in support of the ruling party and also to defame the opposition party, the National Unity Platform (NUP) party led by Bobi Wine. These accounts claimed there was conflict within the party and they were begging for funds from the ruling party.[6061] Therefore, the spread of disinformation with the intent to defame political personnel that many people tend to believe this information without fact-checking it. Due to this, many people's judgement on which leaders to support becomes impaired. People vote and select poor leaders to run the country, leaving out good leaders who would have performed well.

The right to live without discrimination is at risk due to fake news that targets specific, marginalised groups of people, such as immigrants. The spread of false information dehumanises minority groups. In 2017, Sophie Passman posted a tweet mocking the German far right's fear that immigrants entering the country in recent years would endanger German culture. The Tweet was removed, resulting in Germany expanding their defamation rules on online social media platforms such as Facebook and Twitter due to their failure to delete about seventy percent of online hate speech.[62]

58 Przemyslaw M. Waszak, Wioleta Kasprzycka-Waszak, and Alicja Kubanek, "The Spread of Medical Fake News in Social Media – the Pilot Quantitative Study," Health Policy and Technology 7, no. 2 (June 2018): 115–18, https://doi.org/10.1016/j.hlpt.2018.03.002.

59 BBC, "World Leaders' Posts Deleted over False Virus Info," BBC News, March 31, 2020, sec. Technology, https://www.bbc.com/news/technology-52106321.

60 Stephen Kalema, "We Are Ready for Any Propaganda War! Bobi Wine's Brother Nyanzi Speaks out on Allegations That He Begs Money from NUP MPs," Watchdog Uganda, January 23, 2022, https://www.watchdoguganda.com/news/20220123/128778/we-are-ready-for-any-propaganda-war-bobi-wines-brother-nyanzi-speaks-out-on-allegations-that-he-begs-money-from-nup-mps.html.

61 AFSS, "Domestic Disinformation on the Rise in Africa – Africa Center," Africa Center for Strategic Studies, October 6, 2021, https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/.

62 Mark Scott and Janosch Delcker, "Free Speech vs. Censorship in Germany," POLITICO (POLITICO, January 4, 2018), https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech/.

There is a thin line between the spread of false information and freedom of expression. Therefore, organisations and states need to curb the spread of incorrect information in a manner that does not suppress the right to freedom of expression:[63]

1. **Government**: promote news literacy to create awareness on fake news among people

2. **Media industry**: provide high quality journalism and correct fake news and disinformation without legitimising them.

3. **Technology industry and social media platforms**: should invest in tools that can identify fake news such as fact checking tools and reduce financial incentives to content creators that distribute false information in order to improve online accountability.

4. **Educational institution:**should prioritise informing people about news literacy through introduction of short courses at school.

5. **Digital consumers**: should cross check news sources to be sure of correct information before they consume or share with others.

63 Darrell M. West, "Redirect Notice," www.google.com, December 18, 2017, https://www.google.com/amp/s/www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/%3famp.

Digital activism and advocacy

Digital activism and advocacy is an Internet-based communication Technique on social networks that create or manage any form of activism to bring about social and political change.[64] Internet-based activism has proven to overcome challenges by giving people a platform to be involved in public affairs unlike in the past where power, wealth and geographical limitations confined an individual's access to participate in social and political affairs.

The Internet's features such as first real time exchange of information, cascading or virally spreading[65] has enabled social media users to share thoughts with speed and accessibility on different online platforms. Online platform has become a space for democracy and human rights activists to mobilise people through conducting campaigns calling on people to sign petitions and hashtags to influence political, social, and economic reform. Digital activism has become a great means of grassroots political mobilisation and a new way for protestors to demonstrate peacefully and voice their problems.[66]

Digital advocacy has offered a platform to marginalised groups to practise the freedom of expression and advocate for their rights because of digital activism's potential to create awareness on issues. One of the most common digital activism strategies used is hashtags in the activism online campaign. The hashtags have a strong influence and create a buzz in the mainstream media coverage bringing up an opportunity to change the narrative and see things from a different perspective. For instance, the hashtag #MeToo that advocates for survivors of sexual harrassment or assaulted to share their stories. The hastag started as a phrase Tarana Burke the founder of MeToo movement made to promote sisterhood of survivors of sexual abuse that went viral on social media hashtag. This resulted in #MeToo transitioning rapidly into a global movement that saw the male perpetrators facing justice, such as Hollywood producer Harvey Weinstein.[67]

64 Marcela A. Fuentes, "Digital Activism," Encyclopedia Britannica, 2021, https://www.britannica.com/topic/digital-activism.
65 Boyang Zhang and Marita Vos, "(PDF) How and Why Some Issues Spread Fast in Social Media," ResearchGate, February 2015, https://www.researchgate.net/publication/275041532_How_and_Why_Some_Issues_Spread_Fast_in_Social_Media.
66 Marc Lynch, "Mobilizing through Online Media," The Century Foundation, May 9, 2017, https://tcf.org/content/report/mobilizing-online-media/?session=1.
67 Anjani Datla, "Redirect Notice," www.google.com, November 16, 2020, https://www.google.com/url?q=https://case.hks.harvard.edu/leading-with-empathy-tarana-burke-and-the-making-of-the-me-too-movement/&sa=D&source=docs&ust=1652897353206861&usg=AOvVaw0KFj--sWG_0ibxS85YVlaa.

Content Moderation

Content moderation is the process of screening and monitoring user-generated content online to provide a safe environment for both users and brands.[68] Online hosts of user-generated content make decisions daily on what content or account to allow or block. The content moderation mechanism's main purpose is to regulate contents that seem to harm society. Such content could be misinformation or Disinformation on COVID-19 or elections, harassment and abuse. Content moderation is critical to online freedom of expression because it determines what users can say and what information they receive.

AI-based content moderation may negatively impact the right to freedom of expression, security and protection from online violence. In cases when algorithms may fail to detect dis/misinformation, users may use it to incite violence.[69] Such was the case for Mynmar genocide that was as a result of hate speech on facebook against Rohingya muslim in Mynmar causing murders and rapes by Mynmar security forces making more than 650,000 Rohingya Muslims flee Mynmar to Bangladesh for their safety.[70] Online hosts should make moderation decisions that respect human rights by ensuring content moderation practices respect for thoughts and frank exchange of views.

68 Marcela A. Fuentes, "Digital Activism," Encyclopedia Britannica, 2021, https://www.britannica.com/topic/digital-activism.

69 Sebnem Kenis, "Human Rights and AI-Powered Content Moderation and Curation in Social Media," The Raoul Wallenberg Institute of Human Rights and Humanitarian Law, August 19, 2021, https://rwi.lu.se/blog/sebnem-kenis-human-rights-and-ai-powered-content-moderation-and-curation-in-social-media/.

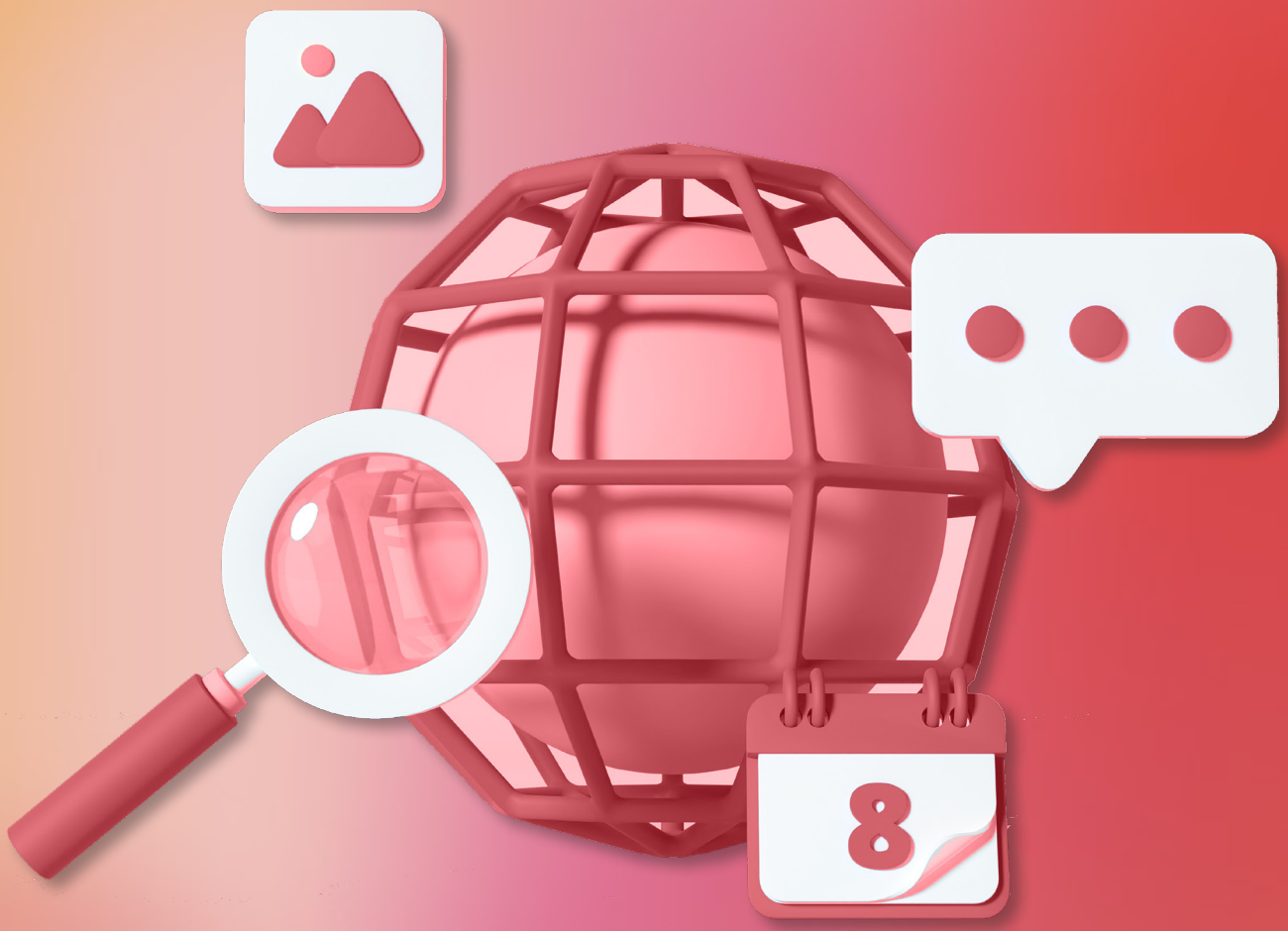
70 Reuters, "Myanmar: UN Blames Facebook for Spreading Hatred of Rohingya," the Guardian, March 13, 2018, https://www.theguardian.com/technology/2018/mar/13/myanmar-un-blames-facebook-for-spreading-hatred-of-rohingya.

Overall conclusions and thoughts

The increase of internet access has enabled freedom of expression on digital media platform is important for people to air out their opinion, Ideas and share information freely with no fear. However some people should not abuse this platform to spread propaganda, hate speech or instigate violence. In order to control these states and technology industry and human rights should develop policies that provides a safe space free of violence for people to interact.

This includes improving AI-based content moderation that fails to flag some posts on disinformation or false news to ensure its efficiency in recognition of any form of harmful content. Also, not forgetting repressive governments that may take advantage of anti-false information policies to censor the internet limiting freedom of expression. It's time to challenge the technology industry to develop strong structures that prohibit states from controlling the internet without meaningful reasons. The same effort organisations, states are pushing and advocating to increase internet access should be put to ensure digital safety for everyone.

New Digital Divide Faces: Access and Inclusion in the Digital Age



What is access and inclusion?

Access is described as the capacity, opportunity, permission, or right to approach, communicate, enter, pass to and from, or see without being obstructed or interfered with. In today's digital era, the concept is synonymous with Digital Access, which is defined as the capacity to participate fully in a digital society. This includes access to the tools and technology necessary for full engagement, such as the Internet and computers.

Digital access has become a fundamental component of digital citizenship. Digital access is a popular topic right now since it examines how many people have access to technology tools and devices. Thanks to internet access, people may now communicate and interact in real time. Access to and use of the Internet has become critical, not only for ICT, but also for economic and social growth, including achieving the Sustainable Development Goals.

However, not everyone has the ability to fully utilise the new digital society's resources. These opportunities are not available to everyone due to factors such as socioeconomic status, handicap, and geographic location. Unable to afford technology for their homes, those with limited technology tools to fully exploit the opportunities of the digital world, and those living in the peripheries with no or unstable internet access have all been disadvantaged by lack of technology access.

Digital Inclusion refers to any efforts made to build a more inclusive information society. Inclusion in this digital age means that individuals including disadvantaged groups have access to and ability to use Information and Communication Technologies (ICTs), allowing them to participate in and benefit from today's increasing knowledge and information society.[71] People from all walks of life can benefit from the internet and related technology, including those who are disadvantaged due to their educational background, physical or mental disability, gender, ethnic origins, or geographic remoteness.

71 Bosua, Rachelle, and Marianne Gloet. "Access to Flexible Work Arrangements for People With Disabilities: An Australian Study." In Anywhere Working and the Future of Work, pp. 134-161. IGI Global, 2021.

Subtopics that fall under the category of Digital Access and Inclusion: Definitions and Context

Access to the Internet refers to Individuals' capacity to connect to the Internet via computer terminals, computers, mobile phones, and other devices, and access services such as email and the World Wide Web. Access to the Internet is critical for global citizens to study, aspire, develop, and evolve. In spite of the fact that no major international human rights treaties explicitly mention access to the internet as a human right, it has been argued that such access is important to the right to freedom of expression and the eradication of socio-economic disadvantage. As a result, some countries have recognized the human right to access the Internet.[72]

Internet Affordability is defined as "1 for 2." One GB of mobile broadband should cost no more than 2% of average monthly income, according to the UN Broadband Commission.[73]

Device Affordability focuses on an individual's ability to own devices used to access the internet like smartphones. Smartphone and device ownership is one of the four pillars of meaningful connectivity[74]. The high costs of these devices is a continuing barrier to internet use for many individuals particularly in low and middle income countries.

Internet Shutdowns are intentional interruptions of the Internet by state or non-state actors which renders the internet inaccessible or effectively unusable, for a specific population and for the purposes of exerting control over the free flow of information[75]. Internet shutdowns can be explicit, when the State suspends the Internet, or implicit, when the State intentionally slows down the speed of the internet, rendering it effectively unusable. With "National" Security being used as one of the main reasons for internet shutdowns, there are several other reasons usually provided for these "Kill switches"[76] including the need to disrupt unrests, close avenues for foreign propaganda, maintain peace during elections, during state exams, punish specific companies, such as messaging services, and so on, but some scholars have cited that there are always suspicions of darker underlying motives, such as hiding voter fraud, stifling dissent, controlling media, weakening minority groups and so on.

72 Tully, Stephen. "A human right to access the Internet? problems and prospects." Human Rights Law Review 14, no. 2 (2014): 175-195.

73 Alliance for Affordable Internet."Affordability Report 2019." Annual Report. Washington DC: Web Foundation. 2019. https://a4ai.org/affordability-report/report/2019/.

74 Policy, P., Accessibility, Rss, & Map, S. "Meaningful Connectivity — unlocking the full power of internet access." n.d. Alliance for Affordable Internet. https://a4ai.org/meaningful-connectivity/

75 "Statement on Intentional Internet Shutdowns," African School on Internet Governance, October 17, 2016, https://afrisig.org/previous-afrisigs/afrisig-2016/statement-on-an-intentional-internet-shutdown/.

76 IFLA. Internet shutdowns: Backgrounds. 2019. https://www.ifla.org/

Digital Economy and Labour Rights. The digital economy[77] is defined as the economic activity generated by billions of daily online interactions between individuals, businesses, devices, data, and processes. The digital economy is built on the Internet, mobile technologies, and the Internet of things (IoT). The digital economy is taking shape and challenging long-held beliefs about how companies are organised, how firms interact, and how consumers receive services, information, and resources. The impact of digitalisation on society and work is growing. However, the shift is complicated by the rise of digital marketplaces and market leaders, which are altering various sectors and worker interactions as well as emerging developments, such as the use of artificial intelligence in the workplace, creating labour rights concerns about surveillance, health, and safety. Employers contend that with the digital economy, employees have greater autonomy and hence need less protection.

Digital divide is the gap between those who have and do not have access to computers and the internet. While it is described in that manner, it is critical to understand that there is no one digital divide; rather, it is diverse and encompasses a variety of characteristics such as access, price, quality, and relevance. The current global digital divide is put in context by ITU's report that 53.6% of the world's population uses the internet, however individuals in developing nations have a broadband Internet connection at 47%, whereas just 19.1% of people in Low Developed Countries (LDCs) do.[78]

77 Deloitte, "What Is Digital Economy? | Deloitte Malta | Technology," Deloitte Malta, October 3, 2017, https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html.

78 ITU, "Press Release," ITU, September 18, 2020, https://www.itu.int/en/mediacentre/Pages/PR20-2020-broadband-commission.aspx.

Contextual implications

Access to the Internet

Many women still lack access to the internet, due to factors such as low technology access, computer illiteracy, poverty, and prohibitively high internet costs. These factors disproportionately affect rural women from low- and middle-income areas, further widening the already pervasive digital gender divide. To avoid offending cultural and familial values, many Pakistani women are forbidden from answering phones or using the internet for communication or entertainment.[79] Beyond internet access, women also face internet-related risks and difficulties such as image-based sexual assault, non-consensual photo sharing, and online scams and hacks, leading many women to self-censor and avoid the internet. In fact a study that focused on African women in sub-Saharan countries like Ethiopia, Kenya, Uganda, Senegal, and South Africa found that 28% of women interviewed had experienced internet harassment.[80]

The world is missing out on enormous social, cultural, and economic contributions if women's access to the internet is made simple, frictionless, and safe. The digital gender divide costs governments hundreds of billions of dollars. Policymakers have a $524 billion USD potential to close this deficit in five years.[81] The digital world is a new, vibrant source of economic productivity and growth, and governments must invest in infrastructure and initiatives that enable female internet use.

Globally, internet liberties like freedom of expression have shrunk, limiting access to the internet, information, and ultimately democracy. More countries are following China's lead in implementing strong censorship and automated surveillance technology to achieve digital dictatorship.

China has one of the world's most restrictive media environments, relying on censorship to control information in the news, online, and on social media using libel lawsuits, arrests, and other means to force Chinese journalists and media organisations to censor themselves, including imprisoning 38 journalists 2017 and about 48 in 2019.[82] We have also witnessed restrictive internet and media regulations being passed in countries such as Egypt[83] and Iran[84] applying to social media users as well as journalists, and critics.

79 Research Authors et al., "Feminist Case Studies on the Gender Digital Divide amidst COVID-19 Design Aniqa Haider Published by Media Matters for Democracy in January 2021 under Creative Commons Attribution 4.0 International (CC by 4.0) Https://Creativecommons.org/Licenses/By/4.0/ Some Rights Reserved," n.d., https://digitalrightsmonitor.pk/wp-content/uploads/2021/01/Women-Disconnected-Gender-Digital-Divide-in-Pakistan.pdf.

80 Neema, Bonnita, and Sandra, "Feminist Research for a Feminist Internet," Pollicy, August 2020, https://ogbv.pollicy.org/index.html.

81 "Costs of Exclusion Report," World Wide Web Foundation, n.d., https://webfoundation.org/research/costs-of-exclusion-report/.

82 Reuters Staff, "China Imprisoned More Journalists than Any Other Country in 2019: CPJ," Reuters, December 11, 2019, https://www.reuters.com/article/us-global-rights-journalists-graphic-idUSKBN1YF0KA.

83 Tony Roberts et al., "Digital Rights in Closing Civic Space: Lessons from Ten African Countries," Opendocs.ids.ac.uk, February 26, 2021, https://doi.org/10.19088/IDS.2021.003.

84 These Technological Advancements, "Iran's 'Protection Bill' to Enhance Internet Clampdown," The Organization for

Some 500 websites, including those of important human rights groups and independent media sources, were blocked by Egyptian authorities as part of a larger assault on dissidents. Social media sites in Sri Lanka were taken down by the government for days after communal violence broke out and at least two people died.[85]

More nations have continued to restrict free access to the internet and its attendant freedoms. Countries such as Uganda implemented the Social Media Tax, which it later abolished but replaced with new charges on internet data,[86] a trend that has spread across the African continent, leaving millions of people struggling to afford the cost of accessing the internet.[87]

In order to safeguard democracy, it is essential to protect internet freedom against the growth of digital authoritarianism. Without compulsion or disguised manipulation, citizens should be able to freely and easily make their own social, economic, and political decisions via the use of technology.

World Peace, March 6, 2022, https://theowp.org/irans-protection-bill-to-enhance-internet-clampdown/.

85 Michael Safi and Amantha Perera, "Sri Lanka Blocks Social Media as Deadly Violence Continues," the Guardian (The Guardian, March 7, 2018), https://www.theguardian.com/world/2018/mar/07/sri-lanka-blocks-social-media-as-deadly-violence-continues-buddhist-temple-anti-muslim-riots-kandy.

86 Daniel Mwesigwa, "Uganda Abandons Social Media Tax but Slaps New Levy on Internet Data," cipesa.org, July 1, 2021, https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/.

87 "Taxing Social Media in Africa," The Internet Health Report 2019, March 15, 2019, https://internethealthreport.org/2019/taxing-social-media-in-africa/.

Internet Shutdowns

Internet shutdowns are perilous acts of digital authoritarianism and continue to jeopardise worldwide access to the internet. Authorities in at least 182 nations shutdown the internet in 2021, an increase from 159 shutdowns in 2020. Notable internet shutdowns have occurred in India (106 times), Myanmar (15 times), Sudan (5 times), and Iran (5 times) as of 2021[88] with trends like prolonged shutdowns, targeted blocking of communication platforms and shutdowns targeting specific locations and populations.

The infringement on access to Internet, mobile services through Internet shutdowns, during the voting and post voting periods was a setback in the role citizen journalism plays in creating civic awareness and civic engagement in the polity of countries like Uganda, Togo, Burundi, Belarus and keeping each other informed inside the electoral space.[89]Internet shutdowns have also harmed minorities and critical groups who rely on the internet for communication, safe expression, and business. Officials in India deliberately slowed internet connectivity, stifling the digital economy.[90] To discourage exam cheating, Indian officials shut down the internet four times. Ethiopians in Tigray were cut off from the internet for 18 months and 129 internet disruptions have been recorded across Asia's seven nations: Afghanistan, Bangladesh, China, India, Indonesia, Myanmar, and Pakistan.

Using data from the last five years,[91] It is evident that internet disruptions are becoming increasingly popular as tools of state control. There is a need for Governments and decision-makers to embrace policies that keep the Internet on and robust to foster strong economies and a successful future for everybody.

88 Marianne Díaz Hernández and Anthonio Felicia, "THE RETURN of DIGITAL AUTHORITARIANISM Internet Shutdowns in 2021," May 24, 2022, https://www.accessnow.org/cms/assets/uploads/2022/04/2021-KeepItOn-Report-1.pdf.
89 "#KeepItOn: 2022 Elections and Internet Shutdowns Watch," Access Now, February 24, 2022, https://www.accessnow.org/elections-internet-shutdowns-watch-2022/.
90 Zenaira Bakhsh and Rayan Naqas, "How Internet Blackouts Have Devastated Kashmir's Economy," Rest of World, April 26, 2022, https://restofworld.org/2022/blackouts-kashmir-digital-economy/.
91 "Internet Shutdowns," pulse.internetsociety.org, n.d., https://pulse.internetsociety.org/shutdowns.

Digital Economies, Taxation and Labour Rights

More African countries have yet to completely grasp the benefits of the digital economy, despite its rapid global expansion. The main issue is whether their tax systems are prepared to deal with this "new" phenomenon. The transition from a physical to an electronic and information-based economy poses considerable challenges to existing tax structures.[92]

For many governments beyond Africa, the digital economy offers a new source of revenue, helping to meet their constantly increasing financial needs. Several African countries have proposed tariffs on users of social media and mobile applications, citing the loss of tax revenue from traditional voice and message services as more people use mobile applications.[93] Uganda, Zambia, and Benin all taxed mobile apps, social media, and data packages.[94] To preserve their revenue basis without inhibiting the development and usage of new technologies or enterprises' involvement in the rising electronic markets, African countries are battling with sustaining their tax bases. To avoid missing out on the benefits of the future of employment, African governments must investigate ways to secure their tax bases without impeding the growth of the global digital economy.

The internet's growth has changed the traditional workforce, allowing the gig economy to grow and diversify. The coronavirus pandemic has also accelerated the rise of the gig economy, with projections of annual growth of 17% to $455 billion by 2023.[95] However, the digital-gig economy has raised new labour rights issues, including artificial intelligence-based surveillance, worker mental health degradation (technostress), and online safety concerns. Employees have more autonomy and hence deserve less protection, employers claim. Also, the exclusion of gig workers from labour and domestic work protection standards has raised concerns, as these policies are targeted toward more traditional work patterns. Women who operate as gig workers in the Philippines are categorised as third-party workers, not eligible for government benefits or even considered ordinary domestic workers.[96] It is vital to create legal frameworks that require companies to be more tolerant, inclusive and address emerging issues and threats to labour rights especially among disadvantaged groups.

92 Solomon Rukundo, "Taxation of the Telecommunications Sector: A Focus on Policy Issues and Considerations in Taxation of Mobile Money in Uganda," SSRN Electronic Journal, 2017, https://doi.org/10.2139/ssrn.3132994.
93 Christoph Stork, Steve Esselaar, and Chenai Chair, "OTT - Threat or Opportunity for African Telcos?," Telecommunications Policy 41, no. 7-8 (August 2017): 600–616, https://doi.org/10.1016/j.telpol.2017.05.007.
94 "After Uganda, Benin and Zambia Impose 'Worrying' Tax on Social Networks | RSF," rsf.org, n.d., https://rsf.org/en/after-uganda-benin-and-zambia-impose-worrying-tax-social-networks.
95 A Gus, "THOUGHT LEADERSHIP Fueling the Global Gig Economy How Real-Time, Card-Based Disbursements Can Support a Changing Workforce," n.d., https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/mastercard-fueling-the-global-gig-economy-2020.pdf.
96 Liza Garcia et al., "Digitization and Domestic Work: The Policy Environment in the Philippines," Foundation for Media Alternatives, May 2019, https://www.fma.ph/resources/reports-and-studies/digitization-and-domestic-work-the-policy-environment-in-the-philippines/.

Data Governance

What is Data Governance?

According to the Data Governance Institute,[97] "Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods" or simply put, "the exercise of decision-making and authority for data-related matters."

The definition of data governance has greatly broadened from its earlier conception as an emerging trend in enterprise information management[98] guiding how enterprises ought to view data to also refer to "norms, principles and rules governing various types of data".[99] This latter definition gives room for the conceptualisation of data governance as an umbrella term related to international legal frameworks such as the General Data Protection Regulation (GDPR) and national Data Protection Regulations (DPRs).

Data Protection and Data Governance

Just like data governance, data protection is a term that encompasses processes involved in the safeguarding of important information from corruption, compromise or loss by corporate interests and which exists as a tool in an enterprise's data governance arsenal. As a legal concept, it has been described as an instance of the historically established right to privacy, also known as the right to be let alone, with an emphasis on personal information.[100]

Today data protection regulations are increasing all over the globe in response to the EU's GDPR and due to the growing significance of data and Big Data globally. The problem of Big Data, a term that describes the "exponentially increasing volumes and variety of data held by corporations and governments that cannot easily be processed or manipulated with ordinary tools"[101] has been described as a problem of variety, velocity, and volume of data, or the three Vs,[102], especially from new sources.

97 "Definitions of Data Governance," The Data Governance Institute, accessed May 9, 2022, https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/.
98 Lai Kuan Cheong and Vanessa Chang, "The Need for Data Governance: A Case Study," 18th. ACIS 2007 Proceedings, no 100 (2007): 999. http://aisel.aisnet.org/acis2007/100
99 "FAQ," Digital Trade and Data Governance Hub, accessed May 9, 2022, https://datagovhub.elliott.gwu.edu/faq/.
100 Christopher Millard, "Data Protection in the Clouds," in Society and the Internet: How Networks of Information and Communication are Changing Our Lives, ed. Mark Graham and William H. Dutton (New York: Oxford University Press, 2019), 148.
101 Susan Bennett. "What Is Information Governance and How Does It Differ from Data Governance?" Governance Directions 69, no. 8 (2017): 463. https://search.informit.org/doi/10.3316/informit.070201793736360.
102 "What is Big Data?," Oracle, accessed May 9, 2022, https://www.oracle.com/big-data/what-is-big-data/#:~:text=Big%20data%20defined,-What%20exactly%20is&text=The%20definition%20of%20big%20data,especially%20from%20new%20data%20sources.

Data, and its associated benefits and challenges, have become an extremely important source of value for corporations and governments, prompting many comparisons with natural resources such as oil and sunlight.[103] For corporations, the ability to access, collect, and process data no doubt provides huge opportunities to create and refine data-driven products and services for profit. Similarly, for governments, data poses opportunities to promote service delivery and concerns regarding cyber risk and opportunities.

For women, data collection and its manipulation and absence are extremely significant. What researchers have called a "female-shaped 'absent presence'" or the gender data gap means that the underrepresentation of women in data collection and reporting affects the development of wearables designed for women as well as government planning.[104]

Algorithmic Harms

An algorithm is a set of instructions for solving a particular problem.[105] Algorithms capable of "learning" on their own or the process through which machines learn from data is known as Machine Learning.[106]

Algorithms are used to accomplish various tasks and are deployed in many settings, platforms and devices such as on social media sites like Twitter and YouTube for content moderation and content suggestion, by fintechs to calculate creditworthiness and grant loans and for surveillance purposes.

However, algorithms, especially in automated decision-making contexts, have come under intense scrutiny and criticism. The Machine Learning process is carried out by training, and machine learning-based systems are heavily reliant on data to "learn". However, as data refers to historical records and distinct pieces of information, stored as values of quantitative and qualitative variables, which can be machine-readable, human-readable or both,[107] these pieces of information and records are heavily embedded with human biases, which when used to train algorithms, replicate historical biases. Algorithmic harms are, therefore, biased inferences which hurt people made by algorithmic systems.

103 "Data is neither Oil nor Sunlight," CIO, accessed May 9, 2022, https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-is-neither-oil-nor-sunlight/77647068
104 "The 'missing women' in data protection reporting," IAPP, accessed May 9, 2022, https://iapp.org/news/a/the-missing-women-in-data-protection-reporting/
105 "What is a computer algorithm?," HowStuffWorks, accessed May 9, 2022, https://computer.howstuffworks.com/what-is-a-computer-algorithm.htm.
106 Stephen F. Deangelis and Enterra Solutions, "Artificial Intelligence: How Algorithms Make Systems Smart," Wired, September, 2014, https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/.
107 Neema Iyer et al., Afrofeminist Data Futures (Kampala: Pollicy, 2021), 35, https://archive.pollicy.org/wp-content/uploads/2021/03/Afrofeminist-Data-Futures-Report-ENGLISH.pdf

In Latin America, for instance, some harmful use cases of AI algorithms include their use to monitor and surveill the poor and predict teenage pregnancy. Its prominent use by public institutions has been criticised for perpetuating racism and poverty as wealthier people are more likely to benefit from the use of AI-product products and services than are the poor. The poor are also more likely to have to rely on automated decision making to access services than the wealthy, who are able to leverage their personal connections.[108] The vulnerability of poor women, in particular to surveillance, leads to the reproduction of economic and gender inequalities.

In the Middle East, surveillance systems have enabled Israel's Population and Immigration Authority to make arbitrary and discriminatory decisions about entry into Israel and the occupied Palestinian territory and keep a "blacklist" of activists denied entry by relying on data from the internet and social media. Meaningful critique is also drowned and conflated with anti-Semitic rhetoric online through the manipulation of social media algorithms.[109]

To turn the tide, it might be useful to borrow a leaf from a group of feminist technologists who created a chatbot, Betânia, who argue for the need to go beyond feminist critiques of algorithms to rather focus on how organisations, collectives, and/or individuals employ algorithms for feminist ends.[110]

108 Cathy O'Neil, Weapons of math destruction: How big data increases inequality and threatens democracy. (New York: Broadway Books, 2016).

109 "Israel releases 'BDS blacklist' banning 20 NGOs from entering country," Adalah, https://www.adalah.org/en/content/view/9347

110 Sophie Toupin and Stephane Couture, "Feminist chatbots as part of the feminist toolbox," Feminist Media Studies 20, no. 5 (2020): 737-740, doi: 10.1080/14680777.2020.1783802

Intellectual Property Rights

Intellectual Property Rights are those rights which accrue to a person over their own creations, usually for a specified period of time.[111] There are basically two types of intellectual property rights, namely copyright and industrial property. While copyright refers to the right protecting an author's work in any circumstance from invasion or infringement, industrial property refers to protective rights conferring an exclusive monopoly on exploitation obtainable through and upon completion of filing and registration formalities. Examples of industrial property rights are patents, trademarks, industrial designs, service marks and geographical indications.

The digital nature of today's world, however, has made piracy and counterfeiting of products easy to carry out. One of the major tensions involved with intellectual property rights is the competing interests of the creative and her right to retain an interest in her creation and make a profit off of it versus the right of the community to enjoy collective access to it for communal benefit.

A particularly interesting example of this conflict are the ongoing international deliberations between pharmaceutical companies, the EU, and Global South countries, including India and South Africa and the World Health Organisation for a waiver of intellectual property restrictions on vaccines for the period of the pandemic.[112]

As it relates to intellectual property, a significant alternative to mainstream, enterprise-centred data governance and data stewardship methods is the concept of indigenous data sovereignty. This concept is intricately tied to legal frameworks such as the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) and the Universal Declaration of Human Rights. The conceptualisation of intellectual property ranges beyond the Western notion of intellectual property to also include the knowledge as well as cultural practices, rituals and belief system that produce these artefacts.[113]

An appreciation for how the data of indigenous communities can be respectfully governed and their intellectual property protected and cherished may grant us further insight into how this field may be better developed for collective benefit.

111 "What are intellectual property rights?," World Trade Organisation, accessed May 9, 2022, https://www.wto.org/english/tratop_e/trips_e/intel1_e.htm#:~:text=Intellectual%20property%20rights%20are%20the,a%20certain%20period%20of%20time.

112 "South Africa hailed by WTO over compromise on COVID vaccine production waivers," Africa News, accessed May 6, 2022, https://www.africanews.com/2022/03/17/south-africa-hailed-by-wto-over-compromise-on-covid-vaccine-production-waivers//; "EU, Africa at odds over vaccine patents ahead of summit," Africa News, accessed May 6, 2022, https://www.africanews.com/2022/02/15/eu-africa-at-odds-over-vaccine-patents-ahead-of-summit//

113 Michael Barry Davis and Department of the Parliamentary Library. Information and Research Services Australia., Indigenous peoples and intellectual property rights. (Canberra: Department of the Parliamentary Library, 1997), https://nla.gov.au/nla.cat-vn1664504

Open Data and Transparency

Open Data refers to data that anyone can access, use and share.[114] The open data movement advocates for the sharing of data to improve and promote research, knowledge sharing, and transparency in government spending and service delivery, among other uses. While the concept of open data and transparency are laudable goals, there are certain challenges in the form of legal, social and technological barriers which pose a challenge to its adoption.[115]

Legally, the existence of intellectual property rights and other forms of ownership poses a barrier to the creation of new open data governance frameworks. Defined to mean the interplay of rules, standards, tools, principles, processes and decisions that influence what government data is opened up, how and by whom, open data governance would require radical shifts in policy at all levels of government while still grappling with the problem of selecting "good" open data.[116]

On a social level, barriers to the implementation of open data would be a natural distrust are related to the history of a community and how this has shaped the value attached to data sharing. In Africa, one such question is if "the African continent should aspire to develop its own data sharing policies and initiatives grounded in its distinct values, context, and communal culture?"[117] Another is "Is data sharing beneficial? Valuable?" and "for whom?"[118] According to Abebe et al,[119] power asymmetries, trust, as well as contexts and local knowledge based on Africa's unique history with exploitation, extractivism and colonisation are some of the challenges to open data on the continent.

Technically speaking, non-machine-readable documents, as well as the use of paper and legacy software, are reflective of some of the infrastructural deficits involved in open data.

114 "What is open data?" Open Data Institute, accessed May 9, 2022, https://data.gov.ie/edpelearning/en/module1/#/id/co-01
115 Jeremy de Beer, Ownership of open data: Governance options for agriculture and nutrition (Wallingford: Global Open Data for Agriculture and Nutrition, 2016). doi: 10.1079/CABICOMM-79-13
116 Ana Brandusescu, Carlos Iglesias, Danny Lämmerhirt, and Stefaan Verhulst, "Open data governance and open governance: Interplay or disconnect?," World Wide Web Foundation. https://webfoundation. org/2019/02/open-data-governance-and-open-governance-interplay-or-disconnect (2019).
117 Rediet Abebe, Kehinde Aruleba, Abeba Birhane, Sara Kingsley, George Obaido, Sekou L. Remy, and Swathi Sadagopan, "Narratives and counternarratives on data sharing in Africa," in Proceedings of the 2021 ACM conference on fairness, accountability, and transparency, pp. 329-341. 2021, https://arxiv.org/pdf/2103.01168.pdf
118 Ibid, 335.
119 Ibid.

Conclusion

Despite the freedoms afforded by an open, fair and transparent internet, many communities, in both democratic and authoritarian governing systems, face a number of infringements on their digital rights. As our lives move primarily into online realms, the importance of our rights and liberties in the digital world becomes increasingly important. It is critical to tackle inherent societal biases, which can be further amplified in online spaces.

In the global South, digital rights is an emerging issue that particularly intersects with civic space, governance and activism. This paper is a step in documenting key issues by mapping the key stakeholders and collating knowledge across the sector, with a focus on traditionally unprioritised voices in the digital rights ecosystem. There is a need for significant and ongoing research, programmatic activities, policy development and movement building to create an ideal internet that works for everyone.

Works Cited

"After Uganda, Benin and Zambia Impose 'Worrying' Tax on Social Networks | RSF." n.d. Rsf.org. https://rsf.org/en/after-uganda-benin-and-zambia-impose-worrying-tax-social-networks.
———. 2019b.

"China Imprisoned More Journalists than Any Other Country in 2019: CPJ." Reuters,December 11, 2019. https://www.reuters.com/article/us-global-rights-journalists-graphic-idUSKBN1YF0KA.

"Data Is Neither Oil nor Sunlight - et CIO." ETCIO.com, August 20, 2020. https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-is-neither-oil-nor-sunlight/77647068.

"The Data Governance Institute. "Definitions of Data Governance," n.d. https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/.

"South Africa Hailed by WTO over Compromise on COVID Vaccine Production Waivers." Africanews, 2022. https://www.africanews.com/2022/03/17/south-africa-hailed-by-wto-over-compromise-on-covid-vaccine-production-waivers/.

Abebe,Rediet,Kehinde Aruleba,Abeba Birhane,Sara Kingsley,George Obaido, Sekou L. Remy, and Swathi Sadagopan. "Narratives and counternarratives on data sharing in Africa." In Proceedings of the 2021 ACM conference on fairness, accountability, and transparency. https://arxiv.org/pdf/2103.01168.pdf

AfricaNews. "EU, Africa at Odds over Vaccine Patents ahead of Summit." Africanews, 2022. https://www.africanews.com/2022/02/15/eu-africa-at-odds-over-vaccine-patents-ahead-of-summit/.
datagovhub.elliott.gwu.edu. "FAQ." Accessed June 1, 2022. https://datagovhub.elliott.gwu.edu/faq/.

AFSS. "Domestic Disinformation on the Rise in Africa – Africa Center." Africa Center for Strategic Studies, October 6, 2021. https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/.

Agwuegbo, Chioma. "Reclaiming Nigeria's Shrinking Online Civic Space." (2021).

Ahmed, Abdulateef. “Mainje: Malawian Nurse Arrested by Police for Cyber Harassment.” News Central TV | Latest Breaking News across Africa, Daily News in Nigeria, South Africa, Ghana, Kenya and Egypt Today. May 3, 2022. https://newscentral.africa/2022/05/03/malawian-nurse-arrested-by-police-for-disrespecting-president-online/?utm_source=newsletter&utm_medium=email&utm_campaign=a_troubling_whatsapp_update&utm_term=2022-05-07.

Alliance for Affordable Internet.“Affordability Report 2019.” Annual Report. Washington DC: Web Foundation. 2019. https://a4ai.org/affordability-report/report/2019/.

Arora, Payal. “Decolonizing privacy studies.” Television & New Media 20, no. 4 (2019): 366-378.
Bakhsh, Zenaira, and Rayan Naqash. 2022. “How Internet Blackouts Have Devastated Kashmir’S Economy”. Rest Of World. https://restofworld.org/2022/blackouts-kashmir-digital-economy/.

Balmforth, Andrei Makhovsky, Tom. “Internet Blackout in Belarus Leaves Protesters in theDark.” Reuters, August 11, 2020. https://www.reuters.com/article/us-belarus-election-internet-idUSKCN2571Q4.

BBC. “Telegram: Why Won’t You Take My Nudes Down?” Www.youtube.com. February 16, 2022. https://www.youtube.com/watch?v=M-arIpw9fVw.

BBC. “World Leaders’ Posts Deleted over False Virus Info.” BBC News, March 31, 2020, sec. Technology. https://www.bbc.com/news/technology-52106321.

Bennett, Susan. “What Is Information Governance and How Does It Differ from Data Governance?” Governance Directions 69, no. 8 (2017): 463. https://search.informit.org/doi/10.3316/informit.070201793736360.

Bernal, Paul A. “The right to online identity.” Available at SSRN 2143138 (2012).

Bisbal, Marcelino. “FROM FREEDOM of EXPRESSION to the RIGHT to COMMUNICATION: Scope and Boundaries,”2013.https://media.sipiapa.org/adjuntos/186/documentos/001/839/0001839740.pdf.

Bosua, Rachelle, and Marianne Gloet. “Access to Flexible Work Arrangements for People With Disabilities: An Australian Study.” In Anywhere Working and the Future of Work, pp. 134-161. IGI Global, 2021.

Brandusescu, Ana, Carlos Iglesias, Danny Lämmerhirt, and Stefaan Verhulst. “Open data governance and open governance: Interplay or disconnect?” World Wide Web Foundation. Accessed May 30, 2022. https://webfoundation.org/2019/02/open-data-governance-and-open-governance-interplay-

or-disconnect/

Buchanan, Tom. “Why Do People Spread False Information Online? The Effects of Message and Viewer Characteristics on Self-Reported Likelihood of Sharing Social Media Disinformation.” Edited by Jichang Zhao. PLOS ONE 15, no. 10 (October 7, 2020): e0239666.https://doi.org/10.1371/journal.pone.0239666.

Cheong, Lai Kuan and Vanessa Chan., “The Need for Data Governance: A Case Study.” 18th . ACIS 2007 Proceedings, no 100 (2007): 999. http://aisel.aisnet.org/acis2007/100

Colleen McClain, “How Parents’ Views of Their Kids’ Screen Time, Social Media Use Changed during COVID-19,” Pew Research Center, 2022, https://www.pewresearch.org/fact-tank/2022/04/28/how-parents-views-of-their-kids-screen-time-social-media-use-changed-during-covid-19/#:~:text=Among%20parents%20with%20a%20young.

Coombs, Elizabeth, and Kara McKee. “The ‘Missing Women’ in Data Protection Reporting.” iaap, June13,2019.https://iapp.org/news/a/the-missing-women-in-data-protection-reporting/.

Cube. “Human Rights Guide.” Human Rights Guide, April 13, 2022. https://www.cilvektiesibugids.lv/en/themes/freedom-of-expression-media#:~:text=Freedom%20of%20expression%20%26%20Democracy.

Dahlgren, Peter. “The internet as a civic space.” In Handbook of digital politics. Edward Elgar Publishing, 2015.

Datla, Anjani. “Redirect Notice.” www.google.com, November 16, 2020. https://www.google.com/url?q=https://case.hks.harvard.edu/leading-with-empathy-tarana-burke-and-the-making-of-the-me-too-movement/&sa=D&source=docs&ust=1652897353206861&usg=AOvVaw0KFj--sWG_0ibxS85YVlaa.

Davis, Michael Barry and and Department of the Parliamentary Library Information and Research Services Australia. Indigenous peoples and intellectual property rights. Canberra: Department of the Parliamentary Library, 1997. https://nla.gov.au/nla.cat-vn1664504

De Beer, Jeremy. Ownership of open data: Governance options for agriculture and nutrition.” Wallingford: Global Open Data for Agriculture and Nutrition, 2016. Doi: 10.1079/CABICOMM-79-13

Deadly Violence Continues”. The Guardian. https://www.theguardian.com/world/2018/mar/07/sri-lanka-blocks-social-media-as-deadly-violence-

continues-buddhist-temple-anti-muslim-riots-kandy.

Deangelis, Stephen F. and Enterra Solutions. “Artificial Intelligence: How Algorithms Make Systems Smart,” Wired. September, 2014. https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/.

Deloitte. “What is the digital economy? | Deloitte Malta | Technology.” October 3 2017. Deloitte Malta. https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

Dizikes, Peter. 2018. “Study: On Twitter, False News Travels Faster than True Stories.” MIT News |Massachusetts Institute of Technology. March 8, 2018. https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

Economy, Elizabeth C. 2018. “The Great Firewall of China: Xi Jinping’s Internet Shutdown.” The Guardian. The Guardian. July 4, 2018. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Farahat, Mohamed. “Egypt Digital Rights Landscape Report.” Digital Rights in Closing Civic Space: Lessons from Ten African Countries (2021).

Frener, Regine, and Sabine Trepte. “Theorizing Gender in Online Privacy Research.” Journal of Media/;p0 Psychology (2022).

Fuentes, Marcela A. “Digital Activism.” Encyclopedia Britannica, 2021. https://www.britannica.com/topic/digital-activism.

Garcia, Liza, Teresita Barrameda, Jessamine Pacis, and Arlen Sandino Barrameda. “Digitization and Domestic Work: The Policy Environment in the Philippines.” (2019).

Gus, A. “THOUGHT LEADERSHIP Fueling the Global Gig Economy How Real-Time, Card-Based Disbursements Can Support a Changing Workforce,” August 2020. https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/mastercard-fueling-the-global-gig-economy-2020.pdf.

Gqola, Pumla Dineo. Female Fear Factory. Mellinda Ferguson Books, 2021.

Hao, Karen. “A Deepfake Bot Is Being Used to ‘Undress’ Underage Girls.” MIT Technology Review, 2020.https://www.technologyreview.com/2020/10/20/1010789/ai-deepfake-bot-undresses-women-and-underage-girls/

Hellegren, Z. Isadora. “A history of crypto-discourse: Encryption as a site of struggles to define internet freedom.” Internet Histories 1, no. 4 (2017): 285-311.

Hernández, Marianne Díaz and Anthonio, Felicia. The Return of Digital Authoritarianism: Internet Shutdowns in 2021. April 2022. Access Now. https://www.accessnow.org/cms/assets/uploads/2022/04/2021-KeepItOn-Report-1.pdf

Hildebrandt, Mireille. “Balance or trade-off? Online security technologies and fundamental rights.” Philosophy & Technology 26, no. 4 (2013): 357-379.

Holloway, Kerrie, and Oliver Lough. “Although Shocking, the Rohingya Biometrics Scandal Is Not Surprising and Could Have Been Prevented.” ODI. Accessed May 17, 2022. https://odi.org/en/insights/although-shocking-the-rohingya-biometrics-scandal-is-not-surprising-and-could-have-been-prevented/.

HowStuffWorks. “What Is a Computer Algorithm?,” September 5, 2001. https://computer.howstuffworks.com/what-is-a-computer-algorithm.htm.

IFLA. Internet shutdowns: Backgrounds. 2019. https://www.ifla.org/

Isman, Aytekin, and Ozlem Canan Gungoren. “Digital citizenship.” Turkish Online Journal of Educational Technology-TOJET 13, no. 1 (2014): 73-77.

ITU, “Press Release,” ITU, September 18, 2020, https://www.itu.int/en/mediacentre/Pages/PR20-2020-broadband-commission.aspx.

Iyer, Neema, Chenai Chair and Garnett Achieng’. Afrofeminist Data Futures. Kampala: Pollicy, 2021. https://archive.pollicy.org/wp-content/uploads/2021/03/Afrofeminist-Data-Futures-Report-ENGLISH.pdf

Johnston, Donald H., ed. Encyclopaedia of international media and communications. Vol. 3. San Diego, Calif.: Academic Press, 2003.

Kalema, Stephen. “We Are Ready for Any Propaganda War! Bobi Wine’s Brother Nyanzi Speaks out on Allegations That He Begs Money from NUP MPs.” Watchdog Uganda, January 23, 2022. https://www.watchdoguganda.com/news/20220123/128778/we-are-ready-for-any-propaganda-war-bobi-wines-brother-nyanzi-speaks-out-on-allegations-that-he-begs-money-from-nup-mps.html.

Karusala, Naveena, and Neha Kumar. “Women’s Safety in Public Spaces.” Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, May. https://doi.org/10.1145/3025453.3025532.

Kaspersky, Eugene. “The cybercrime arms race.” (2008).

Kenis, Sebnem. “Human Rights and AI-Powered Content Moderation and Curation in Social Media.” The Raoul Wallenberg Institute of Human Rights and Humanitarian Law, August 19, 2021. https://rwi.lu.se/blog/sebnem-kenis-human-rights-and-ai-powered-content-moderation-and-curation-in-social-media/.

Koch, Richie. “What Is Internet Censorship, and How Does It Work?” ProtonVPN Blog, March 16, 2022. https://protonvpn.com/blog/how-does-internet-censorship-work/.

Kryss Network. “Online Gender-Based Violence: Issues and Policy Implications.” Kryss Network. 2022 https://kryssnetworkgroup.files.wordpress.com/2022/02/online-gender-based-violence_-issues-and-policy-implications_policy-brief_eng-version.pdf.

Latham, Holly. 2020. “Fake News and Its Implications for Human Rights.” Human Rights Pulse. December 14, 2020. https://www.humanrightspulse.com/mastercontentblog/fake-news-and-its-implications-for-human-rights.

Lewis, James A. and William Crumpler. “Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape.” Center for Strategic and International Studies (2021 September). URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY

Lynch, Marc. “Mobilizing through Online Media.” The Century Foundation, May 9, 2017. https://tcf.org/content/report/mobilizing-online-media/?session=1.

Martin, Jason A., and Anthony L. Fargo. “Anonymity as a legal right: Where and why it matters.” NCJL & Tech. 16 (2014): 311.

McQuate, Mitchell. 2022. “Iran’s “Protection Bill” To Enhance Internet Clampdown”. The Organization For World Peace. https://theowp.org/irans-protection-bill-to-enhance-internet-clampdown/.

Michael, and Amanda Perrera. 2018. “Sri Lanka Blocks Social Media As
Millard, Christopher. “Data Protection in the Clouds.” In Society and the Internet: How Networks of

Information and Communication are Changing Our Lives, edited by Mark Graham and William H. Dutton, New York: Oxford University Press, 2019.

Moyakine, Evgeni. “Online Anonymity in the Modern Digital Age: Quest for a

Legal Right." Journal of Information Rights, Policy and Practice 1, no. 1 (2016).

Mwesigwa, Daniel. 2021. "Uganda Abandons Social Media Tax But Slaps New Levy On Internet Data". Cipesa.Org.https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/.

Naumov, Viktor B. "Information security in identification in the digital age: information law aspect." Gosudarstvo i pravo 9 (2019): 117-130.

O'Brien, Danny. "The 10 Tools of Online Oppressors." Committee to Protect Journalists, May 2, 2011. https://cpj.org/reports/2011/05/the-10-tools-of-online-oppressors/.

O'Neil, Cathy. Weapons of math destruction: How big data increases inequality and threatens democracy. New York: Broadway Books, 2016.

Oracle.com. "What Is Big Data?," 2021. https://www.oracle.com/big-data/what-is-big-data/#:~:text=Big%20data%20defined

Ott, Megan. "Series: What Does That Mean? Gender-Based Violence." Women for Women International. Accessed May 17, 2022. https://www.womenforwomen.org/blogs/series-what-does-mean-gender-based-violence.

Pena, Paz, and Joana Varom, "Decolonising AI: A Transfeminist Approach to Data and Social Justice." 2019, Association for Progressive Communication.

Perera, Sachini. Review of WHITE PAPER on FEMINIST INTERNET RESEARCH. APC. https://www.apc.org/sites/default/files/firn-whitepaper-2022.pdf

Policy, P., Accessibility, Rss, & Map, S. "Meaningful Connectivity — unlocking the full power of internet access." n.d. Alliance for Affordable Internet. https://a4ai.org/meaningful-connectivity/

Pulgarín, Ana María Rodríguez and Woodhouse, Teddy. Costs of Exclusion: Economic Consequences of the Digital Gender Gap. 2021. World Wide Web Foundation. Retrieved May 3, 2022, from https://webfoundation.org/research/costs-of-exclusion-report/

Ranganathan, Nayantara. "A Handy Guide to Decide How Safe That Safety App Will Really Keep You." Genderingsurveillance.internetdemocracy.in. 2017. https://genderingsurveillance.internetdemocracy.in/safety-app/.

Research Authors et al., "Feminist Case Studies on the Gender Digital Divide amidst COVID-19 Design Aniqa Haider Published by Media Matters for Democracy in January 2021 under Creative Commons Attribution 4.0

International (CC by 4.0) Https://Creativecommons.org/Licenses/By/4.0/ Some Rights Reserved," n.d., https://digitalrightsmonitor.pk/wp-content/uploads/2021/01/Women-Disconnected-Gender-Digital-Divide-in-Pakistan.pdf.

Reuters. "Myanmar: UN Blames Facebook for Spreading Hatred of Rohingya." the Guardian, March 13, 2018. https://www.theguardian.com/technology/2018/mar/13/myanmar-un-blames-facebook-for-spreading-hatred-of-rohingya.

Roberts, Tony, Abrar Mohamed Ali, George Karekwaivanane, Natasha Msonza, Sam Phiri, Juliet Nanfuka, Tanja Bosch et al. "Digital rights in closing civic space: Lessons from ten African countries." (2021).

Rukundo, Solomon. "Addressing the challenges of taxation of the digital economy: lessons for African countries." (2020).

Safi, Schia, Niels Nagelhus. "The cyber frontier and digital pitfalls in the Global South." Third World Quarterly 39, no. 5 (2018): 821-837.

Schulz, Wolfgang, and Joris van Hoboken. Human rights and encryption. UNESCO Publishing, 2016.

Scott, Mark, and Janosch Delcker. "Free Speech vs. Censorship in Germany." POLITICO. POLITICO, January 4, 2018. https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech/.

Shanti, Nishtha. "'Smile! UP Police Is Watching': On Distress, Surveillance and Emotion Mapping."Feminism in India. February 10, 2021. https://feminisminindia.com/2021/02/11/up-police-watching-surveillance-emotion-mapping

Sherri Gordon. "What Is the #MeToo Movement?" Verywell Mind, 2019. https://www.verywellmind.com/what-is-the-metoo-movement-4774817.

"Statement on Intentional Internet Shutdowns," African School on Internet Governance, October 17, 2016, https://afrisig.org/previous-afrisigs/afrisig-2016/statement-on-an-intentional-internet-shutdown/.

Stork, Christoph, and Steve Esselaar. "OTT and Other ICT Sector Taxes." (2018). Taxing social media in Africa. The Internet Health Report 2019. https://internethealthreport.org/2019/taxing-social-media-in-africa/

Storyful. "Misinformation vs. Disinformation: What's the Difference?" Storyful, September 24, 2018. https://storyful.com/thought-leadership/

misinformation-and-disinformation/.

Sweeney, Michael S., Nicholas G. Evans, and Barney Warf. “Censorship - an Overview | ScienceDirect Topics.” Sciencedirect.com, 2017. https://www.sciencedirect.com/topics/social-sciences/censorship.

TEDx Talks, “Privacy in the Digital Age | Nicholas Martino | TEDxFSCJ,” (2016-01-21) URL: https://www.youtube.com/watch?v=PuhifEL5VsU

The World Bank, “How Countries Are Using Edtech (Including Online Learning, Radio, Television, Texting) to Support Access to Remote Learning during the COVID-19 Pandemic,” World Bank, 2020, https://www.worldbank.org/en/topic/edutech/brief/how-countries-are-using-edtech-to-support-remote-learning-during-the-covid-19-pandemic.

Toupin, Sophie, and Stephane Couture. “Feminist chatbots as part of the feminist toolbox.” Feminist Media Studies 20, no. 5 (2020): 737-740. https://doi.org/10.1080/14680777.2020.1783802

Tully, Stephen. “A human right to access the Internet? problems and prospects.” Human Rights Law Review 14, no. 2 (2014): 175-195.

UN Human Rights Council, ‘Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye’ (22 May 2015) UN Doc. A/HRC/29/32.

Unicef, “Children at Increased Risk of Harm Online during Global COVID-19 Pandemic - UNICEF,” www.unicef.org, 2020, https://www.unicef.org/southafrica/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic-unicef.

Wang, Yaqiu. 2020. “In China, the ‘Great Firewall’ Is Changing a Generation.” POLITICO. September 1, 2020. https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385

Warf, Barney. “4 - Southeast Asia.” Edited by Barney Warf. ScienceDirect. Chandos Publishing, January 1, 2017. https://www.sciencedirect.com/science/article/pii/B9780081008737000040.

Waszak, Przemyslaw M., Wioleta Kasprzycka-Waszak, and Alicja Kubanek. “The Spread of Medical Fake News in Social Media – the Pilot Quantitative Study.” Health Policy and Technology 7, no. 2 (June 2018): 115–18. https://doi.org/10.1016/j.hlpt.2018.03.002.

Weber, Rolf H. “The right to be forgotten: More than a Pandora’s box.” J. Intell. Prop. Info. Tech. & Elec. Com. L. 2 (2011): 120.

Wessels, Bridgette. “Identification and the practices of identity and privacy in everyday digital communication.” New media & society 14, no. 8 (2012): 1251-1268.

West, Darrell M. “Redirect Notice.” www.google.com, December 18, 2017. https://www.google.com/amp/s/www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/%3famp.

What is open data?” Open Data Institute. Accessed May 9, 2022. https://data.gov.ie/edpelearning/en/module1/#/id/co-01

www.adalah.org. “Israel Releases ‘BDS Blacklist’ Banning 20 NGOs from Entering Country - Adalah.” Accessed June 1, 2022. https://www.adalah.org/en/content/view/9347.

www.wto.org. “WTO | Intellectual Property (TRIPS) - What Are Intellectual Property Rights?,” n.d. https://www.wto.org/english/tratop_e/trips_e/intel1_e.htm#:~:text=Intellectual%20property%20rights%20are%20the.

Zhang, Boyang, and Marita Vos. “(PDF) How and Why Some Issues Spread Fast in Social Media.” ResearchGate, February 2015. https://www.researchgate.net/publication/275041532_How_and_Why_Some_Issues_Spread_Fast_in_Social_Media.