


behind the work of digital justice



POLLICY



Authors:

Amber Sinha & Mardiya Siba Yahaya

Researchers:

Mardiya Siba Yahaya, Soledad Magnone, Colleen Wood, Jason Muyumba,
Phillip Ayazika

Data Analysis

Mardiya Siba Yahaya
Bonnita Nyamwire

March 2023

contents

01	introduction
03	an ideal internet
13	the funding landscape
15	localisation & career pathways
18	conclusion
19	annexure

introduction

01

This study explores and investigates **the reactive nature of digital rights & digital security programs.**

Constantly reacting to rapidly emerging challenges may hinder organisations in this sector from reflecting on the quality of their interventions, including whether they are able to meet understood needs or replicate successes and course correct on mistakes.

During our data collection and analysis, we centred the vision of an ideal Internet that practitioners had, and how a variety of factors both enabled and hindered their attempts to create, grow and sustain communities, ecosystems and networks that can strive towards this imagined ideal. Through interviews, focus group discussion and analysis, the community of practitioners defined their version of the ideal internet, the gaps, challenges and opportunities within the digital rights and safety ecosystem that influence how the community conducts their work, engages in retrospective inquiries, reflects, and adapts learnings from the interventions within the space.

The research was designed to bring together the experiences and narratives of digital rights and security practitioners in five regions globally, i.e. Eastern Europe, the Balkans, Asia, Africa and Latin America, and was conducted through a qualitative study with 56 participants.

We employed a purposive sampling technique to reach out to key digital rights and digital security practitioners, activists, organisations, trainers and institutions. We organised our participants across domains of expertise and practice ranging from digital security, digital rights, data governance, freedom of expression, communication and information, and privacy, anonymity and identification. We also paid attention to whether the participants were individual activists or

members of organisations. Finally, to ensure our data was representative of different genders, we also attempted to create a gender distribution of cis-gendered men, cis-gendered women, non-binary people, and transgender individuals. However, given that most people under certain gender categories may operate and work in a protected way, we designed the research to acknowledge ‘silences’ of people who may be at risk.

Our team were cognizant of the limitations of purposive sampling as a technique, especially when there are certain groups who work at the grassroots level and may not be visible in the mainstream digital rights and digital security ecosystem. Hence, we also employed a snowball sampling technique where we relied on initial interviewees to lead us to individuals from outside of our pool.

The data was collected through semi-structured interviews using video conferencing tools such as Google Meet, Zoom and Big-blue button. Conducting the interviews through these online conferencing tools enabled the researchers to engage with participants from a distance, in different locations and across time zones. The research interviews were also conducted in four languages: English, Russian, French and Spanish. Please see the Annexure for more information on the demographic of our participants, and more detailed information on our research methodology.

an ideal internet

03

- ▼ Access
- Online Safety and Surveillance
- Privacy
- Freedom of Expression



“ [an ideal internet] creates accountability mechanisms which are specific to the intermediary liability of corporations of social media. It may not necessarily be governed by the state because we all know the slippery slope with regulation or securitization frameworks, but feminist driven regulations make the internet safe.
(Participant, South Korea)

When asked to define ideal internets, many of the participants expressed difficulty in coming to a consensus due to the prevalence of violations, surveillance, and censorship that exists on the web today. It is becoming increasingly difficult to imagine a world where these issues are not present and are instead replaced with an environment of trust and safety.

Many rights communities, networks, and practitioners strive to create an ideal internet space. However, **there is no single definition of what this should look like**. Location, needs, and social context must all be taken into account.

Most of our interviewees agreed that an ideal space should be accessible, free, safe and free of violence, private and secure, and inclusive.

It is essential that companies based in the global North do not have excessive control over it. Technology design and implementation must be tailored to fit the complexity of human rights, without making general assumptions and claims to "connect everyone", which lack context.

Regarding power dynamics, participants discussed the importance of reframing the language used to define people. Instead of referring to them as "users," they should be seen as individuals with full engagement in a civic space.

Access

A more nuanced and inclusive understanding of access emerged during our discussions. The gender digital divide was the key theme that emerged from conversations on how social factors influence the digital rights and security community's ability to reach their ideal internet. From access to device ownership to digital literacy, they noted that while access is being pushed from an internet infrastructure point of view, it does not always mean having the necessary resources or freedom to use the internet the way they would like. The participants defined addressing the gender digital divide as unrestricted access, where patriarchal dynamics do not limit how certain groups use the internet. In many countries, spaces that criminalise homosexuality and do not recognise non-binary gender identities make using the internet a tricky endeavour. Even with "access", people may not have the freedom to use the internet in the way they want if their gender or sexual orientation is not recognised or accepted. This can lead to a lack of access to key services, as well as the risk of reprisal and persecution, both online and offline. Therefore, the need to ensure that minoritized communities can use the internet safely, securely and without fear of reprisal or discrimination is paramount.

The participants agreed that the internet should be a safe and secure platform for

everyone, regardless of gender, sexual orientation or identity. They identified a need for increased digital literacy and understanding of digital rights, in addition to necessary resources to help people navigate the internet safely and without fear, as well as to curb the perpetration of negative behaviours that may harm others online. Finally, they called for greater collaboration and understanding between online and offline communities, to ensure that everyone can access and use the internet freely and without fear of reprisal or discrimination.

Urban-rural inequality has a significant impact on accessibility, particularly when it comes to technology infrastructure.

Participants noted that limited access was due to telecommunication monopolies. For example, remote islands, and mountainous regions were typically not serviced by technology infrastructure.

Additionally, affordability and device availability were issues routinely faced. These gaps further exacerbated the lack of engagement with low-income, indigenous, and rural communities. Some also mentioned that children had limited access as well as rights, taking into account potential harms. However, there were also significant gaps in accessibility for the elderly and for persons with disabilities.

“ [an ideal internet] is one that is accessible for people. I know that accessibility is a big problem in this part of the world.
(Participant, Africa)

Access to opportunities and the internet is often a financial issue that may persist due to race, financial class and social status. This gap has been seen especially in communities of colour, where access to resources is disproportionately low. Those without access to the internet and opportunities are left behind and unable to compete in the current economy, leaving them in a continuous cycle of poverty. It is clear that more needs to be done to bridge the gap and provide equitable access to all.

Online Safety and Surveillance

Gendered surveillance within households and communities is an ever-present issue that has far-reaching and devastating consequences for the way people use the internet. Participants in this study noted that access and use can be limited due to religious identity and ethnic background, resulting in censorship and restriction of information. This type of censorship can have a deep and negative impact on an

individual's freedom to use the internet safely and securely, and can even lead to violence in online spaces. It is an essential realisation that gendered surveillance, religious beliefs, and ethnicity can all have an impact on how people access the internet, and these issues must be addressed in order to ensure that individuals are not hindered or harmed due to their gender, religious identity, or ethnic background.

“ **The risks of being online are not evenly distributed. Wealth, age, ethnicity, gender, and sexual orientation all shape digital security risks in Eastern Europe, the Balkans, and Central Asia. It is often women who need to be warned about things like phishing attacks and other things. (Participant, Central Asia)**

The digital divide is a critical factor in understanding the impacts of gendered surveillance, as it can cause users to have different levels of access to the internet based on their socio-economic status. Furthermore, the gender gap in access to digital technology must also be taken into account when examining the issue of gendered surveillance. In order to ensure that all individuals have access to and use the internet

safely and securely, it is necessary to take measures to combat the censorship and violence that can result from gendered surveillance. This includes providing resources to those who may not have access to the same level of technology, and creating policies and practices that address the issue of gendered surveillance in online spaces. Such measures can help to create a safe and secure online environment for everyone.

Privacy

Privacy emerged as a frequent theme in our study. Reflections on the intersection of privacy and security were discussed in depth. Participants agreed that conversations may be end-to-end encrypted, but data stored on servers may be decrypted, thus creating a digital security issue. This raised concern amongst the group about the potential for law enforcement agencies to coerce access to data stored on devices, which could lead to unwanted surveillance and compromise of confidential information. Furthermore, it was noted that there are a variety of methods available to access data, and this in turn could lead to a lack of privacy on the internet. The discussion concluded with a reminder that, while encryption can help protect personal data, it is important to

remember that security and privacy are two sides of the same coin, and both must be addressed in order to ensure a safe and secure digital environment.

For example, in Serbia, public utilities were vulnerable to ransomware, with databases available online until Google indexed them. Data breaches are a significant privacy threat, making personal data and information vulnerable to fraud and states, such as abusing the COVID-19 pandemic to surveil and collect data. CSOs and nonprofits in Central Asia reported lacking the capacity to securely work online and protect sensitive data due to their line of work, showing how security and privacy are interconnected.



I think that they [Privacy and Security] intersect very hugely. I think when we talk about privacy, oftentimes, we also talk about security. For civil society, it's often the synonym for privacy, because privacy is all about what kind of information you have. Who has access to it? What are my rights to this data? How often can I keep it? Do I have a right to be forgotten etc? So much of that depends on good security systems. I think for a lot of people, who talk about privacy, they also mean like, we need to be more secure. So they really do go hand in hand.
(Participant, Asia Pacific).

Freedom of Expression

Most participants defined the ideal Internet as one where freedom of speech and expression thrived without any unreasonable instances of censorship and abuse.

The issue of criminalising internet use is becoming increasingly prevalent across the globe. Participants from various parts of the world shared how states and governments in their respective regions are implementing policies that involve the criminalization of online speech and activities. It is not uncommon for some of these states to also implement censorship measures, which limit access to the internet and thereby restrict the ability to utilise it freely. In some places, such as Ethiopia and Sudan, internet shutdowns have been reported, thus leading to the shrinking of civic spaces. Moreover, participants from Pakistan highlighted that defamation cases and criminal cases have been lodged against people who are vocal about their criticism of the government, often resulting in detentions. All of these examples are indicative of the growing trend of criminalising internet use.

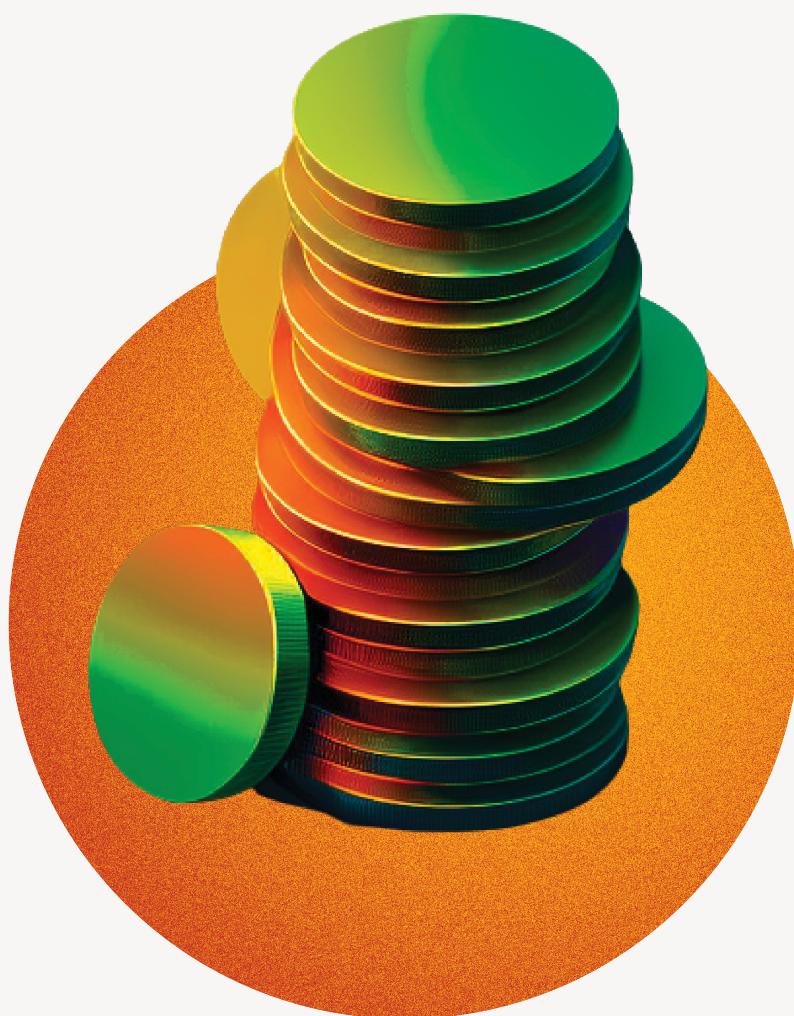
As mentioned above, several participants highlighted instances of bullying, abuse and harassment which complicate the regulation of free speech online. Sexual harassment and abuse are all too common, yet they have been largely overlooked and permitted to persist. Many spaces are unsafe for women and non-binary people, making it difficult to work in such an environment. Consequently, many individuals have had to abandon their work or leave the field due to being harassed, attacked, or abused by people in the field who have not been held to account, oftentimes through coordinated government attacks. In this way free expression is threatened when people leave their line of work within the industry because of the violence they experience. To achieve an ideal internet, according to the participants, freedom of expression will also account for fluid power imbalances between various actors and users online, while centering the protection of marginalised groups.

“ When we had an emergency situation for more than six months when you could not publish anything other than the government’s viewpoint. We have also had an increasing number of prosecutions for libel and defamation. There were cases when people criticising the authorities on Facebook have been detained and questioned. So the situation has gone from bad to worse over the past three, four years. *(Participant, Eastern Europe)*

the funding landscape

- ▼ Roles donors play in determining priorities
Equitable Funding Model

13



We asked the participants about the significance of funding to their work, how it was structured and distributed and what values it represented. Participants reflected on the **role that donors played in determining priorities**, the nature of work and the growth of the digital rights field in their contexts and geographies. In our study, we tried to locate donors and funders and the role played by funding in enabling the participants, their organisations and partners in striving for their vision of the ideal internet.

A participant from Africa highlighted that sustainability funding is critical, but scarce. It is not just the technical infrastructure, servers, and other tools that require support, but also the back office staff such as accountants and human resources personnel. Without the backing of a foundation with resources to build on top of, the sustainability of the movement is put in jeopardy. Consequently, it is essential to secure the necessary resources to ensure that the movement continues to thrive. This includes not only the financial resources but also the human resources that are needed to keep things running. Without both components in place, the sustainability of the movement is in serious doubt.

Equitable funding models are essential for advancing and supporting digital rights and security practitioners and organisations. There is a need to rethink the current bureaucratic models of who gets the money and where they are located. **Trickle-down funding from funders to iNGOs rarely compensates grassroots organisations fairly** for their work. Organisations and networks focusing on feminist internet, sexuality, and gender also rarely receive tech funding. Moreover, organisations and networks that have never been funded before are rarely considered, and eligibility requirements from funders often restrict grassroots groups from the Global South, who might struggle to meet legal requirements such as having to be registered. Funders' uncoordinated goals further contribute to redundancies in who or what gets funded, without much continuity or sustainability.

There is very little emphasis on the part of the funders on the issues of digital security and psycho-social security. For the mental well-being of the at-risk community, the **need for a mental health programs** was articulated. This would need to include capacity-building programs to help people develop long-term sustainability. A participant in Africa pointed out instances of loss of life among the communities they trained due to mistakes. Without a support structure, it remains difficult to discuss these matters and arrive at mitigating strategies for such risks.

localisation & career pathways

15

- ▼ Localisation as a need and a challenge
 - Standardisation
 - Career growth needs



Through interviews and practitioners' profiles, we have tried to document the different pathways that digital rights practitioners go through in their work life in this field. As mentioned earlier, we use narrative analysis to contextualise the career and academic journeys of the interviewees for the practitioner profiles and personas we designed, and provide critical perspectives on the current realities of the digital rights and digital security ecosystem.

The industry pathways and connections are varied. For example, many digital security practitioners are self-taught and become involved due to political issues in their local area. However, these pathways differ depending on the region. Some received formal training and worked in the industry, while others began in feminist activism and explored the link between gender and technology. Yet, others we spoke to started in tourism and moved into human rights and technology advocacy. Some practitioners find it challenging to define themselves, given the lack of clear pathways in the space.

The majority of respondents cited **localisation as both a challenge and a need**. Participants in the digital security space shared how they have been involved in adapting training content to be socially and geographically relevant. This, as most interviewees stated,

also contributes to expanding access to safe and secure internet. Localisation was not only addressed as an issue of language, but also for minoritised communities.

Furthermore, the language of instruction and the predominantly used languages are political and highly colonial. For instance, in Eurasia, most countries were colonised by the Russian empire/Soviet Union, and in Africa and Asia-Pacific some countries were colonised by the British empire, making Russian and English the languages in which content is produced. Additionally, funders are mostly from past colonisers, who set the agendas for the work within the digital justice space. Even though some countries in Africa were colonised by the French, Portuguese or Belgian empires, they remain marginalised in terms of access to information and inclusion. Language politics is also gendered, as gender binaries are argued to be a part of coloniality, thus restricting content, curricula, training, and information within the digital rights and security space.

Digital rights and security is often **too broad a term and lacks a defined scope of work**, which harms practitioners directly and indirectly. This also affects their career growth, as there are no standard protocols for rights groups in security. As a result, practitioners cannot identify clear professional growth in this field. Further, due to limited resources and protocols, rights groups rely on trusted

networks and their own knowledge. As current practitioners phase out or have lower capacity due to age, they are unable to onboard the new generation or provide a clear guiding framework for younger people looking to enter the field.

Currently, there is no standard for people to become practitioners, and everyone comes in with what they have and does what they can. This is not seen as a career worth pursuing, but rather as a placeholder until better opportunities arise. This lack of standardisation and **difficulty in measuring skills, practices, and experience** makes it hard for the field to become more robust and can lead to challenges in ensuring that the training and knowledge shared by practitioners are accurate and effective, rather than endangering trainees.

There is no clear pathway for people to get into the space, and no indicator or checklist to show what is needed to be a digital security trainer. This makes it difficult to advise younger cohorts on what they need to know to work within civil society aimed at digital justice and building an ideal internet. Some participants pointed to a need for more standardisation and a process to measure skills, practices, and experience in this field. However, perspectives also emerged where size, context and funding restrictions can require practitioners to be more innovative

and willing to improvise in ways that may not fit in within a one-size-fits-all standardisation.

Participants from Africa, Latin America, MENA, and Asia discussed standardisation in relation to their careers, while those from Eastern Europe, the Balkans, and Central Asia only mentioned it in relation to internet regulation and protection protocols.

Generational sustainability for Asia and Africa-based participants was another key concern, where they faced intersecting issues of **funding biases, capacity and ability to access certification or up-to-date tools to address advanced threats**. Meanwhile, racial and financial privileges as a result of the participants' location played a major role in their access to career growth plans and certification to advance their skills and knowledge in the industry. Participants with such racial and locational privileges acknowledged that their social positionality was a significant influence.

Other career growth needs mentioned included providing spaces and opportunities for senior-level practitioners to grow and making it easier for people in the early stages of their careers to transition or work within the digital rights and security space, with less gatekeeping.

conclusion

The work and imaginations of digital rights and security defenders and practitioners has thus far been significant to the advancement of public interest technologies, regulations and standards. However, practitioners continue to experience significant challenges layered within socio-political intersections that affect how much progress they are able to achieve or measure said impact.

With the findings from this research, we hope that the report informs strategies that may support digital rights defenders' progress on advancing their vision of an ideal digital space as well as their professional well-being and growth.

annexure

Methodology

Sampling and Data Collection

The research was conducted through a qualitative study, with 56 participants from Central Asia, Eastern Europe, Balkans, Asia Pacific, Africa and the MENA region.

We employed a purposive sampling technique to reach out to key digital rights and digital security practitioners, activists, organisations, trainers and institutions. Our selection criteria was based on:

Are they a digital security or digital rights practitioner?
Are they representing a civil society organisation?
Are they an independent practitioner?
Do they represent a research body or an international NGO?
How do they work on one or more of our five thematic areas i.e. access and inclusion, digital safety, security and protection, data Governance, freedom of expression, communication and information, and privacy, anonymity and identification.
Are they from or work within Africa, MENA, Balkans, Asia-Pacific, Eastern Europe or Central Asia?

Finally to ensure our data was representative of different genders, we also attempted to create a gender distribution of cis-gendered men, cis-gendered women, non-binary people, and transgender individuals. However, given that most people who are transgender or non-binary gender category may operate and work in a protected space, we designed the research to acknowledge 'silences' of people who may be at-risk.

Purposive sampling as a technique may be limiting, especially when there are certain groups who work at the grassroots level and may not be visible in the mainstream digital rights and digital security ecosystem. Hence, we also employed a snowball sampling technique where we relied on initial interviewees to recommend other individuals within the sector to take part in the study.

The Data Analysis Process

Data from each interview was analysed using a thematic and narrative analysis method. Given that this is a research conducted across different locations, the participants' demographics have been disaggregated based on the regions, gender, age range and their work focus i.e. between digital rights and digital security. The goal was to inform our assessment of who was in the space, their work and how long they have worked within digital rights and security

A thematic analysis allowed the researchers to draw out the key themes from the overall research. Thematic analysis is mostly used to assess user experience or research that is studying the experiences of a certain population on a certain product or ecosystem. While this research examines the experiences of digital rights and digital security practitioners and aims to design interventions to support the space, we primarily employed a thematic assessment to identify “who is in

the space”. What this means is that, the thematic analysis was used to draw out patterns on the professional and academic journeys of the interviews to put together the key persona’s in the space. These persona’s are documented in the form of practitioner profiles. The thematic analysis provided insight on the careers and pathways of several practitioners within the space. However, a narrative analysis enabled the researchers to assess the stories and narratives of the interviewees to understand their individual experiences in relation to our research goal. The narrative analysis was used throughout the report to craft arguments and provide critical perspectives on the current realities of the digital rights and digital security ecosystem.

Meanwhile, it is through the narrative analysis we were able to contextualise the career and academic journeys of the interviewees for the practitioner profiles and personas we designed.

Our Community-Based and Participatory Approach

The research was designed to employ a participatory and community-based approach. In a typical participatory action research (PAR), the researcher hands over the research processes to the partners (who would be referred to as participants in a non-participatory study). Meanwhile, in a community-based research, the process is mutually beneficial. In both cases, the research partners are able to directly benefit from the outcome and process of the study.

While our study relied on PAR to govern the design, the researchers had to rethink what “participatory” looked like for this research. Our consideration took into account the scale, the remote logistics and organisation of the research. So “handing over control” of the process was not feasible in this case.

On the other hand, throughout the design and implementation processes we engaged selected community members, who played a role as our Advisory Board. Their feedback and recommendations were integral to the entire process, which was reiterative and collaborative through brainstorming on best methodological approaches, questions and including the writing of the final report. In addition, the research’s goal was framed to ensure that the partners who engaged would gain a direct benefit from this study. Thus, the researchers’ and advisory board members’ intentional design to ensure that the key outcome of the study informs interventions, recommendations and products needed to advance the digital rights and security ecosystem. The research also ensures this by engaging research partners during interviews on questions such as “participants what they would like to learn from this research and/ or how the research can inform changes in the ecosystem”.

Ethical Considerations and Limitations of the Current Study

One of the major ethical considerations for the research related to questions around how we can implement a semi-participatory research within a niche community while ensuring confidentiality and protecting people who might be at any type of risk due to their narratives in this research. Risk here also means groups of people who might be antagonised based on their criticisms of the digital rights and security ecosystem.

In addition, we began this study through a literature review in the form of an annotated bibliography, and organisational mapping. However, through conversations with our advisory board members, a few pointed out that while our intention to put together a database of organisations in the space may be positive, having a public database of this nature may allow for malicious targeting of some of the organisations mapped. Also, some organisations may not want to be visible in the way the database allows. Hence, the researchers are considering alternative processes to make sure our resource database is better secured.

Limitations

The key limitation of this study is that it is mostly representative of civil society organisations, actors, activists and digital security individuals who are either in their mid-career or are senior professionals and may not adequately reflect the voice of practitioners who are just starting out or are new to the space.

The data in most of the regions is made of cis-gendered men although our initial goal was to capture the experiences of minoritized groups. Meanwhile, the research demonstrates that the space is mostly made up of cis-gendered white men, or cis-gendered men from a more privileged background within their respective locations. Hence, the question we continue to reflect on throughout this study is: If our goal is to represent the realities of the digital rights and security ecosystem, and our data in itself show the stark gendered inequalities within the ecosystem, do we take an intentional step to reach people of genders whose experiences have not been represented? More importantly what perspective would a study on the digital rights ecosystem which only focuses on minoritized genders provide us? And how can we complement this initial study through such an impactful focus?