Private Tech Sector Engagement with Global Civil Society

Internews

November **2022**

Table of Contents

I. Research Framework

A. Problem Statement

There are serious shortcomings in the current engagement and consultation practices between the private tech sector and civil society stakeholders and on a global scale. Nonetheless, there is very limited research on current practices of civil society's relationships with the private tech sector and their challenges, needs, and perspectives for successful engagement. This research addresses this gap and serves as a foundation for the work that organizations carry out on this issue over the medium term.

B. Research Questions

- How can private sector technology companies engage in a more productive relationship with civil society? What are the current engagement practices of civil society stakeholders with the private tech sector?

- What are the main challenges for civil society in its engagement with the private sector in terms of access, compensation, confidentiality, language, feedback loops, and more? What are the needs and preferences of civil society to result in positive outcomes?

- What role(s)) can civil society play in shaping industry standards that better align a profit motive with rights-based values and approaches??

- What are the recommendations for impactful next steps to build on this research project and its findings??

- What sorts of approaches have been recommended or implemented for civil society to respond to rapid changes and adapt for the future to avoid further exclusion?

C. Hypothesis

Effective partnerships with the private sector must be based on shared values, best practices, and a solid understanding of risks and benefits. A productive engagement of civil society with private sector technology companies can help to shape and produce improved and adequate business principles.

D. Research Methods

The research employed a qualitative approach using mixed-methods including in-depth interviews, participant observation, and the gathering of pertinent studies and reports.

The interviews consisted of semi-structured conversations with 30 experts from civil society organizations, community representatives, and academia across 24 countries, held between the months of November 2021 and May 2022.

The experts were selected to carry out the qualitative interviews based on 1. their professional background in and knowledge of digital rights in each country; 2. their activism on digital rights; and 3. the sociopolitical relevance and background of each country, to provide a diversity of contexts. While 31 interviews were conducted across 24 countries, only 15 are discussed in this report based on the suitability of the data and the safety of the interviewees. The selected countries are Belarus, Brazil, Colombia, Ethiopia, India, Iran, Lebanon, Myanmar, Pakistan, Palestine, Paraguay, Russia, South Sudan, Sri Lanka, and Taiwan.

A review of the existing literature on a variety of disciplines debating the subject of the tech sector was implemented to provide a basis for the analysis of the empirical data and participant observations.

While the sample size is relatively small considering the global scope of the project, and despite the limited time and resources available, common trends found across the data stemming from different regions can serve as grounds for further research on this topic.

Triangulation was used to analyze the data from the different data sources and collection methods.

E. Conceptual Considerations and Terminologies

Based on interviews, the term "engagement" is not a commonly used phrase in languages other than English; "communication" and "partnerships" are more often referenced. For the purpose of this study, the term "engagement" refers to the different types of communication (e.g., channels to report harmful content or wrongful takedowns); relationships (short-term and long-term partnerships); and consultations (periodic or one-off consultations).

By "private sector," the study refers to a relatively small number of companies that include the big techs, non-social-media platforms (e.g., PayPal, Google Maps); and national telecoms. The terms "civil society," "civil society organizations," and "nonprofit organizations" are used interchangeably to denote academics, activists, advocacy groups, cultural institutions, and professional associations that are not associated with governments or the private sector.

F. Limitations of Research

- People living in rural communities may access and use technology differently from their urban counterparts.

- Civil society organizations that are part of the trusted partners program, and/or have direct established access to the private tech sector, have a different narrative from those outside of these spaces. Therefore, assumptions will be based on the status of the organization included in the interview process.

- Discourses on content moderation or engagement with the private sector are often limited to the "elite" and not inclusive of everyone.

- While 30 interviews were conducted in 24 countries, not all were conclusive or provided sufficient insights. As a result, only 15 countries are represented in this research.

- Due to both safety considerations and lack of availability, certain interviews could not take place. Each interview was also limited to an hour, and not all questions could be answered.

- A deeper study is needed to take into account the intersections of race, ethnicity, gender, and religion in each geographical context.

II. Research Findings

A. Executive Summary

Private tech sector engagement with civil society across the globe has been inadequate, inconsistent and often lacking appropriate practices. While companies have strong relationships in certain countries, they have minimal to no presence in others, with investment seemingly based on market size and coverage in mainstream media rather than objective needs. Rather than being people-centered and locally driven, current engagement practices have been led by the business models of private companies distant from local needs, interests, capacities, and dynamics. Effective transformation requires a systemic framework of industry standards for collaboration using an integrated and intersectional approach based on a deeper understanding of the distinctive nature of technology's roles in local communities and contexts. This is particularly true in fragile and conflict settings where the harms of technology are magnified and vulnerable minorities are under greater threat.

A single approach to engagement thus cannot be applied uniformly across all countries and population groups. The nuances of working in diverse geopolitical, economic, and cultural contexts, including the associated risks and opportunities for different communities, need to be incorporated systematically into the processes carried out by businesses. Language is also a determinant in the type of relationship established with the private sector. While vast portions of user activity on major online platforms take place in non-English languages, the majority of engagement occurs in English, which excludes many grassroots organizations operating in local languages.

Current levels and practices of engagement used by civil society organizations are often bound to their institutional networks and their relationships with specific professionals at the companies.

If the individual leaves their position, the partnership with the business is directly impacted and generally terminated. Creating meaningful relationships with the private sector is also determined by the international exposure of organizations and their attendance at major global digital rights events. Those privileged to be included in the trusted partners circle are able to create and strengthen stronger partnerships and gain direct access to the different teams of the businesses. They have increased awareness of the internal structure of the companies and processes to follow to influence change—albeit minor—related to their products, tools, and policies. The undisclosed selection process of admitting civil society organizations into the trusted programs has meant that many experts are excluded from access to information and engagement with companies, resulting in high risks of tokenism and division among organizations in a given country. While trusted partners often serve as a connector to businesses, they cannot represent the needs and interests of all organizations. Fear of losing their status and the resources received from the companies has resulted in a common narrative being adopted by many trusted partners across the globe.

Nonetheless, engagement in certain regions has evolved over the years from yearly meetings to more frequent and often one-on-one convenings, particularly with Meta. Consultations with civil society experts on products, services, and policies have yielded some changes, although minor and on a case-by-case basis rather than in a substantial manner. For change to be sustainable and meaningful, it needs to happen at a systemic level. However, the power imbalance between tech giants and civil society raises questions around the capacity for both to engage in partnerships that are equal and transformative, yielding changes and opportunities that benefit all stakeholders. Finally, unequal relationships pose a great risk to further digital colonialism and exacerbate existing global inequalities.

These systemic inadequacies of tech industry engagement with civil society have significantly contributed to and exacerbated a profound trust deficit. While civil society representatives have expressed enormous frustration with tech companies, the need to engage constructively with industry to improve products and mitigate harms is keenly felt. Overwhelmingly civil society is eager to deepen these relationships through more structured, consistent and contextually appropriate engagement. A shared framework of industry standards around such engagement would significantly advance this process.

B. Common Findings

While each country included in this study presented unique circumstances and challenges there were a number of consistent findings when it came to engagement between global technology companies and national or locally focused civil society.

Company engagement is consistently inconsistent

To date, efforts led by private tech companies to establish transformative partnerships with civil society have been uneven and intermittent. Providing services to millions of users in countries without often having a physical presence or a good understanding of the context, and while failing to include diverse communities in the conversation and decisions that profoundly impact their livelihoods and security, has had a direct impact on the established trust of users and the sustainability of the initiatives. Companies have invested in engagement with civil society according to their own internal priorities, often with seemingly little interest in proactively understanding the concerns and priorities of even those they are consulting with, let alone underrepresented communities.

Engagement too often relies on ad-hoc personal networks, leaving it vulnerable to changes in personnel. Detailed feedback or ongoing processes are rarely provided. Moreover, addressing each issue separately without using an integrated and coordinated model has resulted in ad hoc interventions and limited results.

One thing that is consistent across countries included in this study is that the companies' lack of consistent approach, clear strategy, or industry standards have left civil society feeling frustrated, angry, confused and mistrustful.

Engagement proportional to market size and media coverage

The ad hoc engagement of the private sector with civil society across the globe has meant that partnerships vary on a country-by-country basis. While the companies can have strong relationships in one country, they may have minimal engagement with another, often contributing to unrestrained hate speech, spread of disinformation, a rise in violence, and in some cases genocide among other outcomes. The disproportionate attention provided to a country has been linked to market size. Weaker economies generally remain outside of the priorities of social media platforms. Smaller countries with populations who do not speak European languages are the most heavily impacted, often despite being home to millions of users of tech company services.

Global media coverage exposing the role of tech companies in inciting and intensifying violence in a particular country—such as the case of Myanmar— with high financial losses has also led to a shift in engagement. With their reputations at stake, companies have changed course with increasing public pressure, taking significant measures for damage control and multiplying their investment in the affected regions. Nonetheless, the changing approach to engagement is linked to the magnitude of the attention of global media rather than directly to the impact of the technology deployed (e.g., the case of Myanmar as opposed to the conflict in Ethiopia).

Civil society groups are keenly aware of this hierarchy of attention, which in turn has a further negative impact on their relationships with the companies.

Engagement largely carried out in English

Beyond digital divides, English speakers have more opportunities to engage than non-English speakers, particularly those who communicate in local languages. Although the platforms are multilingual, there are significant inequalities in the services, products, and tools made available in languages other than English. Many of the meetings convened with the platforms, particularly those at the global level (such as consultations, roundtable discussions, and advisory roles) are often English only.

Additionally, the two largest digital rights global events, IGF and RightsCon, where many of the strong relationships are established between civil society organizations and private companies, are limited to English. Access to the conferences—generally held in person—is yet another barrier and is only made available to those with adequate financial means and exposure, leaving out many grassroots organizations who operate in non-English languages.

Tokenism and access to companies

While the impact of technology affects all civil society organizations, particularly grassroots communities, engagement with companies is limited only to a few such organizations.

The trusted partners, an informal network of consultants—albeit without compensation—to private tech companies, have privileged access to the platforms. On the other hand, the selection process creates tokenism and a division between those who have direct access and those who are left out. No transparency or structure is made available showing how members of civil society are approached by the tech sector.

Trusted partners may strive to hold on to their status to ensure they maintain the engagement and access to resources and support while often avoiding taking any antagonistic action toward the companies, creating a dichotomy between their mission and the platforms' policies and practices. As a result, a common discourse is often shared among some of the selected organizations across different countries.

Outsourcing responsibilities

Faced with the rapid growth in technology and its associated impact, civil society has had to adapt accordingly with limited resources and knowledge while struggling to mitigate the harms. Attempting to communicate with companies and report the adverse consequences of the deployment of the companies' products has become yet another burden. As such, civil society organizations have been fulfilling the responsibilities of the private sector while struggling with funding, time, and other resources. Rather than addressing the adverse consequences of the deployment of their technologies, the platforms rely on the work carried out by civil society, who most often do not receive any form of compensation for their expertise.

State surveillance and other threats

Government surveillance has played a significant role in the engagement of civil society with the private sector, particularly under authoritarian regimes struggling with accountability around government practices on their use of platforms for civil surveillance. Heavy state surveillance often results in government requests for companies to take down content under false charges of inciting violence, terrorism, or hate speech. A uniform approach—global compliance guidelines and content policies—cannot be applied to all countries, and can often lead to increased surveillance.

Civil society are themselves frequently targets of state surveillance, as well as other forms of intimidation, harassment, threats and violence from both state and non-state actors. The countries where these threats are most serious are also likely to be contexts where tech companies are most reliant on context experts and civil society to help them understand and mitigate the impacts of their products. Without clear safety protocols and established trust such engagement is likely to put civil society at increased risk.

Lack of context-specific information

While the most powerful tech companies are global, they are not based in the countries where the large majority of their users live, creating a physical, linguistic, and cultural disconnect with the local context. Social platforms in particular see the world as if it were one and the same, rarely taking into account the nuances and complexities of implementing their products and services in fragile contexts including regions in conflict and under authoritarian regimes. Countries with poor data access and limited research facilities are at an even greater disadvantage.

These gaps contribute to the lack of understanding and information generated about the users' communities and trends in their use of technology, and impede effective engagement with private companies.

Current challenges clearly call for a deeper understanding of the dynamics of technology and users; however, access to relevant data is limited. The asymmetry of data ownership and access inhibits the advancement of scholarship on these issues and widens the gap in research. Increased transparency of tech companies and collaborative relationships with civil society—particularly investing in local research organizations and institutions—would enable researchers to address this need with contextualized information.

Meta — more engaged but no meaningful changes

Across all countries who took part in this study, Meta was found to be the platform most engaged with civil society organizations. In many regions, its engagement has evolved from yearly meetings to more intimate and often one-on-one encounters both at the national level and at its headquarters. Compared to other platforms, Meta was reported to be more present, available, responsive to queries, collaborative, and open to ideas, and more likely to attend civil society events and hold sessions on how to monitor social media. The reporting process is generally more efficient and changes—albeit minor—to its products and policies do take place based on feedback provided by organizations.

Nonetheless, the changes occur on individual cases rather than at the systemic level. Given some of the civil society organizations' dependence on resources received from Meta, they often refrain from taking any action that may put their relationships at stake. Additionally, trusted partners hold on to the current form of engagement as their only means of communication with the big tech companies and as representatives of other civil society organizations.

Journalism and civic space controlled by global platforms

Civic space has increasingly been controlled by tech companies. Online civic activity is often monitored, appropriated, and controlled by the business models of the private sector. Journalism and civil society organizations rely on centralized technologies to continue their work, both in terms of online space and the resources they receive from the companies. This dependance directly impacts their approaches to engagement. Large technology companies define the structure of the entire digital media ecosystem, including what it means for the development of the production and circulation of news, the safety of journalists and media activists, and how and what content stays up or is taken down.

Enforcement of laws on international companies

Internet platforms are facing unprecedented pressure to comply with national laws and regulations to monitor the content posted on their services. Although the major platforms operate globally, US companies are bound by US laws, rendering the enforcement of policies challenging and blurring the definitions that guide the decisions of the companies (e.g., what defines dangerous organizations, terrorism, transparency, etc.).

The enforcement of national laws on international platforms requires the company to be formally registered in a given country. In the absence of national laws on content policies, global compliance guidelines cannot be uniformly applied across all countries, particularly in those under authoritarian regimes.

Beyond social media platforms

While most of the engagement and online challenges faced by users across the globe revolve around Facebook, communities such as Palestinians in the occupied territories struggle with other platforms including PayPal and Google Maps. PayPal has been denying service to Palestinians in Gaza and the West Bank, while full access to the company's products was granted to Israeli settlers. It is not the first time that the platform has refused to cater to vulnerable groups. Unfortunately, PayPal is one of many other US companies to ban entire groups and regions on premises relating to terrorism and sanctions. Google Maps, on the other hand, is solely led by political biases and refuses to label Palestine on its mapping service, even following global outrage and condemnation by civil society and strenuous campaigns by Palestinian and international organizations.

C. Qualitative Interviews

1. Belarus

Belarus has a well-developed ICT infrastructure with Internet connectivity rates increasing in recent times. With one of the highest fixed and mobile penetration rates within the Commonwealth of Independent States (CIS), 8.9 million out of the 9.4 million population have access to the Internet. However, Internet freedom has been under threat and declined dramatically following a series of mass political demonstrations and protests against the Belarusian government that followed the 2020 presidential elections. A government-led campaign of repression resulted in the arrest of over 500 journalists, media activists, bloggers, and online activists, who were subject to beatings and torture. The social media activity of activists and journalists has been heavily monitored, including their conversations on messaging applications. Connection speed was heavily impacted by a government Internet shutdown implemented as a response to the pro-democracy movements.

Belarus has a number of laws that allow the government to extend control over individuals and civil society. While not mentioning the Internet specifically, Article 13 of the Law on States of Emergency limits the freedom of the press and mass media through a presidential decree. In 2018, amendments were made to the law to include online platforms, granting the government the power to block websites deemed to be a threat to national security. These changes complement the existing Interagency Committee on Information Security that assesses "the intense buildup of dangerous trends in the global and national information space." To further limit speech, the government revised the Telecommunications Law in 2021, allowing it to shut down or limit telecommunications operations if deemed a threat to national security. Shortly after, the government raided the media company TUT.by and arrested its employees, including those at Hoster.by, a holding of the company.

Media markets are strongly regulated by the Belarusian state, with no independent regulator overseeing the ICT sector . In addition, the Presidential Administration's Operations and Analysis Center (OAC), which was initially a subdivision of the KGB, has the authority to oversee ISPs and control standards for information security, conduct online surveillance, and manage the country's top-level domains. As reported by the Belarussian Association of Journalists, following a presidential decree in 2019, the OAC was granted additional power over information security and now operates as a state-controlled center to respond to Internet-related issues. Other national surveillance bodies include the State Telecommunications Inspectorate, the State Security Committee, the KGB, and the Prosecutor General's Office. A participant in this research explained that heavy monitoring of online activity also requires all individuals to register with their passport when purchasing a SIM card or data packages.

For people to connect to the Internet, they need to be registered. So if you buy a SIM card for your phone, you need to show your passport and they have a photo of you. To get a contract for your Wi-Fi, you need to show your ID, and when you use public Wi-Fi, you need to provide your information.

State surveillance intensified particularly during the 2020 Internet shutdown, with the authorities taking down any civil society platform considered to contain any information critical of the government. Other platforms such as Telegram channels labeled as "extremist" were blocked. Amendments to the Media Law in 2021 placed even more restrictions on the free flow of information, banning live, on-the-scene reporting and increasing the number of state officials with the authority to block access to online material and reject the accreditation of journalists. The participant stressed that any political speech has been labeled as extremist and harmful content, restricting the work of activists and putting their lives at great risk:

Right now, harmful content is a very popular topic in Belarus and is often related to anti-extremism, but now in Belarus, just sharing independent media is considered to be extremist media. So right now, if any people are sharing any information from those channels, they are also accused of spreading extremism. Just political speech is considered to be extremism; there's lots of laws in Belarus related to political speech.

Forced confessions and defamation on online platforms have been among other tactics used by the government to silence human rights defenders. Videos of the false statements are frequently shared on social media, including the state's YouTube channel. The company's responses were limited, even after numerous attempts by civil society to remove the content:

It's a widespread practice [that] when [the] police arrest activists, they force them to record a video with some confessions, not only with activists but also with [other] arrested people. The head of communications with A1 Belarus … was forced to record a video that he was gay. They release several videos every day on YouTube. They have their YouTube channel. They put those videos as advertisements, so Google advertises videos with captured people who are confessing that they were captured and they participated in some opposition events. After several complaints, some of those advertisements were stopped by Google, though those YouTube videos are still active.

Engagement with tech platforms has been especially challenging when it comes to content moderation. The lack of systemic communication means that civil society has no knowledge of how to access support at tech companies or transparency on moderation processes. The absence of context-specific services such as moderation in Belarusian has furthered the limitations on civil society, in particular when trying to advertise on social platforms:

When you're trying to advertise anything in Belarussian, it's impossible as Google says they have no moderators who can check things in Belarussian. They can do it in Russian but not in Belarussian. When the government puts up videos of people who have been captured, it's always in Russian as it's one of the official languages of Belarus.

The participant in the interview explained that Belarus does not receive the same level of attention from private tech companies as other countries of a similar market size. Companies are often staffed with professionals who are physically, linguistically, and culturally distant from the country in which their users are located, widening the existing disconnect with civil society:

In Belarus we have a number of issues [that] are specific only to Belarus. Smaller countries such as Belarus should be given greater attention from the bigger tech companies despite the fact that they might be a smaller player within the market.

We need some global or regional platforms to [show] how to understand more about their practices and to influence their practices, we need to have more transparency to understand those processes.

Given the poor engagement with social media platforms, the participant reported that civil society usually relies on a third party, Access Now Helpline, to access support. This tactic—deemed as the most efficient approach and with a two-hour turnaround time—is frequently used to block the accounts of detained and arrested human rights defenders, often for their safety and at the request of family members:

With Facebook, we mostly try to block accounts of detained and arrested people, so just for their security, when we are called by relatives of those people, they ask us to close the account, they will give the passwords, so usually, with Facebook we ask the Access Now helpline.

We gather information, for example about a human rights defender who was arrested, and we reach out to Access Now who have some direct communication with the Facebook team, and within two hours they can block the account. When the person is released, they can unblock the account. We also do this with Google and YouTube.

As is often the case in many countries, civil society representatives in Belarus are unaware of the internal structure and engagement procedure of private tech companies. The interviewee states that companies cannot continue to operate in countries without having a physical presence and adept professionals to support the work of civil society and mitigate the harms caused by their technology:

We are not sure where the nearest offices for Google are—some people think that they are in Moscow, some think that they are in Warsaw—we don't have clear communication with them. Before the previous year, we didn't really need that contact. There was a petition [sent] to Google and some other media companies to treat Belarus as a separate market from Russia. So for example, when Russia runs their Google news, even about Belarusian events, they provide links to Russian media rather than Belarusian media.

The lack of a systemic framework of communication furthers the existing challenges that human rights defenders face with the heavy state surveillance and restricted freedom of speech in Belarus. Greater transparency is not only necessary to establish transformative partnerships but also to safeguard the security of human rights defenders under the Belarusian authoritarian regime.

Moving forward

- Staff tech companies with moderators who are fluent in Belarussian and knowledgeable of the local context in Belarus.

- Offer greater transparency on content moderation processes: who moderates content in Belarus and how content is assessed.

- Disassociate content moderation processes from government relations and regulation.

- Provide civil society with information on ways to safely access the support teams of big tech companies and the most efficient ways to report content and make urgent requests.

- Ensure that the same support teams and access to services are available in Belarus as they are in other countries.

2. Brazil

In the run-up to the 2022 presidential elections in Brazil, heated debates made headlines over politicians' attempts to bar social media platforms' abilities to moderate content. In 2021, President Jair Bolsonaro signed a provisional measure amending the Brazilian Internet Legal Framework —which regulates the use of the Internet in Brazil —that would prohibit tech companies from removing content without a court order. The types of content covered include misinformation about COVID-19 and the lead-up to the October 2022 elections. While Congress turned down the decree, the president claimed it to be an effort to defend free speech on social platforms.

In fear of repeating the rampant election-specific disinformation that preceded Bolsonaro's victory in 2018, many Brazilian lawmakers and civil society leaders attempted to influence policy proposals to dramatically reshape the information ecosystem on social media as the country geared up for a major election. The patterns of misinformation spread in Brazil are unique to the ways Brazilians connect with each other, build trust, and form communities. Rather than stemming from content from individuals or competing groups, misinformation in Brazil largely disseminates between family members and between groups that agree with each other. The vast majority of false information shared in the wake of the 2018 elections was shared on WhatsApp in group chats that favored the far-right leader. Much of the COVID-related misinformation, for instance, was created and shared between family members. The dynamics of misinformation on Twitter in Brazil are also distinct, according to a local activist:

> *Twitter is the most different platform, because it allows many groups to discuss the same topic at the same time to reach the top of the tweets. But they are two groups of problems: 1. The people who have the verified symbol: there is no transparency on how Twitter selects these users; and 2. Many of those who spread misinformation in Brazil have this symbol on their profile, so no further verification is ever done.*

The moderation of content is also unique to the local context, in the same way that the violations on these platforms in Brazil are distinct. For instance, racism online presents a major moderation challenge, particularly when civilians attempt to report the harms. Neither the company's moderators or automated tools are equipped with the cultural and linguistic knowledge to detect what is harmful and is considered racist in the Brazilian context:

When racism occurs on platforms, we face many issues with content moderation; most moderators are from the US (with the mindset from the US), which is distinct from other countries. Language is also another barrier: how Black people in Brazil are referred to, what would be considered racist, etc. For example, a Congolese immigrant was killed in Rio on January 24th as he was collecting payment. On platforms, the story impacted Black people because many racist memes, images, and videos were posted on platforms. Black influencers also faced many issues with hate speech on their content coming from racist people.

There is an overall lack of systemic communication between civil society and tech platforms in Brazil. Telegram, for instance, was banned by the Brazilian Supreme Court after it continually failed to engage and respond to the rampant disinformation on its platform. The company has no office in Brazil and its hands-off approach has been particularly popular with right-wing users. While some companies do have a team presence in Brazil and attempt to communicate with human rights defenders, the final decision-making takes place at their headquarters, leaving the engagement at a superficial level, without any significant result:

Platforms do not want to hear that they are failing. Recently, a group of Black researchers were called to engage in a conversation with Twitter on racism on platforms; [none of Twitter's team had] responses and said that they needed to get responses from headquarters; so they need authorization and we cannot go deeper in the conversations.

According to the interviewee, Twitter has been the most difficult platform to engage with. The company has often dismissed reports of harmful content, particularly content related to online racism, citing freedom of expression. Many of the engagements generated a conclusion that racism is a matter of opinion. Additionally, the limited categories available in its reporting system, without distinctions based on race or religious orientation—all fall under hate speech—has fostered further hate and a dangerous ecosystem for many vulnerable groups. Deep fakes and images on a variety platforms including YouTube, TikTok, and Instagram have targeted public figures from Black and transgender communities to delegitimize their authority and work:

Deputy Benny Briolli, the first Black transgender councilwoman of the City of Niteroi, had to leave the country because of threats, and when she came back to Brazil, she received the same threats on [Instagram] and through emails. They used her posts to distort the message, including caricatures, memes, and videos.

According to the interviewee, the lack of an intersectional lens and specific categories in the reporting system of tech platforms poses yet another challenge for civil society. While YouTube has a hateful content category in their reporting system, many posts fall under disinformation and often go undetected.

Instagram has recently taken a more rigorous approach to reporting harmful content in Brazil, nonetheless, civil society experts pointed out that it was more probable to receive a favorable response if the content fell under misinformation. TikTok, on the other hand, classifies hate speech in specific categories, enabling a much simpler process of engaging with its platform. As a strategic approach to some of these limitations, civil society uses mass influence to obtain a response from companies. In addition to reporting to the social platforms through their traditional channels, activists share the content and user profiles with others in their circle for them to report as well and put pressure on the companies.

Polarizing posts generate more user engagement and therefore time-on-platform, and have presented a particular challenge for civil society to communicate with companies. From TikTok to Instagram to Twitter, most users in Brazil who have spread misinformation and caused further polarization have verified accounts, sidestepping any content moderation or profile filtering. The participant pointed out that the absence of a government or independent institution dedicated to a healthy Internet ecosystem in Brazil benefits the private sector, while there is no mechanism to keep the platforms accountable. As a result, civil society has had to compromise to be able to engage with companies and receive financial support to carry out its advocacy.

The need for greater transparency from social media platforms is unfortunately not limited to Brazil. The participant explained that while Brazil represents a substantial market in the number of users, the private tech sector does not maintain the same level of accountability and level of transparency there as in countries in the Global North. Civil society organizations have tried to circumvent this challenge and gain more knowledge on the operations of social media platforms in the country. When companies reach out to civil society to fill an advisory position on their board, organizations advocate to appoint an expert from their team. In exchange, they are granted access to "insider" information on the structure and operations of the companies.

It is worth noting that the engagement with private companies increased during some periods of the pandemic. Social media platforms sought organizations to donate to and to promote further donations for poor communities and even fight health-related misinformation.

The participant emphasized that policymakers' limited understanding of the Internet has led to poor public policies for increased accountability and transparency. While policies exist to address violence toward vulnerable groups, the lack of policies and enforcement of online crimes has impeded an efficient reporting system of harmful content and weakened transformative engagement with private companies.

Moving forward

- Offer more transparency on the internal structures and procedures of operation of Brazilian offices (where applicable).

- Employ dedicated country focussed staff with revelevent cultural, contextual and linguistic expertise.

- Adapt products and services to the reality and needs of each country.

- Provide transparency over what data is shared in each country by each platform, which products are offered and used, and what the process and impact per country.

- Include local experts in the design and decision-making process of each policy, product, and service that is meant to serve local users before they become a problem.

- Generate in-depth research that is intersectional to map out data based on race, ethnicity, and gender, especially in health-related data (but how to proceed in a country that lacks data?).

- Build a coalition of civil society organizations, particularly in the Global South, that can support each other, particularly those living under authoritarian regimes (e.g., Twitter messages and posts during the Arab Spring).

3. Colombia

A divided Colombia gearing up for the 2022 presidential elections faced unprecedented political polarization, with the potential for a left-wing candidate to win for the first time in history. Misinformation ramped up on social platforms and there were personal cyber attacks against members of all parties, in particular against Francia Márquez, the Afro-Colombian human rights defender and vice-presidential candidate.

An absence of settled rules for data governance in Colombia has left platforms without any legal responsibility for the content they host. Nevertheless, several bills have been introduced and are under discussion in Parliament.

Colombia made international headlines in 2021 when national anti-government demonstrations were held in various cities in the country. The military was deployed throughout Colombia to silence the movements, increasing the violence toward civilians that resulted in many injuries and lives lost. Many human rights activists denounced violence toward journalists and the censorship of the protests on social media platforms, a direct reflection of the growing government repression. Attacks on protesters and the systematic censorship of human rights defenders and the press have been a frequent practice in Colombia from the early days of the Colombian conflict. Activists have also been attacked and threatened online with hate content, and were labeled as terrorists and delinquents. Government authorities attempted to distort the claims of hate speech toward activists in their favor by appealing to social media platforms to block certain accounts and content, alleging they shared hate speech targeted toward police forces.

Given the protracted political war in Colombia, the nature of the work of civil society organizations has largely been political. Their advocacy endeavors, both on social platforms and offline, have been crucial in disrupting the historical inequality that gave rise to the armed conflict in Colombia and in ensuring a fair democratic process during elections. Nonetheless, they have seen their content taken down if they discuss any political issues, an interviewee explained:

Despite the fact that we are registered as human rights organizations and that our role is purely political, our posts cannot include the word "politics." If we talk about elections, there is a blockage and we have to find a way to be able to post this information. There is a special Facebook feature that detects that, and blocks your account for 48 hours, during which you have a review process.

Using their tactical creativity, activists have found ways to circumvent the indiscriminate moderation of political content on social media. If their posts are taken down, they fall back on their alternative plan. By using different wording in an already prepared second post while the original content is deleted, they avoid platforms' political restrictions and the complex and long review process. This strategy enables them to continue their advocacy and avoid losing time and momentum during critical periods. The participants in the interview explained that this approach was simpler for civil society organizations to adopt in lieu of attempting to engage with private platforms:

They offer tips between each other to avoid the restrictions, so they have become experts in that. They have different versions of the same message, using different words in each copy. They say that it is easier to do so, instead of waiting to get a response from Facebook and trying to communicate with them. That way, they can continue to cover the elections.

Another unique approach to increase engagement and get the attention of the platforms is to buy advertising. The participants explained that the success of efforts of organizations to report a blocked account, harmful content, or any related issue is connected to the quantity of advertising purchased. The continuity of their work is conditional on how much advertising space has been acquired:

The engagement and entire relationship between organizations and platforms is based on this advertising system, from the prioritization of their requests to the rules on content moderation they have to circumvent. If you don't buy ads, you are not seen. It's like an algorithm that exists: if you pay, you are seen and get more attention. It's like a distinct channel of attention that they set up, because those who have paid have access to this special channel.

The participant stressed that buying advertising gave a certain sense of freedom to civil society to disseminate crucial information, opening the channels to social media platforms. Since their posts fall under advertising, they are subject to that category of content moderation rules.

While activists have found a way to cope with the challenges of engagement with private companies, a hierarchical structure of partnerships exists among civil society organizations. Those who are part of the trusted partners channel receive special treatment and a more direct engagement with tech platforms:

That level of engagement is only for the privileged. It's like a channel for the elite, only for some. A place where the large organizations are known. But I think there are no more than 10 organizations in Colombia that know the people at Facebook.

The selected partner organizations have a simpler and more efficient channel of communication with tech platforms. Although they do need to follow the standard reporting procedures on a given website, they often have access to a designated person who guides and supports them in the process of reporting. At the regional level, they also have access to periodic meetings with Facebook and Twitter where they discuss different issues and opportunities, and are introduced to new products entering the Colombian market. Some organizations have also been invited to participate in global meetings, including at the companies' headquarters. Nonetheless, the participants stressed that no consultation had taken place regarding the design and implementation of new policies.

The power dynamics of partnerships between companies and civil society organizations in Colombia are dominated by the lack of a systemic framework of engagement. There is no assigned department or person responsible for public policy that organizations outside of the trusted partners can reach out to. The current structure is based on a business model that leaves smaller organizations no other choice but to buy advertising to gain visibility, subject to distinct advertising content moderation rules. The participant shared that under the advertising category, civil society could not post any COVID-related content that contained any remedies for local communities without facing heavy restrictions and takedowns. This has been particularly true for content in Indigenous languages, where any post containing the word "COVID" was removed. Other issues stemming from the limited languages available in the content moderation processes of major companies include hate speech targeted toward Indigenous communities in Colombia, which is rarely regulated. While harmful content is sometimes taken down after communities report through standard channels, no explanation is provided, leaving users without any information. This is highly problematic for Indigenous communities as their communication and advocacy heavily depends on their activities and interactions on Facebook. The application is often offered at no additional cost as part of Internet bundles, which is extremely useful for Indigenous communities who often live in remote areas of Colombia with poor infrastructure.

Finally, it is crucial to take into account the fact that engagement with private companies has changed over the years and will continue to do so. The same is true for the socioeconomic and political dynamics of Colombia, which is continuing to suffer a decades-long armed conflict. To establish transformative relationships requires a deeper understanding of the local context and the inclusion of its people in the decision-making that affects their livelihoods and human rights. Policies, products, and services implemented in Colombia have to be in line with the local realities, taking into account the particular harms that the technologies introduced may cause or how they may exacerbate the existing violence, and the impact they may have on the diversity of the country's population as a whole and of particular groups.

Moving forward

- Train staff on the complexities of operating in regions of conflict and understanding the protracted Colombian war.

- Adopt an intersectional lens that recognizes the diversity of people not just within each country in which the company operates as a whole but also within the socioeconomic contexts of each city.

- Take into account the diversity within civil society organizations, as the aim for each entity is distinct. For instance, those who protect children, or who deal with gender-based violence, reject the concept of anonymity and are in favor of blocking accounts (offenders generally hide behind their anonymity online), contrary to the approach of most other organizations.

- Get a deeper understanding of the complexity of diversity and recognize that freedom of expression is based on diversity and complexity.

4. Ethiopia

Since the start of the armed conflict in northern Ethiopia in November 2020, the Ethiopian government, its rivals, and the diaspora have circulated misinformative and violent speech on social media platforms to control the conflict's narrative. The war that flared up online was proliferated by Western broadcasters with click-bait headlines, and misappropriated and manipulated images omitting important context about the war. These fake information campaigns have fed into an existing volatile situation and intensified fear and tensions in a historically ethnically polarized country. Social media companies have been under heavy scrutiny for allowing users to post hateful and false content despite their awareness of their platforms' roles in the Ethiopian conflict. Their inactivity and failure to moderate content in a context of armed conflict has put a strain on civil society.

Nonetheless, local organizations' engagement with technology companies has remained weak in Ethiopia. Only a few of the most visible organizations running digital rights programs have been able to establish partnerships with the private tech sector. The objective of the organizations' engagement is three-fold: to reduce the role of social media in inciting or aggravating conflicts in the country; to protect and respect data privacy by having transparent and accountable data systems; and to increase their use of social media for activism. Elections and conflicts are times when organizations are highly concerned about the role of social media corporations and attempt to increase the channels of communication to mitigate the effects of false information and posts that incite violence. A participant stressed that engagement has not increased during the war and that platforms have barely adjusted their reporting mechanisms and content moderation strategies:

> *There isn't much difference in responses based on threat levels as we've seen in Ethiopia. Content moderation is very delayed on major platforms like Facebook and YouTube. Twitter has delayed responses. Telegram almost has nonfunctional reporting and moderation schemes for Ethiopian content.*

The existing power imbalance between the private sector and civil society means that civil society organizations have little say on the dynamics of the partnerships. Engagement is carried out on the companies' terms. The participant explained that while his organization had the privilege of one-on-one communication with businesses due to its trusted partner status, the large majority of civil society were left out of any engagement. Language often presents an added barrier to any form of efficient partnership, particularly for grassroots communities operating in local languages. As a result, English speakers have more opportunities to establish strong relationships with the private sector and address harmful content on digital platforms more effectively. There is a high perception of risk and urgency related to the issue of safety in fragile and war-affected countries. Content moderation in local languages is crucial in times of conflict that to deal with disinformation produced on social media.

The slow response from tech platforms and their inability to monitor content has shifted the responsibility to civil society organizations. However, no compensation and little support is offered for their increased efforts to mitigate the harms produced by businesses, as specified by the participant:

Generally, the corporations have the responsibility of supporting such initiatives with a systematic structure and financial resources as we are doing their job to make the services of tech companies harmless, both financially and technically.

The partnerships and trusted flagger programs of large tech companies are actually resulting in them outsourcing what should be their own responsibilities. Trusted organizations utilize the trusted partners channels of Facebook, for example, to help the platform moderate content urgently and with priority and contextualize it to local realities and issues. In doing so, organizations face the additional risk of state surveillance with a direct threat to their safety, particularly in Ethiopia where freedom of speech has reportedly been repressed:

We help Facebook understand the issues in our local context and monitor hate content on their platform. This should be done by the Facebook team and not us. This is costly for the partners and also may cause us to be targeted because of it.

The lack of transparency and data sharing around the technologies deployed by tech businesses, including insight into the algorithms, how they work, and the assumptions that power their platforms remains one of the leading issues inhibiting transformative engagement with civil society. Private companies are secretive about how they collect, process, and even use the personal data of their users. In order to assess the effectiveness of companies' responses in fragile states like Ethiopia, there is an urgent need for greater transparency—including information provided to governments and processes to enforce their policies—and access to data for civil society, including organizations, academics, and independent researchers. Increased public scrutiny of the technologies deployed in conflict-affected regions is crucial to minimize the role of the private tech sector in inciting further violence.

Moving forward

- Invest in local language content moderation and civil society engagement.

- Invest in trusted partner channels to allow for better communication and commit to clear targets for response rates and transparency.

- Disaggregate transparency data by key factors (such as language, sex, etc.) depending on the context.

- Disclose data collection methods, data collected, and how algorithms are designed and used.

- Provide local organizations with this information to monitor, document, report, and advocate for improvement wherever they see gaps for the benefit of the wider public.

5. India

Global events, such as RightsCon and the Internet Governance Forum (IGF), had a significant impact on the private tech sector engagement with civil society in India, catalyzed by the participation in 2015 of many of the country's digital rights organizations. The events served as a bridge between the two sectors providing a platform and meetings—thematically organized and invitation only—to enable and foster better communication and relationships. The conferences continued to take place even during the pandemic using an online format; however, encounters in person were much more impactful as per a participant's account:

> *There was one breakfast meeting, invite only. There would be 10 or 12 civil society representatives. If it was meeting with Facebook, it would be on a particular theme. It was usually Facebook, Google, or Twitter, separate meetings; you didn't necessarily end up at all of them, but [at] the one that fitted your sort of work the best. Since we work at the intersection of gender, sexuality, and digital technologies, often we were invited, to one that was all about [the] queer community and say with Grindr.*

While only a handful of organizations are invited from each country, the participant explained that their presence allowed them to also represent other organizations and share their concerns with big tech companies, establishing further trust with grassroots communities and a stronger reputation for working on these issues in India. However, reporting content-related issues and receiving a response from the platforms remains an enduring issue. The changes that do occur are on a case-by-case basis without any substantial transformation, resulting in distrust toward big tech companies and a buildup of frustration over the years. At the same time, organizations feel the need to hold on to the space available to them to be able to communicate with companies.

Through meetings with the products team at Meta, the owner of Facebook, the participant explained that the feedback they provided had some impact, albeit minor, on product design. Following the organization's feedback, the company improved its technology to avoid a user having to upload a non-consensual image to the system during the reporting process. Nonetheless, there remains a need for the user to go through a trusted partner to proceed:

[There have been] no changes externally. There may be [changes] in product design with the oversight consultation there on privacy, in small ways. For instance, [in] the nonconsensual, intimate image conversation, two or three of the recommendations that we made very strongly at that consultation are now visible in the design. Suppose I felt that my intimate image might be put up without my consent on Facebook—they developed a tool where I could report it to Facebook. So there was a whole discussion on should we suppose the person then wants to withdraw their image? Should they be allowed to? Or would it then be treated as a frivolous complaint? The small things, but not the big ones, that's still elusive, sort of how to improve reporting.

The early engagement of the organization with the big tech companies was limited to yearly meetings and based on the interests of the individual leading a given policy team. While Meta's engagement with civil society has evolved over the years and has become more continuous, Twitter's approach remains person-dependent:

The head of public policy, then at Twitter in India, was very interested in getting nonprofits to use Twitter more meaningfully. So we ended up doing a joint event in 2016 where we convened a lot of women's rights organizations, as well as a lot of influential women in Mumbai, and we did an all-day session with Twitter where they introduced us to tools and this and that, and they supported it. But then this person actually left Twitter. And then that relationship has just fallen [away].

Such person-specific engagement is also true for Google. In contrast, Meta now holds more frequent and smaller meetings with civil society organizations through its different teams both nationally and at the company's headquarters. Its safety team, for instance, has reached out to the organizations to understand the layers of harassment and violence experienced by marginalized identities. Through research and collaboration, the organizations have provided the company with a better understanding of the nuances within the different types of identities and experiences of its users, which is often not reflected in its reporting and response mechanisms. Harmful content targeting threatened gender identities and female activists in the form of jokes, viral videos, memes, comments, etc. were also identified and reported to the platform. The participant explained that their engagement with Meta went from discussing general issues to addressing specific points and having a one-on-one relationship with Meta, including the safety, policy, and product teams, both in India and in the Bay Area. Following their conversation with the product team in Silicon Valley, the company is now reviewing its community guidelines.

The role of the organization as a bridge between companies and civil society has been significant in addressing digital harassment and abuse. To facilitate the reporting process for users, a digital helpline was built where callers can submit specific complaints, which will be escalated to the platform.

While the product has not been made available to the public as of yet, attending trusted partner training sessions has enabled the organization to keep up with the new features and products of the company that would be of use to the helpline. Hence, being a trusted partner has become a privilege—though not ideal—and has facilitated the communication with the platforms and improved the reporting process:

So as a trusted partner, they will go one layer above moderation. We've also been invited during the pandemic to, for instance, a big global initiative on nonconsensual, intimate images. So we've been to global consultations and conferences on those, which has actually been quite helpful. We've also [given] our comments to the Oversight Board, so we could influence them to some extent. Finally, we are advisers on Facebook's Global Women's Safety Team, which is honorary, not paid.

Nonetheless, certain types of engagement can often be problematic and go against the organization's principles. The participant expressed that the organization often faces a dilemma accepting the resources offered by the company while being aware of its critical policies and holding on to the relationship as its only means of engagement:

We don't know where the engagement should end when you enter a complicated arena; for instance, they've offered us a grant for some of the work we do, but we don't feel comfortable taking funding from them. How far in bed do you want to [get] with Facebook? So that engagement in itself is a little complicated, because we really need to engage with them to make our helpline service meaningful.

Beyond their established relationships with the companies, organizations continuously face issues with reporting harmful content on their platforms, especially for queer users.

The response depends on the person who decides on what violates community guidelines and who inputs the data in the algorithms, which are found to be highly biased. The process then becomes inflexible, leaving out the diverse gender experiences:

In one of the women's safety consultations, we tried raising the issue of how do you define women? Whose safety are you talking about? Does it only include cis women, or also trans women, nonbinary people? However, [the companies] still remained largely binary, so we don't see any massive shifts in the reporting.

To bypass some of these issues, civil society organizations have resorted to mass reporting where a piece of content is shared among those in a trusted circle who in turn report it to the platform, resulting in a higher probability for the content to be taken down. Civil society has had to be tactical and devise several strategies based on lessons learned. However, the onus still remains on the user to find and understand how to report content, rather than being provided with the necessary information and safety tips by the platform.

Another limitation in the reporting process has been language and a lack of context. As Hindi words are often typed using the English keyboard, abusive language is then not detected by the algorithm and reporting does not lead to favorable results. While the companies claim to be linguistically inclusive, there is no transparency on the data input or if there is representation among the teams to reflect the cultural nuances:

What about language that might actually count as abusive language but has been reclaimed? For example, SlutWalk, which became a campaign. But content might be taken down, because context is missing. What about words that have been redefined or counterspeech?

A system of engagement is necessary to disrupt the current uncertainties and the power dynamics of the relationship between the two sectors. The participant pointed out that engagement has now become a ritual where no feedback or reasoning is ever provided from the companies following a recommendation or reporting. Support from the platforms on their various features and how to use them would help to address content-related issues and facilitate the reporting process for organizations and users:

> *You're never sure what's going to happen. What would help is [if] after the engagement, they write back saying, thank you, this was very useful, these are some of the ideas we are going to take forward. The way of working is [very incremental], which is frustrating. People are facing hate and harassment, and violence and abuse, obviously a huge deterrent to the user experience. [Companies should show us how] one feature will bring you here, then the next feature will take you there.*

The emphasis is currently on the user having to learn every feature of each product and navigate each complex system of reporting, which is highly unsustainable. Grassroots organizations—who mostly use social media platforms on their mobiles—are most affected by having to go through many steps and with little to no knowledge of the process. Rather than addressing the issues individually and in isolation, the participant calls for an inclusive system of engagement and a change of the current framework:

> *To even get to the reporting mechanisms, you have to go through so many hoops. It's very cumbersome, it's not human or intuitive. It's not enough to just keep complaining and saying you're doing the wrong thing, because we get stuck in the framework. Now it feels a little like, why are we engaging at all?*

Moving forward

- Provide evidence of reports on an independent platform and analyze the cases by external experts.

- Create a multistakeholder cohort of experts independent of companies with the power to make decisions and recommendations based on data.

- Convene experts to provide regular feedback on the design of platforms and suggest prototypes.

- Based on the results, build an inclusive system of representatives from various sectors to redesign current reporting mechanisms and gather evidence.

- Implement a pilot project in collaboration with big tech companies where users test proposed ideas and evaluate their efficiency.

- Build a database or a bank of expressions and words that continues to be updated to address the linguistic issues and lack of context in the moderation process.

- To improve user experience, create a button on the app that would activate an alarm during a critical situation and bypass the complex system of reporting and communicating with the platforms.

6. Iran

Until recently, Iran was the most sanctioned country in the world. US sanctions in particular have impacted the ability of Iranians to access the Internet freely and evade government surveillance. Faced with outdated policies and ambiguous guidelines, tech companies have refrained from offering their products and services in Iran. As a result, Iranians must rely on products made in Iran and approved by the state, increasing the risks of state surveillance and censorship. In addition, Iranian civil society struggles with content censorship from tech platforms, often with no clear justification.

With limited access to companies, civil society's engagement began with research produced by small media organizations predominantly on unjustified takedowns by social media platforms and Internet shutdowns. While no platform exists for collective action, advocacy groups and organizations would issue statements to companies often through a third party outside of Iran. The engagement remains bound to personal connections both within organizations based abroad and within corporations. An interviewee explained:

> *[When] many civil society activists/ advocates … get arrested by the authorities, their friends reach out to the tech companies and close their account temporarily. Once they are released, they need to get their services opened but the verifications [are] always a trouble. Some of them don't trust the infected SIM card and they change the phone and [have] trouble to reopen their accounts.*

Safe access to the products and services of technology companies is crucial for civil society to circumvent state repression and international sanctions, including the ability to make transactions online. Antivirus services for instance have the potential to protect users against spyware and government surveillance:
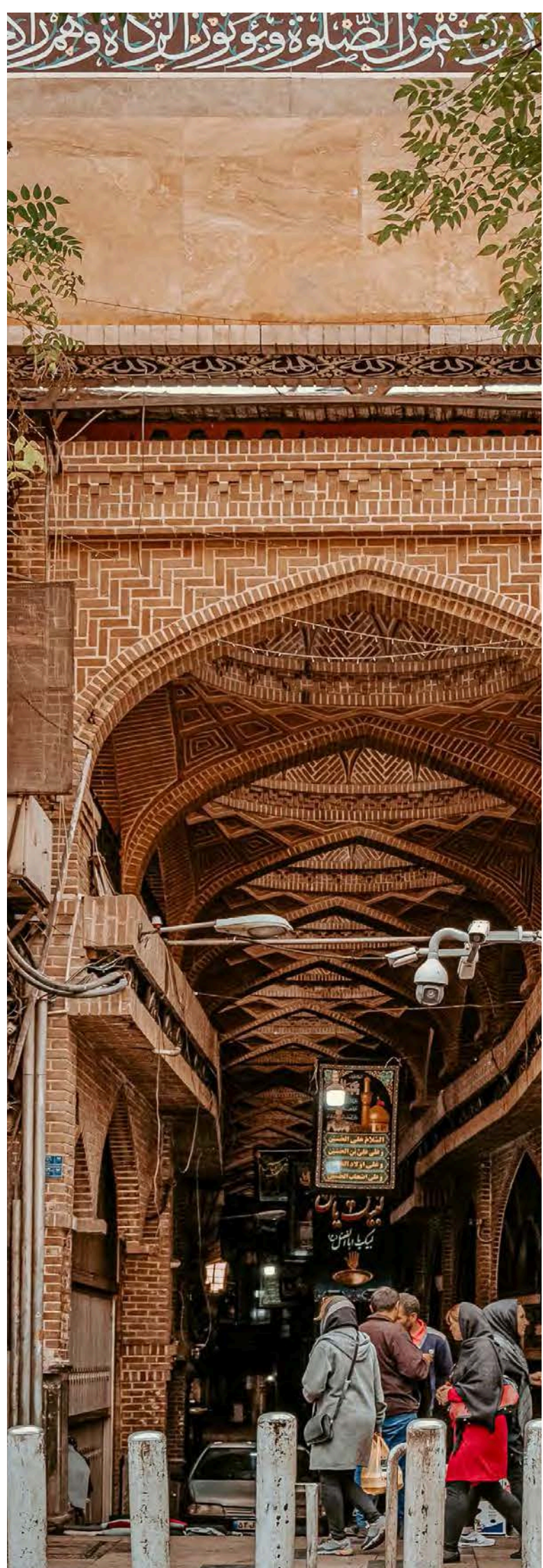
Civil society wants access to the services of technology companies in Iran since some of the services are not accessible due to the US sanctions or some of the tech companies over [complying] with the whole idea of the sanctions. They need to have those services free or design a transactional channel to buy the paid services due to the sanctions restrictions (including VPNs, antivirus services, password management tools, etc.).

Platforms such as dating apps for instance—particularly for the queer population—are often used by the government to target and prosecute users. Through overseas channels, Iranian civil society initiated engagement with dating platforms such as Grindr to hold them accountable for the frequent arrests of its users. As a result, the geolocation tool was obfuscated to prevent users from being identified:

We brought to their attention how some platforms are being used and weaponized to target folks. We had the aim of saying, your tools are being used in this way in contexts and countries you did not really take into consideration when you were deploying or scaling up in, and you need to make specific changes to protect the community.

Prohibitive laws that criminalize certain identities and heavy state surveillance deter engagement with companies, creating a new, chilling effect. Nonetheless, the participants in the interviews stated that users were aware of what they needed and the changes they wanted in their experiences on different platforms. The shortcomings of the private sector, such as the lack of a system of engagement, increases the challenges faced by civil society. Engagement with private companies, when made possible, has been ad hoc and on a case-by-case basis. The safety of users and timely engagement is intertwined. Delayed responses, if any, combined with a lack of understanding of the local context put the lives of Iranian users in great danger, especially those from vulnerable communities:

The absence of knowledgeable people was a big issue at the time, because even if users had communicated with the different platforms to say the police are using fake accounts on the platforms to lure people to a meeting point and to basically use the content of those chats to arrest them, it is not the geolocation [that was the problem], like the conversation wasn't leading there. For some civil society representatives, effective engagement with tech companies might save the lives of their stakeholders.

Activists and civilians who resist the oppressive policies infringing on their freedoms (e.g., women refusing the compulsory hijab; journalists, teachers associations, and environmentalists who protest) are often held by the authorities and need urgent live services to maintain their activities' safety before and after arrest. However, companies' responses do not vary with different threat levels. In addition, the Iranian state has the power to request companies to submit the personal data of their users, putting people's safety in jeopardy. The high risks associated with communicating with the platforms means that local civil society generally goes through the diaspora or outside organizations to ensure a level of separation. Overseas organizations also help to aggregate the necessary data and provide context to private companies regarding a specific issue in the engagement process. Nonetheless, there is no structure connecting the diaspora to local communities when a content-related issue occurs (e.g., an arrest following a YouTube video).

A lack of fluency in Farsi and understanding of the local context have added to the existing barriers to a more efficient engagement. Rarely are the issues specific to the sanctions imposed on Iran discussed during international digital rights events. Given the unique nature of the limitations due to sanctions, solutions should be drafted and implemented by professionals proficient in the Iranian culture, context, and language:

What civil society needs … Farsi-speaking special designated representatives 24/7 with help desk capabilities. What they are getting at the moment is limited offline services, which are not in Farsi mostly. Often, we will not look at the issues in our country in a specific way if we don't have a person from that group, from that country.

With the current difficulties in communicating with local civil society, the Iranian diaspora often leads the engagement with the companies and controls the narrative, according to one of the participants in the interview. Often for the purpose of protecting civil society in Iran, the diaspora refrains from discussing and disclosing any information, operating with local organizations under the radar. Despite the clandestine collaboration of the diaspora and local civil society in Iran on specific issues, the creation of a collective that would enable more systematic engagement has not been possible. In some cases, local civil society has been able to reach out to the companies directly, which has resulted in favorable outcomes (e.g., GitHub's ability to obtain permission to offer its services in Iran despite the sanctions). Academics have also played an important role in reporting and highlighting some of the online-related issues through international publications and involvement with international organizations. Collective actions can often derail an issue, rather than addressing it within the specific context in which it occurs:

The private tech sector's current patterns of consultation with a few selected civil society organizations have generated a common narrative across all included members, according to one of the participants. Given their fear of losing their position and engagement privileges, trusted organizations often refrain from confronting the companies and addressing the issues in an efficient manner. As a result, those outside of the trusted circle encounter greater challenges in engaging with companies and bringing attention to a critical situation:

When you interview trusted organizations, if they're part of the same coalition, they'll use the same kind of language, even if it does not reflect reality.

It's to maintain that relationship, and they're scared to speak against the companies. They want to be close to these tech corporations. So that is a big problem I see.

In the few cases that engagement has taken place, representatives of civil society have been asked to sign a terms and conditions document, which they often do not fully understand nor feel comfortable with. However, the participant explained that they feel compelled to agree with the terms given the unequal power dynamics and the risk of losing their benefits. Their lack of trust in the companies remains a great challenge, particularly in the absence of a guarantee that their personal information will be kept confidential. Clear industry standards around the use of these agreements and guidance would be highly beneficial for civil society.

Moving forward

- Build a framework for engagement that is specifically designed for the Iranian context.

- Design and provide tools that would help Iranian users to bypass sanctions, increase their safety, and avoid state surveillance when possible.

- Provide transparency on how organizations are selected as trusted partners and on their framework for engagement.

- Create and provide urgent live services specific to the Iranian context for users under critical threat.

- Design and provide trusted tools and services made available to the local communities to avoid the great risks associated with state surveillance.

- Foster a global community of stakeholders that would enable local civil society in Iran to have access to tech companies and use their channels to address some of the critical issues they face.

7. Lebanon

In 2016, civil society in Lebanon was among the first in the world to publish a report on online campaigns, digital media, and elections, warning against the potential misuse of data on social media platforms for electoral purposes. The publication also looked at what tech companies, as well as the regulators, should do to make sure that election campaigns do not get sidelined, distorted, and disrupted by the misuse of people's personal data. Lebanese organizations have also conducted an in-depth analysis of each platform and the capacity of the Lebanese government to respect the fundamentals of the digital rights of its citizens. Nonetheless, the level of awareness of the general public on the concept of digital rights remains low.

Given the geopolitical context of Lebanon, the concerns of social media companies on issues of hate speech related to terrorism content were the driver of engagement with community media organizations. The participant in the interview explained that the situation in Lebanon triggered the relationship with tech companies and strengthened their partnerships. He explained that rather than efforts from his organization to communicate with the platforms, it was initially invited to contribute its expertise on the topic in a series of workshops. It eventually became a trusted partner of the various platforms and has been collaborating on content policy issues related to terrorism, developing very strong ties with the journalism arms of the big tech companies, including the Google News Initiative and the Meta Journalism Project. While it has established strong partnerships and advised the platforms on how to best support online media, it has also maintained a critical approach and continuously pushed the platforms to rethink their monetization model by developing parallel advertising structures for independent media:
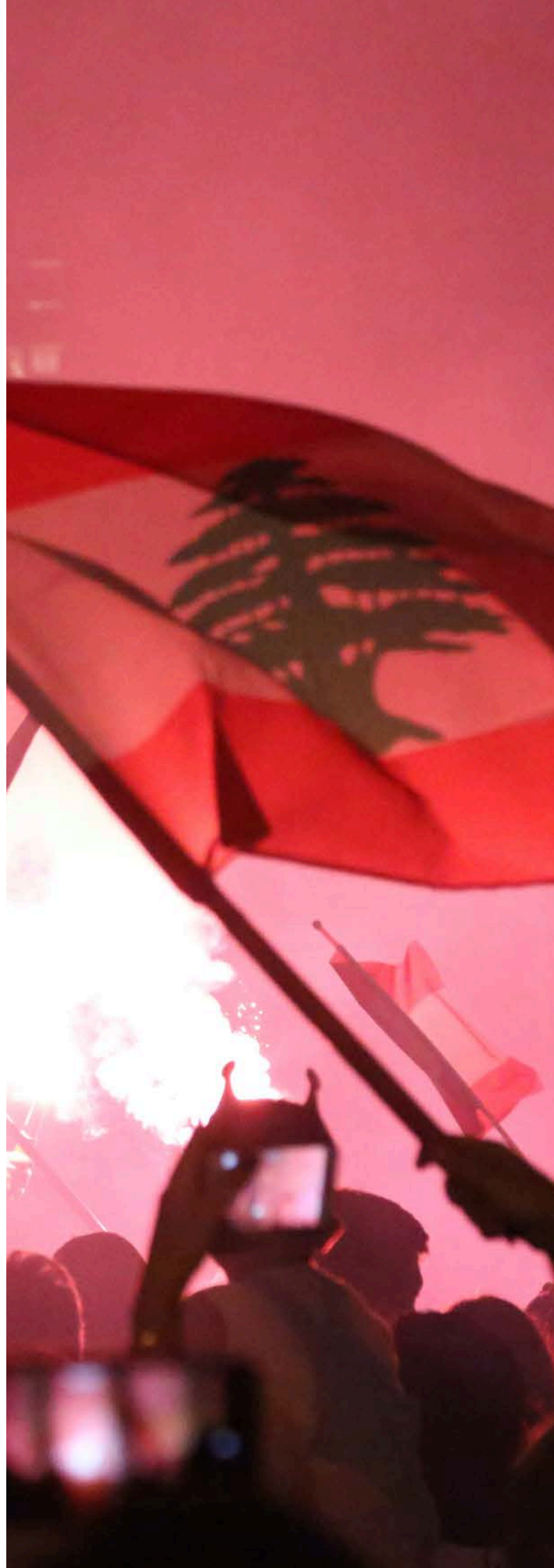
So we developed very positive and strong ties with their journalism branches, who would very often refer us to their policy people. For example, we've worked very closely, but through the journalism people, on horrible takedown decisions by Facebook, because they completely misunderstood what an article was about. So this expedited link through the journalism team helped us quite a lot. And the same applies to Twitter.

The accomplished background of the organization and its trusted partner status mean that it enjoys a much higher level of engagement with the private tech sector both at the national level but also with stakeholders at the company's headquarters. Nonetheless, this does not necessarily translate into an easy process to get decisions reversed, particularly for requests for takedowns:

For example, one of the very prominent writers from Lebanon (the Middle East alias, who you know, big name, potential Nobel candidate) wrote an article that was very critical of Fatah, in Palestine, about their corruption, etc. And actually, Fatah supporters used the fact that he used the word "resistance" several times in his article, although he wasn't talking about [violent] resistance, in order to actually report and lead to his exclusion, I mean, the constant takedown and limitations on his ability to post and share on Facebook.

A poor understanding of the local context, the political agendas of different groups, and the limitations of moderation, particularly for non-English content, have added to the existing challenges:

When there are articles against Hezbollah, actually, Hezbollah supporters report the article as if it was promoting terrorism. And this leads to Facebook misunderstanding or being bad at AI in Arabic and removing the content.

So, for example, in the case of the writer, we reported the situation, etc. And it led to the restrictions being lifted on his ability to use Facebook, although I'm not sure yet if the content was brought back or not.

While the organization has been engaging with Twitter on issues related to online media and journalism, it has not interacted with the platform to report harmful content. Nonetheless, it engages with the company to address other issues, such as accounts of media activists that have been blocked or hacked via direct contacts or through other organizations that work closely with the platforms, such as SMEX (Social Media Exchange). The participant explained that the turnaround time for Twitter's responses was fast for emergency cases and a couple of hours on average. Facebook is generally much slower to respond; however, the level of conversation is much deeper. To complement its efforts with platforms, the organization also works with other smaller institutions and activists on procedures to protect their accounts, adopt safer ways of connecting to prevent further attacks, and recommend that they get certified on Twitter, for instance, among other support.

Rather than working on individual cases when it comes to content, the participant pointed out that the organization's involvement with tech companies had a stronger emphasis on policies. It does however, handle some three to four issues related to takedowns per year on Facebook. Its established contacts with the company, including personal and long-term working relationships with company employees who are Lebanese and familiar with the local context, facilitate the engagement and expedite the response from the platform:

There is no local office in Lebanon, but very often key staff are Lebanese. For example, the former managing director of Facebook in the MENA region, who just left a few weeks ago, is Lebanese and we happen to know him. Same for the new policy director at Facebook for Lebanon and Syria, which helps because they have a contextual understanding. And very often, they used to work in sectors, either in diplomacy or in NGOs or in companies, … with a strong policy focus. This is why our paths very often would have crossed somewhere like five years ago, eight years ago, and it's all about maintaining relationships.

An explosion that took place in Beirut in 2020 triggered an increase in engagement with Facebook, Google, and Twitter when the organization launched its media recovery fund. After mapping the damage suffered by the media sector and journalists, the organization launched a fund to help them recover their equipment, rebuild their houses, buy new cars, and provide those suffering from the economic consequences of the explosion and the Lebanese economic collapse with livelihood support. The fund also offered grants to produce investigative journalism on the tragic event. The platforms stepped in to support the endeavors in various forms. The Google News Initiative, while not supporting the work with financial resources, helped the organization develop internal databases to follow up on the numerous requests it was receiving. Facebook, on the other hand, donated generously and provided the organization with advertising credits to promote the investigative stories resulting from the fund. Twitter ensured the organization's key staff were certified on the platform and recognized as credible actors. During this time period, the three companies' responses were provided within a maximum of 48 hours.

Stronger engagement and transformational relationships are forged mainly during global events, according to the participant.

Taking part in international conferences on a frequent basis can be a key driver to establishing and deepening communication with not only the tech companies but also stakeholders in organizations and governments. In-person meetings are a useful way of creating contacts, particularly post conference social events that have opened more doors than any official letter has, based on the interviewee's account.

Beyond the big tech companies, the organization has also created a relationship with the tech startup scene, predominantly in Beirut. While it is a growing industry in Lebanon, the participant stressed that these startups do not center digital rights in their designs or processes. The organization engages with tech startups to ensure they take digital rights into account in the creation of new products and programs, whether targeted for use by the government, private companies, or individuals:

A good friend of mine launched probably the very first application for food delivery from restaurants, before Uber Eats and all. The idea of actually selling people's preferences to restaurants in order to understand the demographics, etc., was something that made complete sense to him, because he needed to make money, [and did not understand] the potential implication it can have for digital rights, before Lebanon passed its transaction law, and before anybody cared about GDPR [data protection legislation]. So we had conversations with the startup before they launched anything, to ensure that some elements were taken into account. And once the product was launched, just evaluated it and came up with criticism or praise. So we first start with engagement and then we eventually say that there is something going wrong, if, for example, the criteria are not met. So this is something that we're developing slowly but with our local community.

Platforms other than social media have also played an important role in the political scene of Lebanon, particularly with content related to terrorism. The participant explained that engaging with local communities and smaller platforms (e.g., the chat function of Airbnb) that often escape moderation was also central to the organization's work addressing dangerous content. Nonetheless, engagement with tech platforms can only be strengthened if the local communities are made aware of their digital rights and are involved in the conversations and processes, which unfortunately is not really the case. To address this gap, the organization serves as a catalyst informing and educating communities while serving as a connector to tech companies.

Even though the organization has been widely recognized in the media rights landscape, the participant shared his awareness of its limitations and skepticism on its ability to influence lasting change as an individual actor. He explained that as there are fundamental decisions related to how information spreads that the big platforms do not want to take that into consideration, simply because it would affect their business models. Beyond the small victories of civil society, a much more concerted effort is needed to impact policies.

Moving forward

■ Develop sustainable channels for communication and engagement with civil society that do not rely on personal relationships, and are resilient to changes in personnel or similar factors.

■ Address the issue of false-positive content enforcement for news or legitimate comment relating to sensitive terms or groups. Do so with transparency and consultation.

■ Support lawmakers around the world to understand the issues at stake, and reduce the knowledge gap.

8. Myanmar

Burmese civil society's engagement with tech platforms developed in 2012, shortly after the country started to liberalize. During the same period, Facebook became the primary source of access to the Internet as its popularity rapidly grew. With no monitoring in place, the platform became a hotbed for extremism as violence broke out between the Buddhist majority and the Rohingya Muslim minority. Concerns grew about the links between activity on Facebook and the violence and instability in the country. Nonetheless, it was not until 2018 that Facebook began to pay attention to its content-related issues in Myanmar and its role in the massacre of Rohingya Muslims by the military. The company eventually admitted its responsibility in inciting violence offline and the genocide campaign against the vulnerable group.

Civil society's initial point of communication with Facebook was through contacting its policy team in an attempt to warn the company that the platform was being weaponized and to urge them to improve their content moderation. When a response was provided by the company, the solutions offered were highly inadequate and lacked knowledge of the local context, prompting organizations to use alternative strategies for a more transformative engagement. An interviewee stated:

The type of solutions that they brought into the discussion were to window dress the issues, which made it very difficult for us to tackle [them]. So we actually had to bombard them with media, a lot of evidence-based data, and then only after that, we managed to get more of their attention and get in touch with a much wider team.

To make up for the companies' shortcomings in efficiently moderating harmful content, civil society has been monitoring social media platforms and submitting the results to the default reporting mechanisms. In the early years of engagement with Facebook, however, the reporting system was highly unsustainable and inefficient, placing a tremendous amount of stress and workload on civil society. While the company has expanded its monitoring capabilities, the responsibility still lies on organizations to identify and report harmful content. Ambiguous definitions of what constitutes hate speech pose further challenges. As a result, content-related issues are addressed on a case-by-case basis, rather than through an established system of reporting:

So they tell us, if you see [this content], just give it to us, and then we will look at it, and if it's violating our community standards, we will take it down. So we look at it, if we see it, we will give it to them content by content, and then they will look at it, and then they will take it down. Also, what we consider as dangerous speech is different from their definitions. So that reporting doesn't actually work very well and doesn't make sense.

Furthermore, the harmful content identified by civil society only represents a fraction of what circulates on the platform. The company however has improved its response time since the genocide campaign in 2017, and content reported using its tools on the platform is generally reviewed and addressed within 48 hours.

Direct access to individuals representing private companies was made possible through attendance of international digital events. The interviewee noted that initial in-person meetings in early 2012 were mostly with the policy team at Facebook, which led to invitations to visit the headquarters of the company. However, it was not until 2014 that the company made an official visit to Myanmar to meet with different stakeholders after the platform was shut down by the military. Allegations that harmful content on the platform led to a violent uprising prompted conversations with civil society and media professionals in the country.

The company followed up by sending an Australia-based representative to Myanmar twice a year to meet with the different sectors. Facebook onboarded a professional dedicated entirely to Myanmar in 2019. Until then, the platform initially utilized content moderators hired by a third party based in Ireland with no knowledge of the local context, inhibiting any form of efficient engagement with civil society. Once a policy team was established at the company, a sole representative based outside of Myanmar was responsible for the entire Asia Pacific region. Without access to professionals with expertise in the specific context of Myanmar, transformative engagement is not possible:

We did manage to raise issues with them, but that doesn't really work very well. They might give us an email [address] to send [reports to], but then it's more useful for these platforms that they onboard people who know the context, actually care, and whom we can reach out to; it'd be much more useful for us.

Advocacy with the support of Facebook became feasible once the platform expanded its staff beyond policy work, with each team dedicated to a special topic (e.g., media, community engagement, product, etc.). While Facebook has made headlines throughout the last decade for being weaponized and not taking necessary action, the platform has invested more resources and support in Myanmar compared to other tech companies. Through its trusted partners program, the platform provides extra features to selected organizations to enable them to submit detailed reports and escalate an urgent matter to a specific person. On the other hand, the participant explained that none of the tech platforms has a dedicated person for Myanmar other than Facebook and TikTok. Following the last coup d'état, the organization was able to have a meeting with TikTok; however, it is yet to meet TikTok's policy representative for Myanmar.

Personal connections at tech companies are essential to obtain trusted partner status. The participant shared that after sending persistent emails, the organization was finally able to be part of the trusted flagger program at Google, which includes access to a personal email address and prioritized communication. Dangerous content on Google's platforms can be escalated through a special reporting channel. Additional access to emails for activists was also provided to address frequent arrests and to submit requests for their accounts to be deactivated for their safety. Nonetheless, delayed responses and the lack of an expert in charge of Myanmar has inhibited efficient engagement with the company:

For YouTube, it takes them a long time to respond. One harmful [video] that we reported during the elections was only reviewed five months later. We started to bombard them with removal requests, but the person we know at Google is more about accessibility, and not content moderation. That person would have to send it to the specific team, and if they approve, they will call her and then she will talk about the issue. So it's not easy.

As Twitter is not as prominent in Myanmar, civil society only engages with the company to report detained activists and request for their accounts to be deleted. The participant explained that through tweets about a case of uniformed soldiers using TikTok to threaten civilians, Twitter reached out to the organization to arrange for a meeting. Following the initial engagement, the platform onboarded a public policy expert for Myanmar.

Given the common Internet shutdowns in Myanmar, engagement with telecommunication companies is extremely relevant for civil society. The participant explained that prior to the coup d'état, the organization's interactions with telecommunication companies were mostly to advocate for accessibility, prolonged Internet shutdowns, and privacy.

Following the government's initiatives to install intercept software, the engagement expanded to address the operation of the regulatory body and request the easing of restrictions on some of the banned websites. The organization has also been working to encourage the businesses to adopt human rights guidelines and respect users' privacy. The only telecommunications company that it has engaged with is Telenor, initially a Norwegian company and a member of the GNI global network.

Moving forward

- Ensure there is at least one professional dedicated to Myanmar for each of the companies whose products are used in the country. Ideally, several experts committed to different topics to ensure each issue is addressed appropriately and in a timely manner.

- Build capacity within countries sharing similar situations, so civil society from the Global South like India, Myanmar, Sri Lanka, Indonesia, which have similar problems can document the issues they are seeing in their own contexts and hold companies accountable.

- Create collective advocacy, which is useful for building a pool of knowledge and harnessing it for joint activism.

9. Pakistan

Despite the many shortcomings tech platforms face globally, Facebook was found to be more engaged with civil society in the Global South than its counterparts such as Google and Twitter. For example, the platform regularly reaches out to local experts to consult on policies and new products launched in Pakistan. According to the participants, Facebook ensures access to its different teams and has been proactive in its outreach efforts and responses.

> *They held multiple meetings in Pakistan. For example, before the Oversight Board was created, they were doing global consultations on what the shape should be. Then, in terms of how local policy will connect with Facebook as well, they have conducted a series of consultations. So in terms of access, this might also be because of the fact that the Facebook team who deals with Pakistan … were active in the circle beforehand, as well. There are actually four people who look at Pakistan: one who looks at policy, one at legal affairs, one at partnerships, and even one for communication.*

Nonetheless, one of the interviewees stressed that much of the attention provided by Facebook can be regarded as a public relations scheme as not much of the feedback provided by civil society is considered by the platform or results in changes. The participant shared that the platform adopted these engagement strategies to contain any discontent of civil society related to the many issues of big tech companies in Pakistan:

> *How much is this damage control for everything wrong they do and that comes to surface? I keep wondering whether having these personal connections is a way to mitigate the kind of reaction that should be coming from Pakistan, such as with the Facebook Papers. I've not seen a public discourse happening in Pakistan yet. Even when I've asked in groups, I've not seen people responding in the way that I would have thought they would.*

Engagement and responses often depend on the personal connections established with the companies. While one of the organizations interviewed had a direct relationship with a senior representative at Twitter and addressed any problem via messages on WhatsApp as part of trusted partner privileges, the other organization expressed many concerns regarding its attempts to communicate with the platform. The risk of hate speech on Twitter going viral in Pakistan is much higher than on other platforms.

We have had cases of blasphemy accusations obviously being orchestrated by network groups, bots, etc., [and] trending on Twitter. A specific example is a horrific murder of a young woman beheaded by her ex-boyfriend. For consecutive days, a trending hashtag on Twitter by activists was circulating [calling] for justice. However, many other hashtags went viral related to morality and decency, and discrediting the young victim for having said no to marriage.

Many civil society representatives reported the harmful hashtags to Twitter. However, the platform only provided automated responses advising each user to remove the content from their individual panel. While in this particular case the victim had already passed, the participant stressed that many other targeted individuals face death risks due to the unresponsiveness of Twitter. When a response is provided by the platform other than by an automated system, it is often too late to mitigate the harms. The participants explained that hate content is also prevalent on YouTube; however, the platform has remained inaccessible to civil society organizations in Pakistan.

Every time we have reached out to Twitter, we get a polite email back after a couple of days, which doesn't really account for actual engagement. So again, this is very limited to when you actually engage and reach out with regards to a complaint, but overall, with regards to policy, with regards to how it's affecting political or gender discourse, we have never been actively approached by anybody from either Twitter or Google. YouTube is also [becoming] an extremely toxic place.

TikTok on the other hand engages directly with the government and regulating bodies, though rarely with civil society. The unequal power dynamics between civil society and large corporations means that the terms of engagement are only drafted and led by companies. Consultations lack complete transparency from the selection process of local experts to the methodology used and outcomes from the feedback provided.

Engaging somebody in consultations and being transparent about how those consultations are actually considered or not considered during policy discussions or policy decision-making —that's something that's pretty much opaque.

The participant stated that representatives who do engage with civil society often lack any decision-making capacity, resulting in no meaningful changes post consultation. The Facebook team for instance has no authority within the company to influence policies or senior representatives to adequately address the issues faced by civil society in Pakistan. The engagement with civil society is not reflected in the decision-making of tech platforms. As a result, there has been increasing distrust toward tech companies and a reluctance to continue to engage. Many of the consultations are incidental and take place after the harm has been done, rather than being preventive:

The common thread among all platforms is, no matter how actively they engage, or proactively they engage … our voices are sought by some and not by others, but they don't appear to be [reflected] in the decisions that are consequently made.

The government on the other hand has had more success in the changes yielded after engaging with tech companies. The strong state and corporate relationship that has been established has had human rights implications, with regards to surveillance. Under national law, the companies are required to provide the government with unencrypted data of users when required, including normally encrypted data on messaging platforms such as WhatsApp.

Many companies comply with government requests, even if they infringe on user privacy. At the same time, pressure from government bodies —through local policies that could possibly impact corporations, for instance—has propelled an increase in many of the companies' engagements with civil society. One of the participants noted that responses from Facebook for instance corresponded with different threat levels and the outcome of addressing issues largely depended on the nature of the content, directly impacting the safety of users. The relationship of the organization and companies has gotten closer since the government introduced laws and regulations that impact both civil society and the private sector.

The unified front of civil society organizations in Pakistan has been an important factor in both their engagement with companies and the government. A coalition of civil society actors was created in 2015 when the government introduced the Prevention of Electronic Crimes Act, which has since then strengthened the work of individual organizations. The participant stated that they come together to draft requests, statements, and joint reports both for companies and the state, resulting in substantial changes in policies in both sectors. They also pass on opportunities to each other based on the area of expertise of each actor and often organize events together:

The government will come up with a draft law, we will study it and issue a statement, then the Supreme Court Bar Association will talk to them and help us draft a statement, the Human Rights Commission of Pakistan will issue a statement, the Pakistan Federal Union of Journalists will issue a statement, etc. These are really powerful groups— lawyers, media, civil society—and the TV channels will pick it up and do shows strengthening our work. That has helped us to challenge laws and policies in court.

The solidarity between the multisectoral civil society actors has also enabled them to negotiate companies' requests to sign a nondisclosure agreement (NDA) or other form of agreement. According to the participants, most requests were generated by Facebook and TikTok prior to consultations on new products. Consultations on policies on the other hand did not include NDAs. While Facebook has offered no compensation for experts' time and feedback, TikTok has been more open in its remuneration process. In addition, Facebook does not provide complete coverage of costs when inviting civil society actors to its meetings and conferences, an added strain on the limited resources with which organizations operate.

Initial engagement largely takes place during regional and international meetings. One of the participants explained that given the limited relationship with Google in Pakistan, much of the engagement with the company happened during Asia-Pacific Economic Cooperation (APEC) conferences. However, while Google representatives are present during the event, the focus is solely on disinformation-related issues. Rather than holding discussions on how corporations operate, the onus remains on the solutions civil society is creating, removing any responsibility from companies and preventing issues being addressed at their core. As the consequential harms are foundational and structural, there needs to be a proper space for more in-depth conversations, which would also include an understanding of the structures within the corporations and how processes take place:

We don't understand the structures within these corporations. And that lack of knowledge doesn't allow us to propose more directed, more focused recommendations when we are talking to them. So the advocacy becomes very generic. Having that kind of a space where this knowledge can be shared, and where there's more transparency regarding what's going to happen after this consultation, the results, and the ultimate aim [is vital].

The participant stressed that the objective cannot simply be to engage and understand the local context, which is the current framework for conversations with civil society. Rather, the interactions should aim to ensure that policies introduced in Pakistan reflect the local realities and contexts. Finally, engagement should take place with a variety of stakeholders representing diverse communities. Relationships with just a few organizations do not reflect the dynamics of the diverse users within a country, and civil society actors will be bound to their own area of expertise and communities they serve, limiting their perception of the whole of the Internet in Pakistan.

Moving forward

- Create a structured and participatory model of engagement with more balanced power dynamics to keep companies accountable. The agenda should be designed by both civil society and companies, and offer more proactive discussions to design preventive measures rather than being focused on incidents.

- Build a space to hold more in-depth conversations to address issues at their core, and create foundational and structural changes (from defensive to constructive engagement).

- Provide more transparency and bridge the gap in understanding of how the companies are structured and operate so civil society actors know how to reach out to the private sector and address each problem with the appropriate team.

- Establish engagement teams with more authority to escalate issues and incorporate the feedback provided by civil society in the decisions and design of policies and products.

10. Palestine

For over five decades, Western mainstream media has shunned Palestinian narratives, a situation that has not only remains unchanged, but has deteriorated. The unjust status quo has now intensified on digital platforms, silencing Palestinian voices and excluding them from many online services. Global companies offering digital products from Zoom to Facebook, Twitter, Google, and PayPal have contributed to the digital divide targeting Palestinians and adopted a biased approach in their policies.

Civil society in Palestine has been documenting the companies' policies that impact the Palestinian people, including digital rights violations, exclusion from financial services, and censorship by social media platforms. Palestinian users have suffered from unjustified takedowns, account suspensions, and content censorship. Facebook, Twitter, and Google have largely declined to comment on their content-related decisions or generate any changes in their policies affecting Palestinians. Following rampant misinformation, hate speech, and calls for violence from both Palestinian and Israeli users, Facebook set up a round-the-clock "special operations center" to regulate content on the violence in Israel and the Occupied Palestinian Territories.

Beyond social media, platforms such as Google Maps have reinforced the erasure of Palestinian communities by failing to correctly label the territories on their platforms, an interviewee explained:

> *Maps always tell a story of the people, of a place, of a country. Google Maps sometimes disappears Palestinian villages and overemphasizes Israeli illegal settlements, which is considered under international law a war crime. Google assumes that you are an Israeli and not a Palestinian—there are roads that are for Israelis only that lead to Israeli settlements, so they are not accessible to everyone and can be life-threatening for Palestinians. Google Maps favors the Israelis.*

Palestinian civil society has repeatedly attempted to communicate with Google to address this issue, but has gotten no response. Organizations have run campaigns to resist the digital apartheid using petitions that have gathered over a million signatures. In addition, they have sent representatives to international conferences to further their efforts to communicate with Google. While the company provides an appointed person for Palestine, that individual's power to impact decisions is limited and engagement remains minimal:

Google is very difficult. They avoid our emails when we complain but when there are big international conferences, we speak with their representatives and their human rights representative. So we keep running after them, they're not responding, they're just supporting Israelis. Google has one representative in Palestine but she isn't the answer in many cases because she doesn't have a lot of power. There are offices in Tel Aviv but these are run by Israelis. We send emails to the CEO of Google. We did an email campaign and we have created Twitter storms around this.

The exclusion of Palestinians is also made apparent on digital payment platforms such as PayPal. The platform does not allow Palestinians to sign up with addresses located in Gaza or the West Bank, claiming the regions do not meet the service's regulatory requirements and represent too small of a market. The interviewee stressed that the company operates in other countries experiencing political unrest such as Somalia and Yemen, yet has barred its services on Palestinian territories. The organization's efforts to communicate with PayPal have failed to raise a response:

PayPal doesn't answer emails; they are even worse than Google. At least at Google they have somebody, everybody knows that she's there even if she doesn't answer emails. At PayPal this doesn't exist and this is very problematic.

There are more than 100 countries that PayPal works in; however, the official argument is that PayPal doesn't work in places that have political or civil unrest. They say that we are too small a market. Efforts were made to improve aspects of the banking system in Palestine in order to reach international standards; however, this did not help us get access to PayPal. For us, this is a political decision to not work with Palestine because, as a financial company, they should be happy to be part of any market.

These restrictions particularly affect young Palestinians, particularly freelancers who have no means of accessing payment for their work online:

Being blocked by PayPal means that many young people can't work as freelancers. As they are restricted in movement, [freelancing] can be a source of economic empowerment for them, but they are limited when they can't use PayPal.

There is no transparency in the decision-making processes of global companies that impacts the livelihoods and rights of communities in the Palestinian territories. According to the participant, social media platforms use a biased approach in their content moderation policies, without taking into account the consequences of operating in regions in conflict and under Israeli occupation. Besides the geopolitical bias, he identified language as yet another barrier in content regulation. Many unjustified takedowns occur for content in Arabic without any use of context, in particular through automated moderation. The participant added that names that may sound Muslim are also heavily targeted:

Some common words in Arabic have become keywords for immediate takedowns in the algorithms used by the companies. Basically, these companies do not have hate [a] speech lexicon in Arabic. And there's the whole issue of the terrorist organizations in the US that is very unclear. The latest list of individuals and dangerous organizations from Facebook was recently leaked and the large majority of names are from Muslim countries. The racism on these platforms is horrible.

In many cases, Facebook has removed content from Palestinian users under its Dangerous Individuals and Organizations Community Standard, which has proven to be extremely problematic for its ambiguity and vagueness. While the company has been repeatedly confronted by the Oversight Board, no substantial change has taken place. Consequently, Facebook has indiscriminately removed content in Palestine at the request of Israel's Cyber Unit, regardless of any association with terrorism. This includes ad campaigns and live streaming of crucial events, which has impacted the work of civil society organizations. During the protests against the Sheikh Jarrah eviction plans, Palestinians found many of their posts, photos, and videos removed from Facebook and their accounts blocked. While the platform recognized the error and said the posts and accounts would be reinstated, the deletions reportedly continued:

In 2021, there was an uprising in a certain neighborhood in Jerusalem and the Israeli government wanted to kick out Palestinian residents from their homes and put Israelis there. So the Palestinian people streamed this live on their social media and it caused a huge impact. There were Arabs from other parts of the world talking about it. But there is this phenomenon of shadow banning and social media companies were taking down lots of content. It was covered by mainstream outlets and there was a lot of pressure on the company.

Biased content moderation also occurs with other platforms. Instagram removed certain posts related to the Palestinian cause that had no association with violence or hatred. Twitter suspended Palestinian users based on information obtained from Israel's Ministry of Strategic Affairs. Civil society reported that in a two-week period, 500 cases of content related to Palestine had been taken down on social media platforms. In another 20 percent of the cases, Instagram informed the user that they would be removing content but did not provide justification. Nonetheless, engagement with social media companies remains higher than with other businesses, including the newest platforms such as TikTok and Clubhouse. The participants explained that it is largely due to the people-oriented nature of their platforms:

Responses are much higher from Facebook and Twitter, and usually their responses to us are positive. The dynamics with social media companies are very different from the other companies—they are much more [oriented toward] civil society organizations. Maybe because they are people companies and are focused on dealing with people, unlike PayPal or Google who are based on a different business model..

The name and reputation is very important for social media companies, and so engagement with civil society is very important for them to show that they are listening and they are attentive.

While a trusted partner of these companies enjoys regular meetings and communication, the participant emphasized that no substantial change actually takes place. Their organization has had small wins on a case-by-case basis but has not been successful in influencing global policies or the decision-making that takes place at the companies' headquarters.

Moving forward

- Meta should make its list of Dangerous Individuals and Organizations public.

- Meta should follow its Oversight Board's recommendations to conduct an independent investigation into content moderation in relation to Israel and Palestine. As such, this approach would help to determine if Meta's content moderation in both Arabic and Hebrew is being carried out without any bias.

- Form coalitions including local Palestinian coalitions with regional organizations, the international digital community, and the Palestinian private sector.

- Create a coalition of allies, organizations and civil society experts to strengthen their efforts and position vis-a-vis companies, helping to create substantial change. With more people, civil society can have more leverage to influence the private sector.

- Increase leverage with the social media companies through pressure from coalitions and members of civil society.

- Learn from the experiences of others in similar situations, such as in the case of Kashmir.

11. Paraguay

While digital rights organizations are relatively young in the Latin American region compared to their counterparts in Europe and the United States, their accelerated efforts and tactical approach have generated positive results and established transformational relationships with various sectors at the national and international level. The creation of Al Sur, a regional consortium of 11 organizations, has strengthened their work, magnified their impact, and created a robust agenda when approaching different stakeholders to meet their demands and needs.

Civil society organizations in Paraguay—a small country that endured a 35-year dictatorship, the longest-lasting authoritarian regime in South America, and still struggles with its most recently established democratic institutions—have been very strategic about their approach to communicating with private companies. They have established two routes of engagement with the private tech sector. The first partnership includes Internet Service Providers (ISPs), both nationally and internationally based, assessing companies' commitment to transparency and user privacy. Based on the Electronic Frontier Foundation's (EFF) "Who Has Your Back" ranking project comparing best practices, organizations in the Latin American region have adapted the methodology to the local context and realities. The approach aims to hold companies accountable to their users, particularly in regard to government data requests. The participants in the interview explained that using a points system based on selected criteria that creates competition among businesses has enabled their organization to establish a social lens for the project without any sense of threat for companies, furthering dialogue with civil society. With over five years of successful results with the project, the organization has seen its suggestions adopted and implemented by local and international ISPs:

What we suggest are international standard practices and greater transparency in terms of how the Paraguayan State requests information from the companies in a judicial intervention. So these things have changed over time for the better in the last three or four reports that we did with them.

To maintain its solid relationships with the companies, the organization ensures they have access to the report prior to publication. The companies can review the points they have received in different areas, suggest modifications, and send additional information to increase their rankings. The interviewees stressed that this collaborative approach has allowed for a healthy communication system between the two sectors in Paraguay, as well as in the rest of Latin America. As these companies operate in other countries in the region, a natural competition has emerged between the different branches of the same company to improve their rankings and report them to headquarters. The criteria vary per country to adapt to the capacity of the local team and enable the organization to accompany them in their progress and provide positive feedback:

In this process, instead of simply giving those scores to the company and telling them how much of a percentage of the initial commitment they have fulfilled, especially knowing there are no local regulations, we keep it to their discretion to decide if and how much they want to [hold a] company to the standards. This way, we seek to speak to the private sector to be able to have that conversation and for the changes that we, as civil society, are looking for.

Using collaborative tactics, the organization fosters a higher sense of responsibility in the private sector toward digital rights. The participant explained that using the approach set forth by the EFF, an organization based in the Global North, has helped their organization to communicate with private companies and increase its influence, particularly with international businesses with headquarters in the United States.

Being part of the regional coalition Al Sur has also supported the organization to have a stronger impact in the private sector, especially in its other types of engagement that include international tech platforms. The interviewees pointed out that Paraguay represents a small market and is thus of less interest to both ISPs and global social media companies. Thus, approaching the industries from a coalition perspective—generally during in-person meetings with social media companies—has facilitated communication and triggered more engagement. The platforms the organization has the strongest partnerships with are Meta and Twitter, which are the most invested in collaborating with digital rights stakeholders in the Latin American region. The relationship is affected by the particular issue addressed:

With Facebook, the most common exchange we have is on digital gender-based violence, everything that has to do with the dissemination of nonconsensual images, privacy, or personal data processing. With Twitter, it's a more general agenda; however, we are now working together on issues related to misinformation and intermediary liability.

For a general agenda on privacy, the organization engages with Facebook and Instagram during bimonthly meetings. However, for gender-related issues, it has a direct line with Meta's Latin American team, who can then redirect them to the specific professional in charge, both regionally or at the company's headquarters. A similar direct relationship exists with the policy team at Twitter, which grants the organization access to the global team if need be. When dealing with an urgent case, such as the digital security of an activist or journalist, the issue is addressed promptly, in a maximum of 24 to 48 hours. The organization uses a filter system to accelerate the responses of the companies:

When we receive the notification, there is a small methodology to see if it complies with the violations of the platform in order to give them the exact information, and as it has already passed through our filters, they respond much faster. But it always has to be the profile of a human rights activist or journalist.

To define who categorizes as an activist to ensure a timely response from the platforms, the organization provides the company with examples and further information on the nature of work of the attacked user as evidence. The engagement is quite distinct compared to other tech businesses that operate in the country. The participants stated that these businesses are not generally interested in countries like Paraguay, given its small market size, while they do invest in countries like Brazil (e.g., Uber and TikTok). Even a communication platform such as WhatsApp, which is the most widely used communication platform in Paraguay, does not easily engage with civil society. The participants explained the challenge was mostly due to the nature of the platforms, which limits the potential for content moderation. To overcome some of these shortcomings, the organization relies on its membership of Al Sur to communicate with the businesses and have access to their policy teams.

Nonetheless, some of the fundamental systemic limitations have inhibited a more transformative engagement with the private sector and the capacity for the organization to have a higher impact on digital rights, starting with the lack of transparency. The participants stressed that the transparency reports presented by the companies do not provide all of the necessary information and, more importantly, are not adapted to the context and capacity of the Global South:

> *There is no ability to translate the reports to the Global South. So they tell you we give you all of this data so that you can analyze it, but there is no capacity on the ground. We have to analyze so much information to see if it meets the transparency standards.*

By doing so, the companies have placed the responsibility on civil society instead of carrying out the work themselves. The lack of technical capacity on the part of civil society organizations prohibits them from knowing what information they can and should request or how they should analyze it, particularly when it comes to algorithmic transparency.

The participants emphasized that the contextual differences between regions need to be taken into account and the same model cannot be implemented across all countries, primarily when it comes to a small country like Paraguay. Together with the lack of technical expertise also comes the fact that digital rights organizations are young in Paraguay and in the rest of Latin America compared to those in the United States. Nonetheless, the interviewee explained that this is exactly why they have been more active on the ground and have had more local impact— attracting the attention and interest of private tech companies, predominantly through their collective efforts through Al Sur.

Moving forward

■ Lobby for localization and contextualization of transparency reports, in particular disaggregated data by country and algorithmic transparency.

■ Increase the transparency and accountability of the parts of the private sector we do not generally discuss, including companies that focus on contact tracing, AI, surveillance, and facial recognition technology and sell that data to third parties. Most are foreign companies and there is no information available to the public and no regulation from the government.

■ Call for greater accountability of digital intermediaries, especially on issues related to ad moderation and the remuneration of journalistic content on platforms.

12. Russia

Since the conflict escalated in Ukraine in early 2022, Russian authorities and multinational companies have blocked civilians in Russia from accessing the global Internet and further restricted access to information online. Most platforms have either suspended their services or been blocked by the government, adding to the existing heavy monitoring and censorship of the Internet.

While global media has turned its attention to the Ukrainian context, little attention has been given to the increasing challenges civil society in Russia endures. With heightened state surveillance, data leaks from a variety of Russian services have become more frequent, targeting civilians and activists in particular. The government uses technopositivist narratives to justify the use of oppressive technologies for the wider benefit of the public, demoralizing civilians and inhibiting any possibility for a free and open Internet. An interviewee stated:

> *Digital rights in Russia are even more fundamental now. People from NGOs, activists, journalists, and those from grassroots movements have become hopeless, with not much they can do about the repression and private companies. So thinking of productive relationships with tech companies is not feasible in Russia at the moment. Civil society takes the actions of technology companies for granted, believing that no other way is possible.*

Prior to 2022, the Russian social network Vkontakte was the leading platform in the country, with far fewer restrictions for users for social or political content compared to other companies. The participant stated that civil society also received more feedback from the company than from foreign platforms:

> *Facebook does not allow any political or social advertisement in Russia [or by] Russian accounts. [That's] an issue for an NGO that wants to promote an issue or information and cannot do it on Facebook. So they need to look for alternatives.*
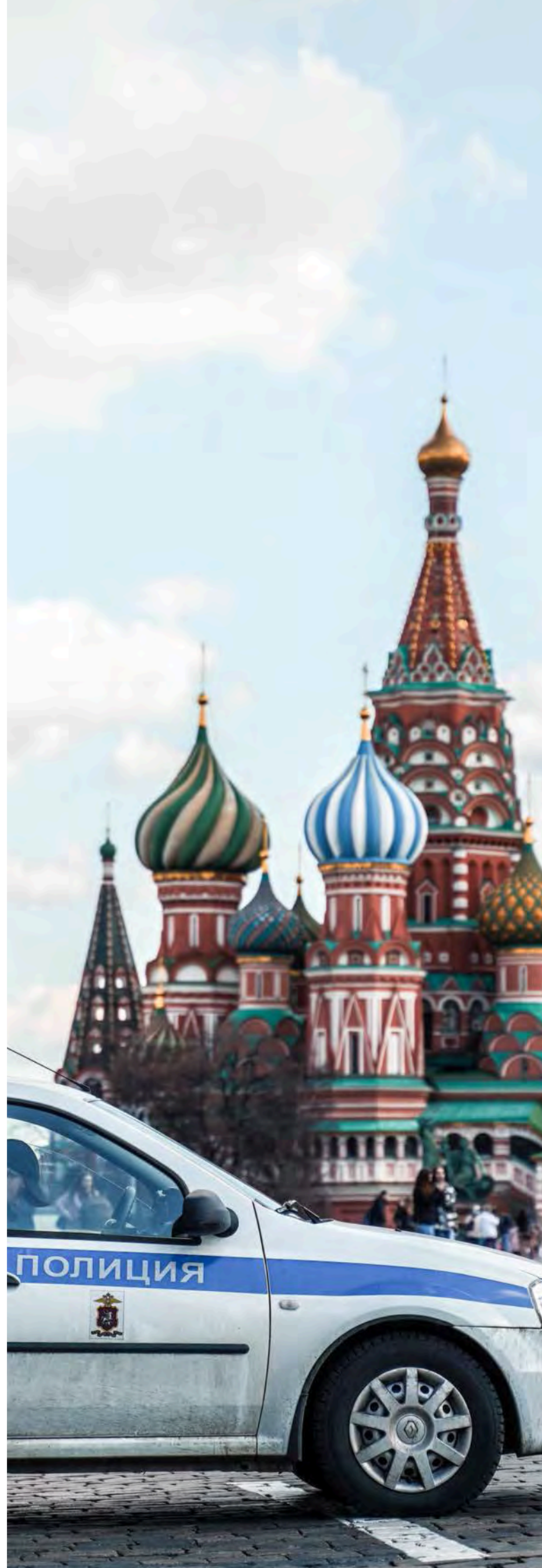
The lack of dedicated professionals posed an enormous challenge for developing a more meaningful engagement with tech platforms. In particular, grassroots organizations with no personal connections within the companies only receive automated responses and have poor or no contact with the platforms.

The issue with feedback from social media platforms is the same for all countries. It's automated responses, so there is no communication. We had an issue with Google accounts that were blocked due to a violation, but there was no response, just an action of blocking, no explanation.

It has been up to civil society to work to engage with the companies, as the companies have failed to establish a system of engagement. The participant explained that their organization has repeatedly tried to report a deep fake to Facebook, but no action has been taken by the platform. This poor engagement increases the risks for disinformation with the sharing and resharing of false content on leading platforms. Complex guidelines and reporting channels further discourage users from engaging with platforms.

Our interaction with global tech platforms is communicating with robots —auto-replies, links to the endless lists of unclear written rules with no clear feedback. It's tremendously time-consuming, often with no results.

US tech platforms provide no explanation when content is removed or an account is banned, according to the participant. When a response is provided, the company simply refers to a long list of rules without any clear reason and with no possibility to appeal. As many civil society actors are unaware of the engagement tools and support products offered by companies, many do not seek to reach out to the platforms. Capacity limitations in technology and the nature of many grassroots organizations often lead to stalled communication with companies and further restrictions.

Additionally, many civil society organizations chose not to register formally as nonprofit entities in Russia to avoid unnecessary attention from the state and added restrictions, and therefore do not receive support or access to the private tech sector, including the privileges associated with holding trusted status with the big tech platforms. Heavy state monitoring inhibits any participation in international digital rights conferences such as RightsCon or IGF where many relationships with the private tech sector are established.

Language is one of the main barriers to meaningful communication with tech companies. Only 10 percent of Russians speak English, the default language used for engagement with the private sector. Tech support is generally offered not by Russians but instead by Russian speakers who are not versed in the local realities. Support content and community guidelines on the main platforms are often not available in Russian, limiting access to information and services for civil society:

Speaking the same language is not enough without understanding NGOs' and activists' realities and work models; under an authoritarian regime, it can be dangerous for us. The translation of services is also an issue and we try to deal with it by doing the translation ourselves, as [that] can help to circumvent censorship. But [the platforms] can also help us to have access to services, compensation, consultation, and more. We are isolated without communication.

Though many foreign companies have removed their services in Russia, many users find alternative ways to continue to be active on the platforms (e.g., opening bank accounts in neighboring countries to pay for services). The participant stressed that those means are limited to those who can afford them and those who have the technical skills to circumvent the bans. Translations are still needed to minimize harms and avoid the complete isolation of Russian civil society from the rest of the world. TikTok, for instance, has become more popular among activists.

The company faces less restriction from the government, feedback is provided in Russian, and adverts are permitted, enabling civil society to communicate. Given that the risks are higher on Russian platforms, civil society organizations still opt to use non-Russian services when possible. Nonetheless, Telegram has become the most popular platform since the conflict started, even though the company has extremely poor moderation strategies:

Violent content has been circulating on Telegram, but there has been no response from the company, or [it] just said that it is the duty of channel owners to moderate content.

The Russian government has been heavily advocating for the use of non-US products and promoting Russian and Chinese services. State surveillance and data breaches have limited the number of users on national platforms, particularly with recent data leaks on activities and information on the purchase of foreign services. Internet speed has also been highly reduced and prices for connectivity have soared, limiting activities online for the large majority of Russians. Additionally, the supply of services necessary to bypass the restrictions does not meet the demand, erecting a digital wall between Russian users and the rest of the world. As a result, disinformation campaigns targeting Russians have also been on the rise.

Moving forward

- Provide live support for civil society to connect to and obtain responses from professionals knowledgeable and interested in the Russian context, not robots (receive meaningful feedback). Civil society requests are now lost in piles of reports.

- Establish tech support for every country with professionals from that country and with understanding of the local context and realities.

- For countries that are under sanctions, provide customized support and products that can help circumvent restrictions and surveillance (e.g., extra resources for moderation).

- To minimize the risk of disinformation, ask users to check content before posting (similar to Twitter).

- Build technical capacity for grassroots organizations to level the inequality in access to support and services of platforms. Offer free online and offline courses that are accessible and localized. Help people to understand the benefits that tech companies can provide, to get to know each other, and to share successful practices (more skilled actors can help the less experienced and create a cross-country exchange).

- Utilize the data provided by civil society and analyze it to offer adequate solutions.

- Provide simple off-the-shelf solutions to implement in the everyday work of NGOs rather than complicated procedures.

13. South Sudan

South Sudan became one of the youngest countries in the world when it became independent in July 2011 after over 20 years of civil war. However, despite its newfound independence, the country has been falling in and out of armed conflict and struggles with numerous attempts to broker peace. The long-standing conflict has destroyed South Sudan's limited infrastructure, further collapsing its economy and triggering a high dependency on imported diesel to meet its energy demands. As a result, access to digital infrastructure remains among the lowest on the African continent, with a little over 10 percent of its population being online.

Civil society engagement with tech platforms in South Sudan is determined by the Internet penetration and available infrastructure in the country. The participant in the interview stressed that it becomes extremely challenging to make any requests from the companies and to keep them accountable when basic needs are not met and little to no research has been done. Providing the example of neighboring Kenya, he explained that the fast growing digital progress and high engagement with the platforms there is not due to the companies' good intentions but rather to the country's high Internet connectivity and its use by a large, young middle class. In contrast, South Sudan's lack of infrastructure has allowed international platforms like Facebook to take over the digital gap and become the Internet:

> *Facebook is the Internet. You can't just shut down Facebook; people use it, they have to use it. It's their gateway to the Internet. Facebook is investing over one billion dollars in subsea cables to address the Internet issues on the continent. They are conquering the whole of Africa, and that means that in less than three years, Facebook will be the biggest Internet provider on the continent. How can we compete with this?*

With the expanding power of Facebook in the region, South Sudanese civil society has found itself powerless and with no leverage to negotiate or collaborate. The absence of data that would equip organizations with evidence on user experience including the trends, successes, and failures of products and services offered in South Sudan presents yet another hurdle for more efficient communication and relationships with businesses. Access to information and recommendations by local experts, such as content and products made available in African languages, could help to better address issues of digital safety and content moderation, particularly in volatile regions with weak democracies, such as South Sudan.

However, there is a disconnect between the United States where the decisions are made and products are designed and the countries on the African continent where the company deploys its services. The Western-centric approach used by the private sector without engaging with local communities prevents its technology from being fully scalable in these regions. The cash economy in South Sudan means that users often do not have the resources to purchase products online. Payment systems that are not adapted to South Sudan—e.g., they request a zip code—further limit the use of services. The investment and support systems provided by the company are proportional to the market size of the country:

The products of these companies reach more places than they're willing to support. So this leaves a very big gap, where the kind of products and the user base is growing, but the support is not given. The revenue per user is small in South Sudan, so they don't care about countries like us. They even group a bunch of us in stats for the MENA because the revenue per user is not high. Their priorities come from a financial perspective—they give support in countries that bring them more money.

Political restrictions also impact engagement. Until recently, South Sudan had been on the list of countries supporting terrorism for nearly two decades. Although the country was removed from the list in 2019, users were not able to access many online products, particularly from Google. The interviewee's organization reached out to Google to address the issue, but received a standardized response and no change was made. As a result, millions of people are excluded from services that are essential to daily life. The growing number of young South Sudanese entrepreneurs are particularly impacted by these bans.

So entrepreneurs in Sudan, and young people who are doing YouTube videos, in order to monetize their channels would need to set up an account outside the country. It's monetized outside the country, and then it comes back to them somehow.

Until recently, global platforms had no appointed person in charge of the region that organizations could reach out to. The participant gave the example of Facebook, which only had one expert based in Nigeria and another in London, with ad hoc visits to neighboring Kenya but never to South Sudan. While its team has grown exponentially in the past couple of years, the tendency remains to group countries by region without any discrimination based on context, language, or needs.

These companies are faceless. Somebody in an office in Nigeria or London would not know of the realities in South Sudan. They now have someone who is Africa-focused but per region. They put us in groups as if we were the same. They even call it Africa and the Middle East—tacky and very strange.

With Facebook's increased presence on the African continent, the participant affirmed that civil society has a much better chance of engaging with the company. However, there remains a need to address how these engagements are taking place, document their impact, and identify the key takeaways. Engagement, including communication method and response time, also varies depending on the company in each country:

Some of the biggest challenges are contact and response time. Many of the organizations, like Twitter, don't have an expert or a civil society channel established for organizations. So most of the time, if I want to reach out to Twitter, I have to reach out to a generic reporting system. No priority is given and our messages are not dealt with any degree of urgency or intent in this part of the world. So that becomes very frustrating.

When I go to folks on the ground and tell them, hey, we reach out to Facebook, and they're like, Who's Facebook? How can you talk to Facebook? How can you talk to Twitter? Unlike people in the West in New York or San Francisco, where you could reach out to someone who knows someone there. So that makes the initial point of contact very difficult.

The participant attributed many of the current engagement efforts to marketing masqueraded as support. The poor investment of resources is directly proportional to the weak engagement and lack of inclusion of local communities in South Sudan in the decision-making process.

Some platforms have inclusive policies, others don't. The more inclusive you want to be, the more resources you need to spend. You can't just have a blanket cover over the problems. You're seeing tech companies with someone at a desk somewhere in East Africa and nothing happens.

Distrust of the global platforms has grown due to the inconsistency of their interventions with civil society. Out of the few projects carried out by companies in the country, many were left incomplete, resulting in an even greater disconnect with civil society. In addition, with no structured approach to communications, efforts to engage generally came from civil society through personal contacts:

One of the things we wanted to do with Google [was] skills for journalists, like really teaching journalism, how to do Advanced Search and stuff like that. So I reached out to a friend who knew someone who was a fellow at Google. Then the person was able to come in and provide some training. But then halfway through the training, he bailed out. And that was it, there was no way to reach back and establish contact.

Nonetheless, some improvements have been made based on communication efforts and feedback provided by civil society. The participant gave the example of Slack, which was blocked in South Sudan until recently. Their organization contacted Slack to request its services be opened in the country after South Sudan was no longer under embargo:

So I sent them an email, actually, with links to the US Treasury, listing the countries under embargo, and it took them like three days or so to remove the ban. And thanks to yours truly, it was [opened] for the whole of South Sudan.

Smaller businesses in South Sudan appear to have better engagement with civil society, according to the participant. The organization has been able to complete a data story on visualizing hate speech and harmful content in collaboration with a software company that shared the project on its platform and provided substantial feedback. The participant emphasized that the focus should not only be on the will and efforts of the private sector to engage. With increasing distrust toward international companies, it is also necessary to provide incentives for locals to engage.

Moving forward

- Document how engagement is taking place in each country, with details on what has and has not worked, evaluate the impact on communities, feedback, responses, and make that information public.

- Create a global, or at least Global South, tech inclusion index published on a yearly basis that will document how the private tech sector engages with civil society in each country (as you cannot compare South Sudan to Kenya, for instance). The index should also include a scoring system that assesses accessibility to the platforms in terms of communication, products, inclusion, physical locations of the companies in the country of operation, representation of the local people in the company, ability to engage with local communities, etc.

- Set up research design labs in Africa: localized and contextualized research carried out by Africans in each country that documents trends, patterns, what has worked, and statistics. The research would make it possible to increase engagement and apply pressure on the companies to be more accountable.

14. Sri Lanka

Anti-government protests throughout Sri Lanka made international headlines in 2022 as a result of a devastating economic crisis and rising inflation, eventually leading to the resignation of the president. In an attempt to curb the demonstrations, the government requested restrictions on social media, including Facebook, YouTube, TikTok, Twitter, and WhatsApp.

Shutdowns and limited access to digital platforms have been a frequent occurrence in Sri Lanka in recent years. The country has witnessed a series of violent events and political instability that highlighted the role of popular digital platforms in the dissemination of hate speech and intensification of conflict. Evidence suggested that hate content and misinformation on Facebook targeted toward the Muslim community led to fatal unrest and rising violence during the anti-Muslim attacks of 2018. The hate discourses spread to other towns throughout the country and had repercussions that lasted through 2019. The critical situation led the Sri Lankan government to declare a state of emergency and ban access to Facebook, WhatsApp, Instagram, and Viber.

While Facebook recognized its role as a perpetrator in the deadly conflict, the company's responses only came after international pressure and media coverage. The same was true for other platforms such as YouTube, which started to monitor its content following the 2018 events. The companies allocated further resources to Sri Lanka, including expanding their trusted partner programs to include local civil society organizations. The interviewee explained that as a result, their organization's efforts to monitor social media for harmful content became more relevant. The organization developed a methodology to detect dangerous content, monitored by its analysts, who record detected content in monthly, quarterly, and annual reports. The approach allows the organization to notify tech platforms to take action and monitor their responses, which is further facilitated by the organization's status as a trusted partner of Facebook, YouTube, and TikTok:

We record how many things we reported to the social media companies and their response, like how many did they take down, how many did they say do not violate their community guidelines, and the time [taken] to respond. Sometimes they respond fast and others only after one or two months.

The feedback provided by the organization has helped companies mitigate some of the possible harms, particularly after the 2018 attacks. The participant reported that Facebook improved its content monitoring in local languages as well as its operations and support systems following the tragic events. Nonetheless, responses from the companies remain inconsistent and take place on a case-to-case basis:

The problems we have, specifically with Facebook, is the time taken to respond is very inconsistent. In some cases, they respond within one day, and in others, they will take up to two to three months. On average, it will be 20 to 30 days, which is absurd. The harm of that content would already be done.

Although Facebook has been the most engaged with civil society in Sri Lanka and—unlike other platforms—responsive to queries, attending civil society events, and open to new ideas, the participant stressed that no substantial change has actually taken place within the company:

If we want to take down a content or account urgently, we can always reach out to them on a personal level, they are very available for that. And they've asked us to do so. They always attend the symposiums, conferences, and all, but nothing gets changed on a policy level.

The organization submits its content and account-related requests by email for Facebook to respond to, often in batches that include upwards of 15 cases. For more immediate concerns, it has direct access, including the team's mobile numbers.

Nonetheless, the lack of a structure of communication and transparency inhibits transformational change and more efficient engagement with companies. The participant attributed this deficiency to the limited categories and unclear guidelines in the reporting process made available to users. No explanation is provided after a decision has been made following a request. The organization often has to manually check if the content reported has been taken down.

The inconsistent and slow responses became more prevalent during the pandemic. The interviewee pointed out that they received an automated message from Facebook justifying the delays in feedback during that period, highlighting the lack of interest and intent in improving its engagement with civil society. YouTube on the other hand was faster in its responses and displayed them on its dashboard, making the process more efficient. The platform's increased engagement is largely due to a higher number of users on their platform—people had more time to watch videos and create new content, as per the participant's account.

The limitations of automated moderation—which Facebook heavily relies on—has created significant barriers in addressing harmful content on digital platforms. Current models lack local context and the ability to moderate in local languages, presenting a bigger threat in communities affected by violence. Evidence has also shown that AI focuses on polarized content and can become a catalyst for increased conflict, "because the algorithms show us what we like to see," as reported by the participant. The organization has tried to advise the companies on their design and implementation of automated tools; however, it has not received much feedback or further information on the companies' processes.

To increase its influence and apply pressure on tech companies, the organization has leveraged its membership in regional and global networks and its relationships with partners, particularly during the pandemic. The status of the organization as a trusted partner facilitates the communication process and enables it to serve as a bridge between individuals and other civil society organizations and the private sector. It often receives requests and complaints from third parties and intervenes on their behalf. Its role as an adviser with the platforms also helps to impact the decision-making process:

For some cases, Facebook comes to us when they receive a complaint that they can't verify or are uncertain about. They reach out to a few of the trusted partners in Sri Lanka and ask us to assess the situation. What do we think about this? Should this content be online? Or should it be taken down? On some occasions, they send us the content and ask what our thoughts are and also [to] help them report an individual case through our channel. Not everyone has access to social media companies, only trusted partners.

In a more recently developed relationship with TikTok, the organization has established a more systematic way of reporting. The participant described that trusted partners are guaranteed a response from the company within 72 hours, which has been fulfilled up till now. Having structured communication with companies has proven to be extremely effective for civil society and an important component of what they need. Rather than the organization reaching out to the company to request to be a member of the trusted partners program—as it had done with YouTube and Facebook—TikTok contacted the organization to invite it to join and asked for its help to moderate content. Nonetheless, while the organization expanded its methodology to include TikTok, the participant noted that the content is often shared on other platforms, further complicating the monitoring process.

Other platforms are also used in Sri Lanka, such as Twitter and Instagram. However, the organization has not identified any significant harmful content, unlike the case with Facebook and YouTube. The participant stressed that Facebook has become the Internet and the culture, particularly in rural areas. In his words, "village dwellers would know of Facebook but not of the Internet."

The efforts of civil society would be more significant if paired with national policies and enforcement by the Sri Lankan government. However, in the absence of registration in the country, the multinational companies cannot be held accountable to comply with state legislation. Furthermore, a local team within the company with contextualized knowledge of Sri Lanka would also improve and increase engagement with local organizations.

Moving forward

- Increase their engagement and consultation with civil society: feedback provided by tech experts in Sri Lanka led to changes, for example the small notification on a message on WhatsApp that has been forwarded too many times.

- Improve performance of trusted partner channels, commit to clear targets for response rates and provide transparency on performance.

- Explore possible efficiencies in trusted partner reporting across platforms, reflecting the reality that both partners and content are often shared.

15. Taiwan

For Taiwanese people, Facebook and Line play a significant role in their daily lives, with 90 percent of the population being users of their platforms. The popularity of the products has turned them into the largest drivers of misinformation, particularly with the most recent rising tensions between Taiwan and China. The Taiwanese government's handling of the pandemic, with a sharp rise in deaths and infections in 2021, resulted in a growing distrust of the state. Taking advantage of the shifting circumstances, China used information operations targeting Taiwan to attack the state and disseminate misinformation.

The dominance of China over Taiwan and the political situation between the two countries has meant that civil society has had little to no power over the content on Chinese social media operating in the country, such as Weibo and WeChat. The same is also true for Chinese entertainment widely consumed in Taiwan, a shift in the industry that took place over 15 years ago with a great impact on users on YouTube. According to the participant in the interview, there are no regulations to moderate content produced on Chinese platforms and by mainstream media, even when streamed on other non-Chinese social media:

> *There're a lot of Chinese TV shows or public content from China and we have no policy or regulation that can prevent those things. With that, YouTube [user numbers] are also getting higher and higher, especially with viewers of Smart TV. It's kinda like traditional TV is fading away. Even for senior people, if they have a smart TV, they also watch YouTube.*

While not dominating the industry, Chinese apps are still prevalent among the Taiwanese. The similarities in the culture and language particularly appeal to the elderly and young people below the age of 25, based on the account of the participant. During elections, that consumption increases as most political content is produced by China and shared on different platforms.

Although false information can generate the same message across various channels, its impact—both on the general public and how civil society organizations address it—differs based on the platform that hosts it.

Some of the earliest engagement with the private tech sector began with issues regarding child protection, mainly led by children's organizations and conservative groups. The participant explained that civil society developed a self-regulating mechanism that would report harmful content to the companies through a direct channel. Nonetheless, engagement practices shifted during the political elections in 2018, with rampant misinformation and Chinese propaganda on social media platforms.

So, in 2018, there is a lot of disinformation with the election of the city mayor, including content on Taiwanese identity, anti-LGBT rights, etc. That's when people start to look into fake news and disinformation and whether Chinese agents support those activities. And when we start to witness more fact-checking initiatives and build a more direct channel with social media platforms, along with Facebook, Google, and so on, we start thinking about how we do more research and get the resources to understand cyber activities from China during elections.

In its attempt to influence the 2018 elections in Taiwan and target political content, China launched many websites with similar political messages that were in sync with a variety of fan pages and groups on Facebook. The participant pointed out that many of these fan pages were popular with the Chinese diaspora, who are particularly keen on spreading patriotic content and attacking Taiwanese politics. The organization and other civic tech groups would detect many of these pages on Facebook and report them to the platform.

With an office in Taipei and a public policy point of contact easily accessible to organizations, Facebook has been the platform that is most engaged with civil society. The company has made a direct line of communication available on its app for trusted partners with responses within 24 hours. Through its fact-checking tool, the platform also enables civil society to report false information and dangerous content. To avoid repeating the same mistakes, the company took a more proactive role during the presidential elections in 2020 by creating a "war room" to counter misinformation and interference ahead of voting day. The participant attributed this change on behalf of the platform to both the Taiwanese employees who were advocating from within the company and pressure from civil society to allocate more resources ahead of the national elections:

So they would do takedowns, they would do downgrading, they would do lots of investigation on fake accounts and delay or suspend those fake accounts, and then they opened up more of their database to researchers, especially independent researchers in Taiwan. So yeah, we do have a good experience.

While Facebook has opened dialogue with researchers and engages with civil society on a regular basis to detect harmful content and misinformation on its platform, the participant stressed that it is still not doing as much as it could. A lack of transparency still remains with the process of selecting the stakeholders that take part in the "war room" and how and who has access to specific information. The participant emphasized that it was also unclear if the company shared any information with the government. As a result, the organization will be creating its own "war room" in light of the upcoming local elections with increased transparency and using a multistakeholder approach.

Other platforms such as the messaging app Line have also been involved in addressing false information. The company launched educational projects on information literacy for its users to detect common forms of misinformation on its platforms. Through its chat bots, users can fact-check by forwarding the information to the bot and receiving feedback. The participant explained that the answer is actually generated by volunteers and various civic tech groups, who also hold media literacy programs for communities with a focus on the elderly in an attempt to raise awareness about misinformation and how to address it. On the other hand, hackers have created their own open source tools for fact-checking that complements the research carried out by the organization. The interviewee stated that companies like Google have invested in researchers and organizations in Taiwan carrying out fact-checking to increase capacity:

YouTube, for instance, uses an approach that is more about if they trust a researcher and this researcher reports malign [content] or a suspicious channel and they just shut down the channel. YouTube has less resources to have their own researchers do the work, compared to Facebook and Twitter.

Line has had a completely different approach. While it has an entire team in Taiwan, including its development and public policy experts, and strives to show it cares about content-related issues, both to its users and the government, it remains conservative about political matters and its responses are generally slow. The interviewee added that the company uses the encrypted nature of the messaging app and its emphasis on users' privacy to justify its lack of intervention to address issues of content on its platforms:

Line emphasizes they are an encrypted messenger platform, where they value the user's privacy. So they tell civil society and government that they cannot do anything for those messages because they belong to the people, even if they are spreading inside, let's say, a 2,000-people group.

We tried a lot to actually tell them that there are a lot of things they can do without violating users' privacy and stop those messages from spreading widely. But they are really slow.

To boost its tactics and strategy for a transformational engagement with the private tech sector, the organization relies on the impact of collective action. As a member of the Next Billion Network and the Digital Rights Network, the organization exchanges tactics to create more transformational relationships with the private tech sector. It also utilizes its network among local and regional fact-checking initiatives. The collaboration between countries in the region was at its highest during the early stages of the pandemic, with an increase in misinformation stemming from China, highlighting the role of the fact-checking community in Southeast Asia. Additionally, its trusted partner status has enabled the organization to further its work in digital rights in Taiwan both through the government, with other civil society organizations, and in its engagement with the private tech platforms. As a result, it has had more access to information to advance its research, increased transparency, and gained access to a variety of assets made available by Facebook.

Moving forward

- US policymakers should increase regulation of US-based platforms, particularly relating to their operations in other countries. With their efforts to increase democracy worldwide, they should be responsible for the US companies that are currently supporting authoritarian regimes and impacting human rights in other countries.

- Hold the Taiwan Facebook branch accountable for content disseminated in the country and abide by Taiwanese law. The current branch is only responsible for its advertising department, and does not moderate content on its platforms, including in ads.

- Special attention and regulations should apply to small countries like Taiwan, as they represent a small market and are of no interest to the multinational companies, creating a power asymmetry and a barrier to negotiating policies to regulate these platforms.

- Other countries should unite to address similar issues in other smaller markets. Unlike in the EU, there is no GDPR (data protection legislation) implemented in Taiwan. Australia has been able to put pressure on tech companies to pay for news content. The Taiwanese government does not have the same negotiating power to compete with these countries and relies on collaboration with other countries and networks. This is why the EU and the US should adopt and enforce more policy to control global tech platforms and keep them more accountable for business information, the transparency of their operations, their collaboration and relationships with harmful actors, etc.

IV. Follow-on Actions

Develop an industry framework for stakeholder engagement

Effective partnerships between the private tech sector and civil society require a systemic industry framework for engagement that is shared and consistent, whilst allowing for responsiveness and adaptation to very different contexts. Documented industry standards, even if voluntary, would provide stakeholders with clear expectations about how such engagement should take place.

Development of an effective and widely acceptable industry framework for civil society engagement will itself require a collaborative and consultative process involving companies and global stakeholders. A process which was initially civil society led may be best placed to succeed, and should be a focus of multilateral forums and collective advocacy.

Establish a company focal teams and sustainable points of contact for each country of operation

Civil society needs a consistent channel of communication to company representatives who possess contextual understanding, cultural competency, and relevant linguistic skills. For global companies a team or representative for each country with a meaningful userbase should be a minimum requirement. For fragile and conflict-affected regions in particular, companies should increase their investments in local teams who are knowledgeable of the sociohistorical and religious realities and put the necessary measures in place to minimize harm.

Include local expertise in decision-making

Prior to making concrete decisions that can impact the entire globe, companies must include experts from each country and a system that harnesses the expertise of each region. In many instances, consultations with civil society have yielded feedback that led to changes to the companies' products and policies (e.g., the tech experts in Sri Lanka providing the idea to limit the forwarding feature on WhatsApp, which helps to mitigate the risk of the spread of misinformation on the platform).

Provide compensation for consultation with civil society, and establish standards for doing so

Civil society has long served as an "early warning system" bringing awareness to tech companies and policymakers of possible crises with extremely low to no resources while trying to adapt to the fast and ever-changing nature of technology. Organizations, activists, and academics are often requested to share their expertise and provide feedback during meetings and consultations that benefit businesses while not getting compensated for their time. Companies need to acknowledge the value brought by civil society and the important role they play in mitigating the harms of the implemented technology and ensure they provide adequate compensation for their knowledge and time.

In order to make this process transparent and fair, companies should establish their own standards for compensation for consultation, which clearly lay out when compensation should be expected and how it will be determined. These should be developed in consultation with stakeholders and made available to partners and prospective consultees. Clear information about the use of non-disclosure agreements should also be included in these standards.

Provide greater transparency

Private tech companies must provide greater transparency on their operations and content moderation processes, whether through the use of professionals or algorithms, including how content is assessed. Civil society needs to be provided with greater knowledge on the internal structures of the regional and global platforms, their practices and how they are implemented, and how organizations can influence those processes. Local organizations need to know how each country office operates, as well as the complex structures of the headquarters and how to access the various support teams of tech businesses.

Transparency reporting must be localized and disaggregated by country and language rather than presented in global aggregate as is current practice. Reporting the volume of hate speech removed globally does not provide accountability to civil society in Sri Lanka or Ethiopia - reporting the same information for specific countries would remedy this and generate meaningful data for use by those trying to prevent harm.

Make tech support available in each country and in local languages

Companies should provide technical support in the languages—at the minimum in the lingua franca— of each country in which they operate. As context is central to the interpretation of language, distinctions should be made between the different applications of the same language across various countries (e.g., the Arabic lexicon in South Sudan versus the Arabic lexicon in Lebanon).

Provide contextualized courses for local actors

Customized and contextualized free online and offline courses made accessible to civil society in each country would enable users to understand the benefits and support that tech companies can provide and to assess successful practices, helpful tools, and products.

Fill the gap in research using a more contextualized and intersectional approach

The current poor understanding of the uses and impacts of technology in a variety of contexts, in particular in fragile settings (conflict regions, authoritarian regimes, vulnerable groups, racial-ethnic inequalities, etc.), has amplified the consequential harms and inhibited the creation of transformative partnerships with civil society. Systemic, context-specific, and people-centered research producing data that is intersectional (differentiated by race, ethnicity, age, gender, etc.) would enable more structured and consistent engagement and collaboration with local civil society. More in-depth research on the operational procedures of platforms in each country, how data is retrieved, what data is made public, and what products are provided can form the initial steps toward more sustainable policies. Additionally, using a bottom-up approach would establish trust, improve coordination, and balance the power dynamics between stakeholders.

Create an independent global multistakeholder coalition

Companies should take part in the creation of an independent global coalition using a multistakeholder and multilayered approach that would include regional organizations (both at the grassroots and national levels), the international digital rights community, the private sector, and government representatives. A stronger coalition with stakeholders representing all the different sectors and strata of global communities would result in greater influence, increase leverage to keep companies accountable, and help to balance the unequal power dynamics between the private sector and civil society, particularly in smaller markets and fragile contexts (e.g., Belarus and Palestine).

Build an autonomous cohort of experts with decision-making power

An international organization should create a completely independent and autonomous body of experts using a multistakeholder approach, including big tech representatives but as a minority. As such, it would be a system outside of the companies where decisions will be made and justification will be provided for each recommendation based on actual data.

Create an alternative reporting system

Companies should collaborate and select respected experts from different sectors, with one set of professionals who would document cases of users who have tried to report harmful content across different platforms, and another set examine and analyze the data. This model would offer alternatives to the current reporting system while continuing to provide prototypes for other approaches. In parallel, companies should support the creation of an inclusive system where technologists, designers, and community members redesign the current reporting mechanisms and publish the outcomes.

Rethinking the design of current platforms

Tech businesses should participate in creating a group of experts to provide feedback on the design of platforms (e.g., if you had to redesign this platform, what works, what does not work, etc.) and provide prototypes. As such, the experts would demonstrate the standards and alternatives to the different ways these platforms should and could be operating and rethink the ways civil society currently operates and engages with them. To continuously evaluate the efficiency of proposed solutions, companies should implement pilot projects in parallel where a subsection of users would test one of the ideas, analyze its impact, what has worked and areas that could be improved.

Acknowledgements

We are grateful for the time and contributions of experts who shared their experiences and views, and helped to inform, advise and guide this research effort. We have maintained the anonymity of the participants in this study to ensure their protection and respect their privacy, particularly in fragile and conflict contexts.

This report was researched and written by Niousha Roshani, a multi-sectoral expert practitioner in technology, business and human rights addressing the inequality gap between companies globally and civil society.

In her current and past roles, she has advised governments, NPOs, universities, and the private sector on digital entrepreneurship, innovation and conflict resolution, on gender and digital media (LAC and Africa), on childhood and media (LAC), on race, disability and digital rights (USA); on tech + policy (SSA, LAC and ME); addressing dis- and misinformation online and best practices for the new economy (Europe, Africa and LAC).