PARADIGM INITIATIVE

AN ADVOCACY TOOLKIT
On Internet Freedom and Internet Intermediaries

An Advocacy Toolkit on Internet Freedom and Internet Intermediaries

June 2022

Authors:
Bulanda T. Nkhowani, Senior Programs Officer, Paradigm Initiative
Rigobert Kenmogne, Programs Officer, Paradigm Initiative

Editors
Thobekile Matimbe, Community Manager, Paradigm Initiative
Nnenna Paul-Ugochukwu, Chief Operating Officer, Paradigm Initiative
Leandro Ucciferri, Global Partnerships Manager, Ranking Digital Rights

Design & Layout
Kenneth Oyeniyi, Communcations Assistant, Paradigm Initiative.

PARADIGM INITIATIVE   @ParadigmHQ

Introduction

In recent years, there has been a growing movement to hold technology companies accountable on their human rights practices, particularly on how their business models impact individuals and communities. The United Nations' Guiding Principles on Business and Human Rights set the standards and mandate all businesses, regardless of sector, nature, or size, to respect and remedy any potential human rights abuse in the course of their operations. Through the "Protect, Respect, and Remedy" framework, the guiding principles set guidelines for concrete and actionable steps for government and companies to ensure their respective duties and responsibilities to prevent abuses and protect human rights in service provision.

As digital technologies and the internet become increasingly accessible, the need to assess, remedy and provide a platform for dialogue with businesses on potential human rights violations among service providers, governments and users has become vital. This toolkit is one of the first attempts to produce a resource to support human right defenders and partners in Africa in their advocacy efforts on corporate accountability engagements with Internet intermediaries. Through this toolkit, Paradigm Initiative (PIN) seeks to highlight tools and ways in which organisations can assess human rights practices and respect for internet rights by Internet Service Providers.

To achieve this, PIN partnered with Ranking Digital Rights (RDR), an organisation that works to promote human rights online by studying the most powerful technology companies around the world and their commitments to respect the rights to privacy and freedom of expression.

> PIN works to provide digital opportunities to young Africans and promote digital rights and human rights respecting legislation and policies across Africa. Internet freedom advocacy is a vitally important part of PIN's mission to connect young people to digital opportunities by promoting a human rights respecting ICT policy environment where innovation thrives.

Definition of Terms

Internet Freedom

Refers to a basic set of internet-related human rights such as "privacy; freedom of expression; the right to receive information; various rights protecting cultural, linguistic, and minority diversity; and the right to education".[1] Other examples of Internet freedoms include the right to association and assembly online and access to the Internet. The term Internet Freedom is closely linked to Digital Rights and can be used interchangeably to mean human rights that in the digital age that are enjoyed using online platforms or digital means[2].

Internet Intermediary

Refers to "an entity which provides services that enable people to use the internet, falling into two categories: (i) conduits, which are technical providers of internet access or transmission services; and (ii) hosts, which are providers of content services, such as online platforms (e.g. websites), caching providers and storage services".[3]

The following are examples of internet intermediaries:
- Network operators such as MTN, Orange, Unitel, Vodacom, Econet, etc.
- Internet Access Providers, such as Mweb, Skyband, Africa Online, etc.
- Internet Service Providers, such as Liquid Telecommunications, iBurst, Orange, etc.
- Network infrastructure providers: such as Cisco, Huawei, and Ericsson.
- Content Delivery Networks: such as Cloudflare, Fastly, Azure CDN, and AWS CDN.
- Social network websites: such as Facebook, Instagram, Twitter, LinkedIn, TikTok, and Snap.
- Search engines: such as Google, Yahoo, Bing, and DuckDuckGo.

From the above definitions and examples, internet intermediaries do not include content producers. In a 2010 report, the Organization for Economic Co-operation and Development (OECD) explains that internet intermediaries 'bring together or facilitate transactions between third parties on the Internet.[4] They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."[5] Therefore, we engage with Internet intermediaries as they are essential stakeholders when it comes to promoting Internet freedom.

1   Kuburlija, J. (2014), An Introduction to IG, 6th Edition, Malta, Diplo Foundation.
2   Association for Progressive Communication, What are Digital Rights, https://www.apc.org/en/news/co-conet-what-are-digital-rightshttps://www.apc.org/en/news/coconet-what-are-digital-rights (accessed 24 May2022).
3   Media Defence, What is an Internet Intermediary? https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-2-introduction-to-digital-rights/what-is-an-Internet-intermediary/ (accessed 21 March 2022).
4   Karine Perset/OECD. March 2010. The Economic and Social Role of Internet Intermediaries. Paris, Organization for Economic and Cooperation and Development, p. 9. (DSTI/ICCP(2009)9/FINAL.) www.oecd.org/Internet/ieconomy/44949023.pdf The report also credits Internet intermediaries with 'provid[ing] the Internet's basic infrastructure and platforms by enabling communications and transactions between third parties as well as applications and services'. p. 6.
5   See note 3 above.

OECD[42]	Special Rapporteur La Rue[43]	Article 193[44]	CDT[45]	Global Partners[46]
Internet access and service providers	Internet service providers (ISPs)	Internet service providers (ISPs)	Access providers/ISPs Network operators and mobile telecommunications providers	Physical layer: makes communications possible
				Connectivity & code: the language or protocols of the communication
Data processing and web hosting providers		Web hosting providers	Domain registrars and registries Website hosting companies	Applications: tools to navigate content
Internet search engines and portals	Search engines	Search engines	Internet search engines and portals	
E-commerce intermediaries			E-commerce platforms and online marketplaces	
Internet payment systems				
Participative networking platforms	Blogging services Online communities Social media platforms	Social media platforms	Online service providers In general, any website that hosts user-generated content or allows user-to-user communications	

Table 1: *Categories and key examples of Internet intermediaries[6]*

---

6   UNESCO, Fostering freedom online:The role of intermediaries, page 21, https://unesdoc.unesco.org/ark:/48223/pf0000231162 (accessed on 3 May 2022).

Role of Internet Intermediaries in Promoting Internet Freedom

Internet intermediaries play a crucial role in respecting and promoting freedom of expression, access to information and privacy online. An Internet intermediary provides access to an Internet service, which facilitates communication and exchange of information thereby allowing people to express themselves, access and exchange information and maintain their privacy online.

Freedom of expression and access to information is established under international human rights law and entrenched in national constitutions. Article 19 of the Universal Declaration of Human Rights (UDHR)[7] states that;

"*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*" Furthermore privacy and freedom of association are established under Article 12 and 20 respectively.

Similarly, Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[8] provides for freedom of expression and access to information while he African Charter on Human and Peoples Rights (ACHPR)[9] establishes under Article 9 that;

"*Every individual shall have the right to receive information and every individual shall have the right to express and disseminate his opinions within the law.*" In addition, Article 10 and 11 affirm the freedom of assembly and association.

The African Commission on Human and Peoples Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa[10] elaborates on article 9 of the African Charter, in particular, freedom of expression and access to information and as such offers relevant guidance on the conduct of Internet intermediaries. Part IV affirms freedom of expression, access to information and privacy on the Internet. Specifically Principle 39 addresses the role of Internet Intermediaries;

---

7   Universal Declaration of Human Rights (UDHR), https://www.un.org/en/aboutus/universal-declaration-of-human-rights (accessed 21 March 2022).
8   International Covenant on Civil and Political Rights (ICCPR), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed 24 April 2022).
9   African Charter on Human and People's Rights (ACHPR), https://www.achpr.org/legalinstruments/detail?id=49 (accessed 21 March 2022).
10   African Commission on Human and People's Rights (ACHPR) Declaration on Freedom of Expression and Access to Information, https://www.achpr.org/legalinstruments/detail?id=69 (accessed 21 March 2022).

- Internet intermediaries must enable access to all Internet traffic equally without discrimination blocking or giving preference to particular traffic.
- States shall not require Internet intermediaries to proactively monitor content which they have not authored or otherwise modified.
- In moderating or filtering online content, human rights safeguards must be mainstreamed into their processes and they must adopt mitigation strategies to address all restrictions on freedom of expression and access to information online, ensure transparency on all requests for removal of content, incorporate appeal mechanisms, and offer effective remedies where rights violations occur.
- Internet intermediaries are not required to facilitate the removal of online content when approached by the government unless such requests are: clear and unambiguous; imposed by an independent and impartial judicial authority, subject to due process safeguards; justifiable and compatible with international human rights law and standards; and implemented through a transparent process that allows a right of appeal.
- Law enforcement agencies may request Internet intermediaries for the expedited or immediate removal of online content that poses imminent danger or constitutes real risk of death or serious harm to a person or child, provided such removal is subject to review by a judicial authority.
- States must ensure the development, use and application of artificial intelligence, algorithms and other similar technologies by Internet intermediaries shall be compatible with international human rights law and standards, and shall not infringe on Internet rights.

Therefore, any restrictions on digital rights by Internet intermediaries through filtering specific content or keywords from websites, shutting down Internet or social media services, throttling or slowing down of Internet speeds or specific websites and failing to provide the necessary safeguards for anonymous and private communications constitute a violation. From the above, it is clear that both the States and Intermediate intermediaries have a role to play in guaranteeing freedom of expression and access to information online. Any limitations of any of the above digital rights need to be made in terms of law, and must be necessary and proportionate. And in cases where such laws do not exist, intermediaries often develop publicly available terms and conditions that specify their responsibilities and those of their customers.

Monitoring and Evaluating Performance of Internet Intermediaries

The conduct of Internet intermediaries must be critically monitored in order to assess if they are doing well in advancing Internet freedom. Drawing from research conducted by PIN in collaboration with RDR,[11] below are some indicators that can be used to assess the performance of Internet intermediaries which have an adverse impact on Internet freedom:

1. Freedom of Expression

Indicators in this category seek evidence that the company demonstrates it respects the right to freedom of expression[12] and access to information, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international human rights instruments. Ideally the company's disclosed policies and practices demonstrate how it works to avoid contributing to actions that may interfere with this right, except where such actions are lawful, proportionate, and for a justifiable purpose. Companies that perform well on this indicator demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others' demands, but also how they determine, communicate, and enforce private rules and commercial practices that affect users' fundamental right to freedom of expression and information.

- Access to terms of service: does the company offer terms of service that are easy to find and easy to understand?
- Process for terms of service enforcement: Does the company clearly disclose the circumstances under which it may restrict content or user accounts?
- Network management (telecommunications companies): Does the company clearly disclose that it does not prioritise, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring the quality of service and reliability of the network?
- Network prioritisation practices: If the company does engage in network prioritisation practices for reasons beyond assuring quality of service and reliability of the network, does it clearly disclose its purpose for doing so?
- Network shutdown (telecommunications companies): Does the company clearly disclose the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network?
- Restriction of access to specific application and protocols: Does the company clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?

11   Paradigm Initiative, Ranking Digital Rights in Angola, CAR and DRC, https://paradigmhq.org/report/ranking-digital-rights-in-angola-democratic-republic-of-congo-and-central-african-republic-2/ (accessed on 5 May 2022).
12   Paradigm Initiative, Ranking Digital Rights in Angola, CAR and DRC, pages 12 & 16 , https://paradigmhq.org/report/ranking-digital-rights-in-angola-democratic-republic-of-congo-and-central-african-republic-2/ (accessed on 5 May 2022).

- Government demands: Does the company clearly disclose its process for responding to government demands to shut down a network or restrict access to a service?
- Commitment to push back on government demands: Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?
- User notification of network restriction: Does the company clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service?
- Network shutdown demands: Does the company clearly disclose the number of network shutdown demands it receives?
- Demands by legal authorities: Does the company clearly disclose the specific legal authority that makes the demands?
- Number of government demands: Does the company clearly disclose the number of government demands with which it complied?
- Identity policy: Does the company require users to verify their identity with their government-issued identification, or with other forms of identification that could be connected to their offline identity?

2. Privacy

Indicators in the privacy[13] category seeks evidence that in its disclosed policies and practices, the company demonstrates relevant ways in which it respects the right to privacy of users, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international human rights instruments. The company's disclosed policies and practices demonstrate how it works to avoid contributing to actions that may interfere with users' privacy, except where such actions are lawful, proportionate, and for a justifiable purpose. Such companies also demonstrate a strong commitment to protect and defend users' digital security. Companies that perform well on these indicators demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others' demands, but also how they determine, communicate, and enforce private rules and commercial practices that affect users' privacy.

- Access to privacy policies: Does the company offer privacy policies that are easy to find and easy to understand?
- Collection of user information: Does the company clearly disclose what user information it collects, and how?
- Inference of user information: Does the company clearly disclose what user information it infers and how?
- Sharing of user information: Does the company clearly disclose what user information it shares and with whom?
- Purpose for collecting, inferring, and sharing user information: Does the company clearly disclose why it collects, infers, and shares user information?
- Retention of user information: Does the company clearly disclose how long it retains user information?
- Users' control over their own user information: Does the company clearly disclose to users what options they have to control the company's collection, inference, retention and use of their user information?
- Users' access to their own user information: Does the company allow users to obtain all of their user information the company holds?
- Process for responding to government demands for user information: Does the company clearly disclose its process for responding to governments' demands for user information?
- Process for responding to private requests for user information: Does the company clearly disclose its process for responding to requests for user information that come through private processes?
- Data about government demands for user information: Does the company regularly publish data about government demands for user information?
- Data about private requests for user information: Does the company regularly publish data about requests for user information that come through private processes?

- User notification about third-party requests for user information: Does the company notify users to the extent legally possible when their user information has been demanded by governments and other third parties?
- Data breaches: Does the company publicly disclose information about its processes for responding to data breaches?

3. Governance

Indicators in the governance[14] category seek evidence that the company has governance processes in place to ensure that it respects the human rights to freedom of expression and privacy. Both rights are part of the Universal Declaration of Human Rights, and are enshrined in the International Covenant on Civil and Political Rights.

- Policy Commitment: Does the company publish a formal policy commitment to respect users' human rights to freedom of expression and information and privacy?
- Governance and management oversight: Does the company's senior leadership exercise oversight over how its policies and practices affect freedom of expression and information, and privacy?
- Impact assessment – Governments and regulations: Does the company conduct regular, comprehensive, and credible due diligence, through robust human rights impact assessments, to identify how government regulations and policies affect freedom of expression and information and privacy, and to mitigate any risks posed by those impacts in the jurisdictions in which it operates?
- Impact assessment – Processes for policy enforcement: Does the company conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments, to identify how its processes for policy enforcement affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts?
- Stakeholder engagement and accountability: Does the company engage with a range of stakeholders on the company's impact on freedom of expression and information, privacy, and potential risks of related human rights harms such as discrimination?

---

14   2020 RDR Corporate Accountability Index Methodology - https://rankingdigitalrights.org/2020-indicators/ (accessed on 11 May 2022).

The Advocacy Strategy

To conduct meaningful advocacy, the following steps are necessary.

1: What is the problem?

Identify the problem posed by Internet intermediaries. This is a process which starts by actively monitoring their conduct, reviewing their platforms and using key indicators such as those provided by RDR[15] to measure their performance. Address the 'who, what, where' questions. Is the government part of the problem? Is it just the Internet intermediary? Is it both? What is the issue and where did it arise?
For example, in countries like the DRC and CAR, governments shutdown the Internet and electronic communication networks to stifle public demonstrations and social demands. In this context, Internet intermediaries participate directly or indirectly in network disruptions or Internet shutdowns.

2: How and why must the key players be engaged?

Having identified the duty bearer who is the cause of the issue, address how they can be engaged or made aware of the problem. Here, note the objective of your advocacy steps.   Step 1 and Step 2 are critical to the advocacy strategy captured in the text box below. The objective of the advocacy strategy is to conduct advocacy campaigns to change the practices of governments, companies and Internet intermediaries on all specific activities. To succeed in an advocacy strategy, actors must answer certain key questions.

---

15   RDR 2020 Indicators https://rankingdigitalrights.org/2020-indicators/ (accessed on 24 April 2022).

The key elements of an advocacy strategy

• **WHAT change do we want to make in Internet freedoms?** How can Internet Intermediaries help us? It is about determining what is wrong and what needs to change (context and problem analysis). It is important to provide solid evidence and to be clear (low Internet penetration rate, poorly adapted Internet policies, level of development of Internet infrastructure) on what needs to be stopped, in comparison with what needs to change, and what alternative solutions can be adopted (change goals and objectives). It is also about identifying the harm to real people, which is usually the most important driver when we talk about human rights. Introduce best practices.

• **WHO can bring about change?** How can the actors and resources of Internet intermediaries strengthen its ecosystem? It is about questioning the people who have the power to bring about the desired change and the people who can be potential allies and opponents (analysis of stakeholders, targets and allies). It is also important to understand how stakeholders are involved in decision-making and may or may not have a role in the change (dynamic power analysis).

• **HOW can you get them to make the change you want?** This involves thinking about potential strategies and tactics (media campaigns, door-to-door, various workshops, conferences) to influence those who have power, but also defining the messages to be transmitted to the different targets and identifying the times and the most opportune places to defend ideas and advocate for long-term change.

3: Identify the Context and Problem

This analysis requires paying particular attention to the normative frameworks or their practical application, assessing their effect on Internet users. The analysis of relevant existing laws, policies, strategies, technical guidelines or budgetary documents in the field, as well as their non-existence or the constraints in their implementation, is necessary to understand what level of priority is granted to the issue by the stakeholders (government, media, CSOs, technology companies, etc.) that we seek to influence. This identification of the context and problem helps in formulating the appropriate action.

For instance, despite not having a comprehensive Data Protection Law, in August 2019, the Nigerian government passed and signed the Federal Mutual Assistance in Criminal Matters law that allows it to conduct surveillance on citizens on behalf of foreign countries conducting criminal investigations.[16] This raises privacy concerns as the law empowers authorities to track, intercept and monitor calls.

4: Goals for change and specific objectives

Once the advocacy issue has been identified, you are able to define your goal and specific objectives. While change goals will be broad in bringing lasting change, advocacy objectives should be as specific as possible. Advocacy objectives contribute to the achievement of the change goal. There can be one or more specific objectives and each of them must be SMART (Specific, Measurable, Achievable, Realistic, Time-bound). In this way, their follow-up will be easier, as well as the evaluation of their achievement or not. Change goals and advocacy objectives should be classified into different categories, depending on whether they are political, institutional or concern changes in practice.

Case Study of Paradigm Initiative's advocacy strategy in the DRC

Problem Identification	1. Internet freedoms in the DRC are regularly violated. 2. Internet intermediaries do not contribute enough to the stability of the network in the country. 3. Several disturbances of the Internet network have been listed in the last 10 years in the country before, during or after political mobilizations
Objective of change	Work to limit all forms of digital rights violations in the country
Advocacy outcomes	1. The government (Ministry of Digital - DRC and other ICT ministries) ensures compliance with international instruments on digital rights and freedoms on the Internet; 2. The government accepts the development of a transparent legal framework for the freedoms of the press, expression, assembly and association online; 3. The government accepts the strengthening of the legal and regulatory framework for digital communications and the Internet ecosystem; 4. Internet service providers are committed to supporting the digital rights of users and customers; 5. The government sets the axis for the promotion of good governance of the Internet ecosystem by taking into account all the stakeholders in the decisions.

16   Londa – Nigeria Country Report 2021, https://paradigmhq.org/report/londa-report-2021/ (accessed on 2 June 2022).

Stakeholder and Power Analysis

A stakeholder is a person or group of people who have something to gain or lose from the outcome of a planned project or process, and who can have a great influence on the project or the process in question. Undertaking a stakeholder analysis will help identify individuals or groups that have an interest in the advocacy issue, allies and opponents.

Stakeholder and power analysis is an essential step in identifying the different groups that might have an interest in a policy or debate, and in assessing their ability to influence the final outcome. This will make it possible to design strategies to involve, convince, or manage the different groups of stakeholders. Generally, many actors are involved in the development or adjustment of government policies and strategies (the various ministries and other public organisations, donors and technical partners, research organisations, etc.), and in the way in which official consultations with civil society and/or the private sector can be organised.

Stakeholders in the process of advocating for freedom on the Internet can be the following: national institutions (Ministry of ICTs, ICT regulatory agencies etc.); technical and financial partners (embassies, bilateral and multilateral donors; foundations etc.); global initiatives (World Bank, Global Fund); civil society (media, churches and faith-based organisations, CSOs); Internet Governance Forums (national/regional and global IGFs, digital rights forums, International Telecommunications Union, Internet Engineering Task Force and Institute of Electrical and Electronics Engineers) and academia (Universities and research institutes); private sector (private telecommunications companies, technology companies and social networks).

To be successful in the process of stakeholder engagement in advocacy, sharing information with the target stakeholders is often important, rather than simply waiting for them to provide the information. Regular participation in networks, platforms and alliances should also improve the quality of the information collected and make it easier to share information sources.

Targets

Some institutions or individuals have the power to bring about a change in policy or practice, while others can influence those institutions or individuals. Some also have the ability to create faster change and some slower. This is how primary and secondary targets can be defined, with the latter often being the most difficult to identify.

Taking the example of violations of Internet freedoms, the primary targets should be ministers from different ICT and digital sectors. In the private sector, the Chief Operations Officer is a primary target while the Stakeholder Engagement Manager can be a secondary target. However, most senior executives are unable to devote enough time and attention to a particular topic. Secondary targets are often more available as an entry point in the engagement process. Primary targets who bring about the policy change must be copied/addressed in the messaging when tools like press releases or open letters are drafted and shared through the Internet and secondary targets so that the message is well delivered.

Messages, times and places

Advocacy messages are formulated according to the objectives to be achieved. Messages should be:
- Clear and brief: use precise and powerful language, active verbs.
- Specific: who is the message addressed to?
- Simple: make sure your message is clearly understood.
- Evidence-based: based on research and program experiences.
- Action-oriented: stated demands must be concrete to the target audience and with suggestions for solutions adapted to each audience. Recommendations must be clearly formulated.

Opportunities

Once the messages have been defined, the success of the work will largely depend on the ability to be in the right place to speak to the right people at the right time. It is therefore crucial to identify the opportunities and to have the best possible understanding of the process, the places, the time allowed and the actors involved. Meetings and conferences are good opportunities for advocacy, since they represent good opportunities to address key targets and those who have influence, especially during coffee breaks! Platforms like RightsCon, Internet Governance Forum, Forum on Internet Freedom in Africa and the Digital Rights and Inclusion Forum (DRIF) may be good opportunities for meeting the relevant Internet intermediaries. Sessions may be hosted at these fora to present any evidence based research or articulate key recommendations of policy briefs.

Tactics and strategies

It is important to identify the target of the advocacy strategy from the onset. Below are likely targets and allies:
- Decision-makers and those with influence (government authorities, Internet intermediaries and other private sector actors).
- The media, particularly journalists with interest in the subject matter, are great allies in a robust campaign.
- Other non-governmental organisations (local or international), think-tanks and academia who can be allies for joining in advocacy action.

Many different actions can be taken to influence targets. Deciding the best tactic or how the combination of tactics can be used at any given time to achieve the maximum level of influence, keeping in mind the links to evidence based research and policy briefs is crucial to deploy a robust advocacy strategy. The following are key actions:
- Conduct Research: Refer to case studies and lessons learned from the programmes, technical support, reports on the state of digital rights etc.
- Lobby relevant targets: Have direct links with a series of targets, draft letters of engagement and schedule meetings with them on the policy issues. Lay out the issues and recommendations, convince targets and negotiate common positions.
- Bring the media on board: Through written articles and interviews (radio , TV, newspapers), raise awareness and highlight the issues and recommendations clearly. Influence opinion leaders and primary targets by making messages and action points visible.
- Raising awareness and mobilisation: Host events to raise issues. Policy dialogues raise awareness of the issues and also make the call for a response from the relevant duty bearers/targets. Consider mobilising allies in a campaign which can be online or offline. Mobilise support for open letters, press releases or petitions.

Forms of Engagement

- Request a meeting with the Internet intermediaries to discuss issues and present any research findings.
- Organise a workshop with the appropriate Internet intermediaries and government actors.
- Follow up on any agreed outputs, actions and timelines.

Research

- Conduct background research to fully appreciate if you have the right target and to have all the facts of the problem. Read official notes and documents, sector strategies and policies ,the national budget, donor strategies and reports, NGO reports, information documents and analyses, etc.
- Use Internet search engines to conduct desk research on developments and solutions in other countries. Look at the performance of other Internet intermediaries for a comparative analysis.

Communication and media

The open letter or press release (PR) is a major reactionary or informative media tool. It can have several objectives:
- To immediately react to digital rights violations or actions by Internet intermediaries or other duty bearers.[17]
- To inform the media about the launch of a report, a campaign, or a project. See more in the DRC Londa Report.[18]
- To influence the agenda of a negotiation or the position of an actor prior to a conference/meeting.
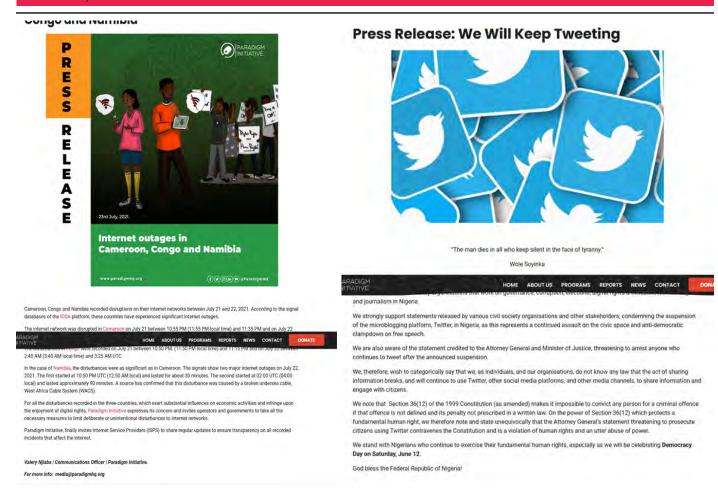- To make a message or activity visible to the public or decision-makers.

Make use of press media briefings where there is no response following a press conference. Ultimately, the purpose of a press release is to get an interview (in a newspaper, radio, or Television) or to be quoted by the media or a news agency. It is a technique of indirect influence which can sometimes prove to be more powerful than other modes of action. It is particularly useful when it comes to introducing a dissonant voice into the debate, or if the targeted decision-makers are particularly sensitive to their public image.
Please find samples of press releases below:
- [Internet outages in Cameroon, Congo and Namibia](#)
- [We Will Keep Tweeting](#)
- [Federal Government reverses Twitter Ban in Nigeria after 222 Days](#)
- [Your online data belongs to you and must be protected, declares Paradigm Initiative.](#)

17　　Digital Rights: How Francophone Africa is bracing for COVID-19's impact? https://paradigmhq.org/digital-rights-how-francophone-africa-is-bracing-for-covid-19s-impact/ (accessed on 30 May 2022).
18　　Londa – DRC Digital Rights & Inclusion 2020 Report,
 https://paradigmhq.org/report/londa-drc-digital-rights-inclusion-2020-report/ (accessed on 30 May 2022).

Public mobilisation

- Raise public awareness of an issue through different media such as factsheets, radio programs and media interviews.Public support for an issue can be a powerful force for policy or legislative change.
- Run petitions to mobilise joint action and call for immediate action. Gathering endorsements for petitions must be time-bound and once all signatures are collected, it is delivered to the Internet intermediary or government representative concerned with all targets in copy. It can be distributed through a website or via SMS, email or other social media platform. Many online tools have been developed in recent years. Change.org is an example of where you can develop an online petition in a simple and effective way, putting this type of action into practice.

Resources and tools

- Ranking Digital Rights methods and standards
  https://rankingdigitalrights.org/methods-and-standards/

- 2022 Ranking Digital Rights Big Tech Scorecard
  https://rankingdigitalrights.org/index2022/

- Ranking Digital Rights Corporate Accountability Index Methodology
  https://rankingdigitalrights.org/2020-indicators/

- Ranking Digital Rights in Angola, Democratic Republic of Congo and Central African Republic
  https://paradigmhq.org/report/ranking-digital-rights-in-angola-democratic-republic-of-congo-and-central-african-republic-2/

- ACHPR Declaration on Freedom of Expression and Access to Information
  https://www.achpr.org/legalinstruments/detail?id=69/

- RIPOTI
  https://ripoti.africa/

- Petitions
  https://www.change.org/

- Press Release Sample 1
  https://paradigmhq.org/press-release-internet-outages-in-cameroon-congo-and-namibia/

- Press Release Sample 2
  https://paradigmhq.org/press-release-we-will-keep-tweeting/

- Press Release Sample 3
  https://paradigmhq.org/press-release-federal-government-reverses-twitter-ban-in-nigeria-after-222-days/

- Press Release Sample 4
  https://paradigmhq.org/press-release-your-online-data-belongs-to-you-and-must-be-protected-declares-paradigm-initiative/