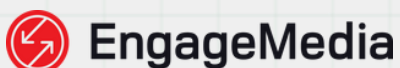




Addressing Internet Censorship and Content Filtering


A TOOLKIT FOR CIVIL SOCIETY ORGANIZATIONS

Produced by



With support from





EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at engagemedia.org.

The Global Network Initiative is a nonprofit that protects and advances freedom of expression and privacy in the ICT sector. GNI helps companies respect freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content, or restrict communications. The network comprises a growing alliance of Internet and telecommunications companies, human rights and press freedom groups, investors, and academic institutions from around the world.

Learn more at globalnetworkinitiative.org/.



TABLE OF CONTENTS

Acknowledgements	i
Table of Contents	ii
Regional Context	1
What is this toolkit for?	2
Section A: What is internet censorship and content filtering?	3
What is internet censorship?	4
How does it happen?	6
What is content blocking?	8
What is content filtering?	9
Who is responsible for censorship?	10
Section B: How can you circumvent internet censorship and content filtering?	13
Use a Virtual Private Network	14
Use a secure browser	15
Change your DNS provider	17
Use a proxy service	17
Section C: How can you monitor internet censorship and content filtering?	19
Partner with OONI	20
Use a censorship measuring app	20
Use or contribute to test lists	21

Case study: Internet Monitoring Project	22
Section D: How can you advocate for an open internet?	23
Ask the basic questions	24
Case study: West Papua	28
Determine the message	29
Craft the campaign plan	29
Consult with other groups	30
Identify the stakeholders	31
Engage with stakeholders	35
Spotlight: Global Network Initiative	38
Execute the campaign	39
Measure the impact	39
Campaign stories	40
A reminder on measuring impact	42



Regional Context

In South and Southeast Asia, internet censorship and content filtering have become tools to silence dissent and limit freedom of information. These forms of digital rights violations are contributing to shrinking civic spaces in the region. Recent notable cases include the 2021 blocking of critical progressive websites in the Philippines, under the allegation of “being affiliated to communist-terrorist groups” and the 2023 permanent shutdown of Voice of Democracy (VOD) in Cambodia for its alleged actions against the “dignity and reputation of the Cambodian Government” in early 2023.

Taking these incidents into account, EngageMedia, supported by the Global Network Initiative (GNI) produced an open source toolkit on Addressing Internet Censorship and Content Filtering. This toolkit for civil society organizations and advocacy movements empower key stakeholders to navigate and advocate for the potential removal of internet censorship and content filtering.

What is this toolkit for?

The purpose of this toolkit is to assist civil society, particularly members of local human rights organizations, in developing a better understanding of internet censorship and content filtering from a regional perspective in order to more effectively advocate for a more open internet. This toolkit, produced by EngageMedia and supported by the Global Network Initiative, is informed by the stories and experiences of civil society organizations (CSOs) in South and Southeast Asia when dealing with internet censorship and content filtering

The toolkit is broken down into the following sections:

Section A Definition of internet censorship and content filtering

Discusses the definition, context, and relevant actors. It also addresses the technical aspect of how internet censorship and content filtering are generally implemented.

Section B Circumventing online censorship and content filtering

Focuses on ways to bypass internet censorship or content filtering. It elaborates on how to use specific tools, such as VPN and proxy services; identifying and choosing DNS providers and secure browsers; and directing you to further resources available in our DigiSec Directory.

Section C Monitoring online censorship and content filtering

Details possible ways to monitor online censorship and content filtering by measures such as building partnership with the Open Observatory of Network Interference (OONI) and creating and/or contributing a test list of monitored websites. It also provides success stories to study from.

Section D Advocating for a free internet

Focuses on developing an advocacy campaign for a free internet. The directory provides guidance on how to build a case in local context as well as determine key messages; identify relevant stakeholders to internet governance; engage with said stakeholders; and measure the success of the campaign, including ways to improve it.



WHAT IS INTERNET CENSORSHIP AND CONTENT FILTERING?





What is internet censorship?

Internet censorship refers to the control and restriction of what can be accessed, created, or viewed on the internet. This practice has had a significant impact on people's freedom of expression worldwide, particularly in countries under authoritarian governments. Various factors drive internet censorship, with motivations varying in their legitimacy. Average censorship measures and policies are directed towards preventing access to copyrighted material and harmful content. However, there are instances where authorities take advantage of such policies to control or restrict access to information with the intention of manipulating public narratives, suppressing political dissent, and restricting access to information. Examples include the news filtering in many countries during the COVID-19 pandemic, as well as the propagation of hate speech perpetrated against the Rohingya in Myanmar.

Internet fragmentation is one method governments may use to enact censorship and create controlled online spaces. Fragmentation can be conducted in three different ways, as outlined in the [2016 World Economic Forum paper](#) on internet fragmentations:

1. **Technical fragmentation**, which occurs when the internet's infrastructure makes it hard for different systems to connect and share data;
2. **Governmental fragmentation**, which results in restrictive policies limiting access to information;
3. **Commercial fragmentation**, which is driven by business practices that constrain internet usage and information distribution.

This strategic approach allows for more effective control over online content. Alarming trends indicate a notable rise in national governments blocking websites that host nonviolent political, social, or religious content. Such actions directly undermine the fundamental rights of individuals to freely express themselves and access information. As a result, global internet freedom has experienced a continuous decline for the 12th consecutive year, exacerbating the deteriorating environment for human rights online. These developments raise concerns about the restriction of online discourse and access to information on a global scale and the subsequent impact on individuals fundamental rights.



Learn more about the technical aspects of internet censorship on [EngageMedia.org](https://www.engage-media.org).

How does it happen?

Moving beyond local networks, Internet Service Providers (ISPs) and Telecommunications Service Providers (TSPs) play a significant role in internet censorship. They have the ability to block specific websites or even the entire internet, giving governments broad control over what users can access. Additionally, they can throttle the internet, slowing down targeted online services or applications.

Furthermore, governments can exert influence on ISPs and TSPs through laws and regulations to enforce censorship on their behalf, thereby blocking access to certain pieces of content or ordering an internet shutdown. When compelled, ISPs may use one of the methods listed below to enact internet censorship:

Fundamental infrastructure shutdown	failure of or damage to the physical communications infrastructure necessary for internet services. An example would be the physical destruction of a power grid or cellphone tower.
Routing	Manipulating network routine works by altering the route information at key points (for example, international gateways) so that network traffic is blocked and does not pass beyond the controlled infrastructure.
DNS manipulation	Manipulating the <u>DNS naming system</u> that translates human-readable domain names (like google.com) to machine-readable IP addresses (like 142.251.32.46) to direct users to either a non-existent server or a server controlled by the perpetrator.

Filtering	use of Commercial filtering appliances and <u>transparent proxy</u> to block access to internet services by analysing metadata from network traffic and then allow or block access based on that metadata.
Throttling	restriction of Data flow through the network to render the service or resource effectively unusable; for example, by downgrading mobile internet to 2G or capping data speeds.
Deep Packet Inspection	Inspection and screening of network data. If the data packet is found to be non-compliant with the criteria set by the shutdown perpetrator, the data packet is blocked from passing through the inspection point.
Denial of Service (DoS) attack	Targeted fake traffic to a specific platform or server to keep it busy and prevent it from providing data to users.

Lastly, search engines, which serve as a primary tool for content discovery, can be subject to censorship and content filtering. Governments can require search engines to block certain queries or manipulate search results to display only government-approved content.



What is content blocking?

Blocking typically refers to the act of preventing access to blacklisted websites, domains, IP addresses, protocols, or services. Depending on the legal regime, the justification for blocking often revolves around the objective of preventing access to illegal content, content that poses a threat to public order, or content that may be objectionable to a particular audience.

Internet blocking in South and Southeast Asia has always been a major concern, with reports of website blocking, content restrictions, and cyber surveillance. According to the [iMap: The State of Internet Censorship report 2022](#) focusing on 8 countries in Southeast Asia, news and media and human rights issues websites were the most blocked, with approximately 4% of websites in these categories being inaccessible (anomaly and confirmed blocked). Southeast Asian governments have been known to block websites and social media platforms for various reasons, including, but not limited to, national security and combating online piracy. Several laws and regulations have also been imposed to take action on civilians, political activists, and human rights defenders.



Following the South and Southeast Asia Digital Rights School held in April 2022, representatives from Bangladesh and the Philippines wrote about how their respective governments used existing censorship-related laws against their critics. Read more at EngageMedia.org.



What is content filtering?

Content filtering and blocking are interrelated practices that involve restricting access to information based on specific criteria. While blocking can involve blocking entire websites or IP addresses, content filtering focuses on the use of technology that **blocks pages by reference to certain characteristics**, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful.

This approach is often employed when authorities wish to avoid complete blockages but still want to restrict certain content. Content filtering utilizes software or hardware solutions to analyze the content of digital communications, such as websites, emails, or instant messages. These solutions assess whether the content meets certain criteria for accessibility, which can be based on factors like traffic patterns, protocols, keywords, or its association with inappropriate or unlawful content. This process allows authorities to selectively control the availability of information deemed illegal, a threat to public order, or objectionable for certain audiences within a specific jurisdiction.

Depending on the configuration, filtered content may be prevented from loading altogether. Users may also be redirected to alternative content or receive a warning message indicating restricted access.



Who is responsible for censorship?

National governments often play a significant role in implementing and enforcing internet censorship measures. They may establish regulatory bodies or specialized agencies responsible for monitoring online content.

There have been cases of government surveillance and limitations on freedom of expression and privacy, including the monitoring of online activities through the use of [spyware](#) and other techniques, and occasional blocking or censoring of certain websites and social media platforms to combat the dissemination of rumors and hate speech.

Regrettably, countries enact laws and policies seemingly aimed at addressing online wrongdoing, yet end up penalizing individuals who voice criticism against the government or its leaders. Bangladesh's [stringent internet legislation](#), exemplified by the Digital Security Act adopted in October 2018, has tightened the government's control over the Internet by imposing severe penalties for expressions deemed critical of national symbols, religious sentiments, and communal harmony, as cited by rights groups, is an unfortunate example of treating peaceful critics as offenders.



Who is responsible for censorship?

Internet service providers and owners of social media platforms are crucial in the implementation of internet censorship measures. Social media platforms and other platforms with user-generated content often pro-actively implement content moderation measures, whether as part of the legal obligation imposed by their country of operation, or part of their internal policies.

South and Southeast Asian governments have legislated laws that mandate the responsibility for filtering content moderation to companies. Indonesia's [MR5](#) regulation obliges Private Electronic System Operators to prevent the dissemination of a predetermined, prohibited content, and Bangladesh's [Regulation for Digital, Social Media, and OTT Platforms](#) bans intermediaries from publishing the broadly-termed "unlawful information" upon receiving actual knowledge of such information's existence from relevant authorities.

Large and well-established social media companies such as Facebook and Twitter have also integrated [measures for content moderation](#) in their company policies to respond to the [rise of disinformation and hate speech](#) online. These measures include [fact-checking measures](#), [warning labels](#), and [redirection](#) to credible, science-based information.



Censorship in South and Southeast Asian regulations and policies

[The Draft Cybersecurity Law in Myanmar](#)

grants authorities the power to order providers to ban websites.

[Thailand's Computer Crime Act](#)

enables the government to restrict access and block undesirable online content.

[Cambodia's National Internet Getaway Sub-decree](#)

requires all internet traffic to be routed through a regulatory body charged with monitoring online activity before it reaches users.

[Bangladesh's National Telecommunication Monitoring Center](#)

is implementing the "content blocking and filtering system" which may block and filter antigovernmental propaganda and other content to be used for criminal activities on the internet.



HOW CAN YOU CIRCUMVENT INTERNET CENSORSHIP AND CONTENT FILTERING?



There are several ways to get more freedom online if you are subject to internet censorship at home, at work, through your ISP, or by your government. While some solutions are free and others have a cost associated with them, all of them are easy to set up and will significantly increase your protection from censorship.

1. Use a Virtual Private Network

A virtual private network (VPN) creates an encrypted tunnel between your device and the VPN server. Your DNS requests and other internet traffic are then forwarded through the VPN server, making it impossible to identify you personally for your ISP. By doing this, your ISP is unable to identify the websites you are attempting to browse and cannot impose any blocks. You can then connect to a server in another country where that content or service is not blocked.

There is a wide variety of paid and free VPNs available to use. Before you start using one of them, you must verify that they are protecting your privacy. Be careful to check the following:

- ✓ If they are responding to government requests for user information
- ✓ If they are keeping users' usage logs
- ✓ The type of encryption they are providing.
- ✓ The number of countries where servers are located

The aforementioned can be done by checking a VPN provider's privacy policy. To access the VPN policy, check if the provider undergoes annual third-party security audits and shares the results publicly. This indicates their commitment to security; however, be cautious of hyperbolic claims.

You can evaluate your VPN provider's privacy and security performance using [VPNalyzer](#), a crowdsourced investigation initiative focused on promoting public interest, setting practical standards, and ensuring transparency and accountability in the VPN ecosystem.

2. Use a secure browser

Some secure browsers enable you to bypass internet censorship. The downside to using this mechanism is that all other apps on your devices will continue to be blocked.

Recommended VPNs



TunnelBear

Has Free and Paid Options



ProtonVPN

Connected with ProtonMail account



Outline VPN and Bitmask

Combine a self-hosted VPN like Outline with an open-source application like Bitmask that provides easy and secure communications

Recommended Secure Browsers



Tor (onion router)

Hides your IP address and clears cookies just as soon as you close website tabs

Encrypts all your browser activity and routes it through three random Tor nodes, ensuring that you'll be safe even if you've visited restricted websites.



Brave

Hides your IP address and clears cookies just as soon as you close website tabs



Ceno

Allows users to access and share web information in and across regions where VPNs are deemed too risky

3. Change your DNS provider

If you know you are facing DNS filtering, you can simply switch who handles your DNS queries. Note that your new DNS provider will obtain the information about your browsing activity that your ISP once had, which can be a privacy concern.



For a list of DNS providers that have strong privacy policies and commitments to not share your browsing data, go to [Mozilla.org](https://www.mozilla.org).

4. Use a proxy service

A proxy service is a tool or service that allows users to access the internet indirectly through a different server. It acts as an intermediary between the user and the websites they want to visit, helping to bypass censorship and access blocked content.

It is not recommended to rely on web-based proxies. While they can be useful in certain situations where software installation is not possible, experts advise using dedicated tools like Psiphon and Lantern. These standalone tools are considered more secure and reliable compared to web proxies.

Recommended DNS Providers

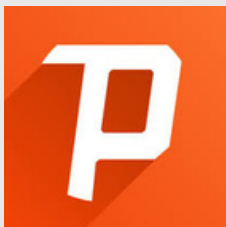


[Quad9](#) is a popular DNS provider that can help you bypass blocks. Quad9 provides a comprehensive [setup tutorial](#). However, you will need to change your operating system settings to utilize a new DNS provider.

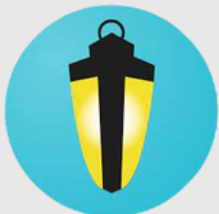


You may also use DNS from [Cloudflare](#). They also have a good [setup guide](#) to help you onboard.

Recommended Proxy Services



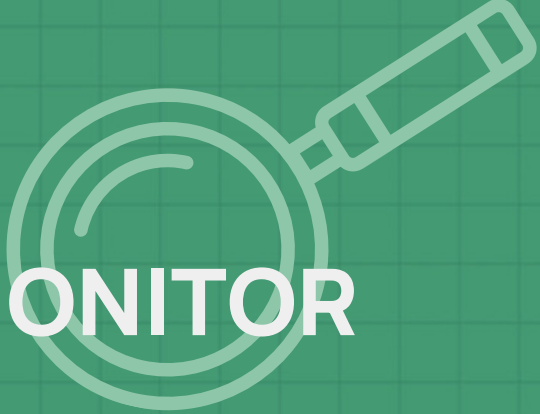
[Psiphon](#) is a secure, open-source, and public anti-blocking tool that provides uncensored access to online content by using VPN and SSH proxies. If the download pages for Psiphon are blocked, you can email get@psiphon3.com, and they will send you an alternate link. Its Direct Download link for Android requires you to allow your device to Install Unknown Apps, which will make your device vulnerable to malware.



[Lantern](#) is a secure, open-source, public anti-blocking tool that uses HTTPS proxies to provide uncensored access to online content.



Visit [Digisec.directory](#) for an ongoing resource database of circumvention tools available in select Southeast Asian languages.



HOW CAN YOU MONITOR INTERNET CENSORSHIP AND CONTENT FILTERING?





1. Partner with OONI

If you are experiencing website blocking in your region while accessing the internet, the [Open Observatory of Network Interference \(OOONI\)](#) is interested in receiving reports from such situations occurring globally. OONI collects data to better understand and document these instances of website blocking.

2. Use a censorship measuring app

The [OOONI Probe](#) app is a useful, free resource that detects censorship and traffic manipulation on the internet. This tool can be a helpful way to collect data that can be used as evidence of restrictions to access. Their software can help measure:

- [Blocking of websites](#)
- Blocking of instant messaging apps (WhatsApp, Facebook Messenger and Telegram)
- [Blocking of censorship circumvention tools \(such as Tor\)](#)
- Presence of systems (middleboxes) in your network that might be responsible for censorship and/or surveillance
- [Speed and performance of your network](#)

3. Use or contribute to test lists

Test lists consist of websites that are examined for censorship using tools like OONI Probe and [Censored Planet](#).

[The Citizen Lab](#) has hosted these [lists on GitHub](#) since 2014, encouraging community participation and ensuring their ongoing updates. There are two types of test lists: the [Global test list](#) and [Country-specific test lists](#).

Contributing to these test lists is vital to ensure comprehensive monitoring of censorship. If a relevant website is blocked but not included in the test list, it won't be tested, and the results won't be publicly available. You can contribute to test lists regardless of your technical skills or knowledge. If your organization is interested in regular contributions to your country or region's test list, you can reach out to OONI for review and updates. You can also reach out to them for more technical details on how to contribute to test lists.



To understand more about how to use OONI tools to measure internet censorship, OONI has created an [online course](#) on the Advocacy Assembly platform. You will learn how to access and understand real-time data about internet censorship worldwide using OONI.

CASE STUDY

iMAP: Internet Monitoring Project

[The iMAP initiative](#) is a three-year collaboration among civil society organizations that advocate for online freedom of expression. Its objective is to measure network interference and restrictions on freedom of expression in South and Southeast Asian countries using OONI tools.

EngageMedia has coordinated internet censorship measurements in Indonesia and the Philippines as part of the iMAP initiative with the support of [Sinar Project](#) and the Open Observatory of Network Interference. EngageMedia has maintained internet censorship monitoring test lists and probes in both countries.

The research and reports conducted by EngageMedia have shed light on internet censorship and restrictions on online freedom of expression in [Indonesia](#) and the [Philippines](#). These findings emphasize the importance of ongoing monitoring and reporting efforts to address these issues.

These collaborative initiatives have contributed to capacity building among digital rights advocates in the region. This exemplifies the significant role of civil society organizations in promoting and defending online freedom of expression through internet monitoring programs.



HOW CAN YOU ADVOCATE FOR AN OPEN INTERNET?



Advocating against internet censorship and content filtering is integral to upholding digital rights. Civil society organisations can meaningfully contribute to the broader open internet movement through compelling advocacy campaigns grounded in local contexts and clear case studies. These kinds of well-documented stories can serve as an entry point to engaging with and gaining the support of various stakeholders.

You or your organization can create your own campaign for an open internet with the following steps:

1. Ask the basic questions

In internet censorship and content filtering, identifying the issue in the region is really important to know the specifics of what we are demanding. Asking these questions might be helpful to assess and contextualize the specific situation in your area;

What type of censorship and/or filtering is being implemented in your region?

This helps to identify the type of disturbance that the community is facing, the proportionality of the measure to the issue at hand, and possible ways to circumvent it. You can use the tools provided in the earlier section to assess your circumstances.

Who is the censorship and filtering targeting?

This question identifies the individuals, organizations, or websites affected by censorship and content filtering, and assesses whether the limitation is justifiable and necessary for public order. The target for censorship and content filtering varies across countries, and while some measures of censorship can have a legitimate cause – such as preventing access to child pornographic content and blocking fraudulent gambling sites – others might be an indication of a discriminatory practice. To distinguish the two, one can ask additional sub-questions:



Where is the censorship taking place?

Is it in areas that have historically experienced systemic discrimination? Is it affecting organizations and individuals who are notably vocal and critical of existing socio-political issues, specifically sensitive ones?



What are the events leading up to the censorship?

Is the censorship carried out incidentally, i.e. the wake of protest movements or leading up to big events such as political elections? This can be seen as an indication of whether the imposed limitation is used to silence certain groups from speaking out and/or deprive the wider public of information.

Who is the censorship and filtering targeting?



What justification is provided by the executor of the censorship?

Reasons for implementing censorship/filtering can vary depending on the context. Ways to determine such include finding out whether the justification is backed by sufficient evidence of the claims, whether previous countermeasures are deemed inefficient, and an assessment from independent third parties.



What is the impact of the censorship?

Internet censorship can impact a broad range of human rights of individuals and communities. The report "[Disconnected: A Human Rights-Based Approach to Network Disruptions](#)" by the Global Network Initiative documents the human rights' impacts of network disruptions on vulnerable communities including marginalized ethnic groups, immigrants, women, and girls. The report "[The Economic Impact of Disruptions to Internet Connectivity](#)" highlights the significant economic damage caused when governments around the world deliberately shut down or disrupt Internet services.

How is internet censorship and/or filtering regulated under local laws?

Policies on internet regulation will differ per country and region. Once you identify any bills, laws, or decrees of relevance, you can then check whether there is legality behind your chosen case study and whether the laws adequately protect internet freedom. Existing policies can be benchmarked on how rights-respecting they are by using the three-part test as ascribed under Article 19 of the International Covenant on Civil and Political Rights, which posits that a restriction may be imposed only if it is 'provided by law and are necessary and proportionate: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.



Resources made and recommended by GNI:

1. [Country Legal Frameworks Resource](#) (GNI): Examines governments' legal authorities to intercept communications, obtain access to communications data, or restrict the content of communications in over 50 countries
2. [Manila Principles on Intermediary Liability](#): Framework of baseline safeguards and best practices
3. [Content Regulation and Human Rights Policy Brief](#) (GNI): Uses human rights principles to analyze and inform legal and regulatory efforts to address content challenges
4. [The Consequences of Network Shutdowns and Service Disruptions](#): Available in 12 languages

CASE STUDY

2019 Internet Shutdowns in West Papua

A case study that we can examine together is the [internet censorship in West Papua](#) by the Indonesian government in 2019. Internet access was severely limited and about 700,000 local websites in the province were censored between August and September that year. The Indonesian government justified the censorship by claiming that online discourse in West Papua was “rife with hoaxes”.

This claim, however, should not be taken at face value. Historically, the Papuan people and region have [suffered systemic discrimination from the Indonesian government](#). In fact, the internet shutdown was implemented to stop and discredit the riots in some West Papua cities stemming from an alleged [racially-charged attack against Papuan students in Surabaya](#), one of the country’s biggest cities situated on its main island. Human and digital rights organizations were also active in condemning the shutdowns in both online and offline spaces. In June 2020, the Administrative Court of Indonesia (PTUN) ruled that the internet censorship in West Papua [violated Article 40 of the Electronic Information and Transaction Act](#), and that many of the techniques used by the government went beyond what was legally permitted.

2. Determine the message

Your chosen case study for the campaign will result in several key points that need to be addressed. To determine which messages should be sent to whom, one can ask these questions to the case you have at hand, or use the SMART method to determine which messages should be prioritised. The message should clearly relate to the purpose of the campaign and contribute to your advocacy.

Building a comprehensive case and a compelling message in internet censorship advocacy is crucial to present a nuanced and detailed narrative to the targeted audience. We also recommend that you carry out a SWOT analysis to determine your overall advocacy campaign's strengths, weaknesses, opportunities, and threats to success. By doing so, you will be better equipped in planning future steps in advocating for the cause.

3. Craft the campaign plan

Successful advocacy campaigns are backed by concrete timelines, enumerated outputs, and measurable outcomes. Campaigns can span for as long as you or your organization continues your advocacy, or even be short and built on top of existing campaigns and calls for action.



In crafting your campaign, we recommend completing the Smart Chart by Spitfire Strategies.



In assessing our own organizational capacities and mapping potential partners, we can use the [Framework for Determining Advocacy Capacity](#).

4. Consult with other groups

To confirm your initial data gathering and check for potential biases in your case study, we recommend gathering like-minded organizations and [organizing a working group](#) to analyze the issue(s) at hand. The working group can consist of other human and digital rights organizations, and other sectors such as academe, journalists, and grassroots communities. Ensure that any working group you form is as diverse and inclusive as possible, paying special attention to incorporating underheard and underrepresented voices.

The analysis should aim to unify existing voices and gain context of the case presented from all members of the group, and it should hold the principle of being meaningful, open, and facilitated.

Building a comprehensive case and a compelling message in internet censorship advocacy is crucial to present a nuanced and detailed narrative to the targeted audience. By covering all the bases, you or your organization will be better equipped in planning future steps on advocating for the cause.

5. Identify the stakeholders

Who are the stakeholders of the Internet? A stakeholder is defined as an entity – be it a person or organization – who may be affected by or have an effect on an effort, both direct and indirect.

In advocating for an open internet, we must first understand who are the main stakeholders of the internet to plan our course of action. In 2015, the Internet Corporation for Assigned Names and Numbers (ICANN) identified the following main stakeholder groups for internet governance, including concerns for internet censorship and content filtering. This list can serve as a starting point for your own stakeholder mapping exercise.



GOVERNMENT

The government is one of the most important stakeholders in the internet governance scheme. In many countries, the government is the main regulatory body of internet usage in their jurisdiction; they are capable of directly affecting the internet through a series of laws and policies, and they have the responsibility to train the officials that will oversee the day-to-day usage of the internet and make decisions accordingly. In many internet censorship and filtering cases, governments often play a central role in determining which content may and may not be accessed.



BUSINESS SECTOR

Business sectors on the internet are oriented towards profit, and what that interest looks like varies depending on which sector of the Internet that the Business is working on. In many cases, the Business sectors are both those who hold direct effects and are directly affected by Internet shutdown and content filtering.

- Domain-name company: This includes registrars and registries selling internet domain names, like .com, .org, and .net. Their main interests are ensuring that their domain names remain profitable in the long run, and that might not always be in favor of the public needs. An incident that may be worth noting is the near-sale of Public Internet Registry – which runs the domain .org, the go-to domain for many CSOs and grassroots mobilizing their causes online – to private equity firm Ethos Capital that plans to transform the aforementioned domain registry into a heavily indebted for-profit entity. Had the sale gone through, it would have severely impacted how the domain worked, affecting many online movements of the nonprofits that are registered with the said domain. Many compare the threat of the sale as equal to its own field of censorship, as it effectively silences many communities on the internet.



- Telecommunication companies and internet service providers: As the name explains, these companies facilitate internet traffic and provide internet services and infrastructures. Some are nationalized and/or affiliated with the government, whereas others are fully private and even multinational, operating in several countries. Since their main function and interest is to maintain service providence, they are the key online intermediaries, and as such are particularly important for internet governance. Particularly for internet censorship, the ISP has the power to carry out censorship and content filtering, and often does so whether due to the [government's instructions](#) or [overwhelming public demands](#).
- Internet content companies: Three of the most notable internet content company types are social media companies such as Meta and Twitter; search engines with Google being the most famous example; and content producers like Disney, Netflix, and other streaming platforms. Their business model is very much affected by government arrangements related to data and privacy, and their primary interest is preserving the global outreach and protecting its copyrights globally.

a tool by GNI and BSR provides [A Map of the Tech Ecosystem and Associated Definitions](#).





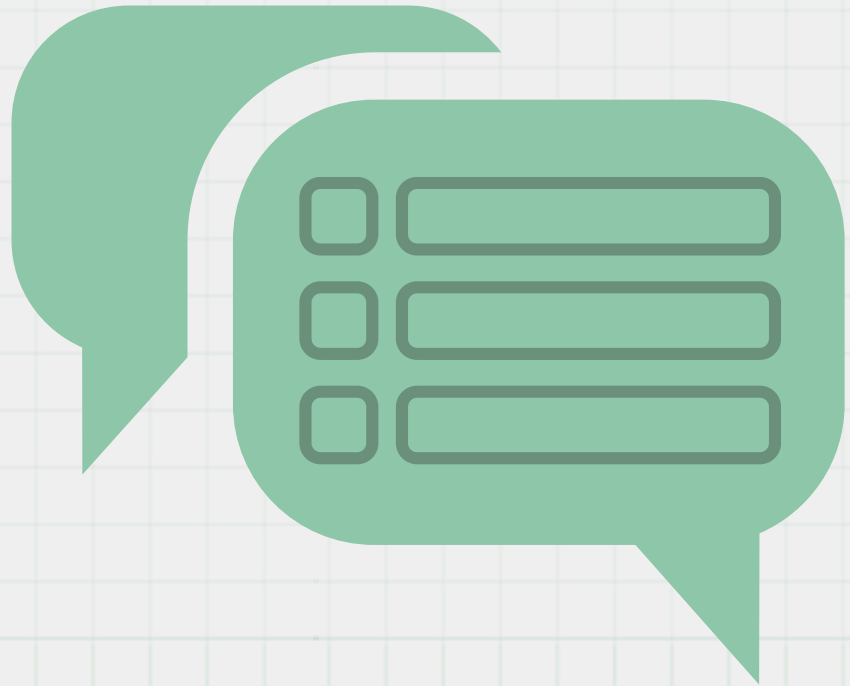
CIVIL SOCIETY

Civil society is often the most affected by the policies of the government regarding censorship and content filtering, as their content – especially the ones containing critics of the government and highlights regarding existing abuse – might be blocked from gaining further viewership and engagement. Civil societies on all levels have been the most vocal and active promoters of a multi-stakeholder approach to internet governance to ensure that rights-respecting principles and accountability remain central to the discussion throughout. However, the main issue in civil societies is the lack of proper coordination and the presence of too many voices, which are sometimes dissonant.



STANDARDS SETTING ORGANIZATIONS

Bodies seeking to guide the development of professional standards that go beyond technical specifications to protect human rights. Examples include the [Internet Engineering Task Force](#), the [World Wide Web Consortium](#), the [Internet Society](#), and the [Internet Research Task Force](#) for those focused on internet governance. International and multi-lateral bodies have also been involved in establishing norms and guidelines, such as [UNESCO's Internet for Trust](#).



6. Engage with stakeholders

WHAT IS A MULTI-STAKEHOLDERS APPROACH?

The Multi-stakeholder approach is a strategy that addresses and engages with all types of stakeholders involved. In this model each stakeholder's input is given equal weight, helping to produce more inclusive policies and dialogue around specific issues. Advocacy strategies incorporating this approach can create an environment where a decision-making process [accommodates the views of the main actors concerned](#) at all stages.

HOW DO WE ENGAGE WITH STAKEHOLDERS?

Different stakeholders will need different plans of engagement in order for them to join your advocacy campaign.

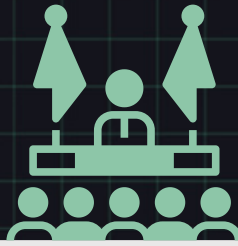
We outline here three kinds of engagement you or your organization can use depending on your targeted audience.



Public engagement is targeted to the general public with the aim to raise awareness regarding internet censorship and content filtering. As the targeted group is often not well-versed in the topic, it is advised to use simpler languages and popular tools and schemes in order to educate them.

Remember – the main goal of the engagement is to educate and update, which may elicit sympathy and care for the cause. Engaging with the public can be made by:

- Public campaigns can take the form of [a social media campaign](#) to reach younger, more tech-savvy audiences that might be particularly vulnerable to the issue, or partnering with traditional news media for newsworthy incidents to update the latest developments and amplify marginalized voices.
- [Running a petition](#) for the general public to support. There is strength in numbers, and a petition can help show urgency and concrete steps that can be done.
- Conducting [advocacy research](#) on the matter, which can be built from previous research as a baseline.



Government engagement focuses on relevant government actors to the cause. Prior to deciding on what to do, we have to first identify specific bodies responsible for the regulation and enforcement of internet censorship & content filtering; this might take the form of a specific Ministry, a focused legislative chamber, or an independent body. Once we have identified these actors and the specifications they deal with, we can plan our engagements accordingly based on the urgency and opportunities presented.



Engagement with corporations and for-profit organizations is focused on demanding accountability and ensuring rights-respecting principles are at the forefront of the existing company practices. [The Global Network Initiative is one of the most successful partnerships](#) that involve multi-stakeholder collaboration towards responsible company decision making in support of freedom of expression and privacy rights. GNI's membership includes ICT companies, civil society organizations, academics, and investors from Africa, Europe, Latin America, North America, and the Middle East.

SPOTLIGHT

Global Network Initiative

The Global Network Initiative is one of the most successful partnerships that involve multi-stakeholder collaboration towards responsible company decision-making in support of freedom of expression and privacy rights. GNI's membership includes ICT companies, civil society organizations, academics, and investors from Africa, Europe, Latin America, North America, and the Middle East.

GNI, in collaboration with Global Partners Digital, has also created the guide "Engaging Tech Companies on Human Rights: A How-To Guide for Civil Society" to support CSO's in engaging with the tech sector around issues affecting human rights.

7. Execute the campaign

Each advocacy campaign should be catered to the needs of the stakeholders you or your organization are trying to engage with. We share below some examples of how others have done their own campaigns and projects that push for open internet.

8. Measure the impact

Determining the success of an advocacy campaign can be tricky, but there are tested methods you can reference to assess your campaign's success. A [Monitor and Evaluation template for digital campaigns](#) can be adopted to help measure the success of the campaign in the public sphere.

For measuring the success of campaigns targeting political and legal changes, you can report updates to your local laws and policies to assess whether your campaign messages have been incorporated by the existing or proposed framework. [GNI has the Country Legal Framework Resource](#) to assist you in capturing the detailed set of resources examining governments' legal authorities to intercept communications, obtain access to communications data, or restrict the content of communications in more than 50 countries.

It is important, however, to acknowledge that impact can take time, particularly in our advocacy for an open internet. Laws are not ratified or drafted overnight, nor are individuals going to become immediate changemakers after being part of awareness campaigns.

CAMPAIGN STORIES

#KeptOn

One of the most notable success cases of internet shutdown campaigns and a case study we can observe in building a successful coalition is [Access Now's #KeptOn campaign](#), which was started in 2016 and has successfully raised awareness and mobilized action against internet shutdowns in various countries.

What makes the campaign so successful is in part due to its coalitions; The campaign builds and maintains coalitions across 105 countries in the world, and focuses on delivering human stories who are affected by the shutdown to the public and relevant stakeholders. It prioritizes inclusion with various actors, and strategically uses these connections by encouraging the members of the coalition to build various campaigns such as grassroots advocacy, direct policy-maker engagement, technical support, and legal intervention. These campaigns are tailored to the needs of the region, yet integrated into a larger, global goal and narrative, making the issue cohesive, contextual, and more nuanced.

CAMPAIGN STORIES

Digisec.directory

Digisec.directory is an open-source digital security directory populated by contributors to EngageMedia's Localization project, which aims to increase the number of digital security resources available in Southeast Asian languages. It also seeks to enhance the capacity of civil society organizations and community groups in the region in identifying and managing digital security risks and threats in their lines of work. The directory includes a list of open-source digital safety and security tools that serve as more rights-respecting alternatives to more mainstream applications. It is available in English and Bahasa Indonesia, and will soon include translations in Burmese, Filipino, Khmer and Thai.

This campaign is notable for its focus on localization and open-source model. By adapting these two core principles, it allows everyone to be able to impart knowledge from these tools, and also contribute to adding more to the directory. This allows a wider outreach with ever-growing resources available.



A Reminder on Measuring Impact

Remember: Impact can take time, particularly in our advocacy for an open internet. Laws are not ratified or drafted overnight, nor are individuals going to become immediate changemakers after being part of awareness campaigns. What matters is persevering throughout the process, and focusing on the end goal.

Be kind to yourselves.

The image features a dark background with a light grid pattern. In the top right and bottom corners, there are decorative geometric shapes consisting of multiple parallel lines forming angular patterns. The text is positioned on the left side of the image.

**EngageMedia.org/
Greater-Internet-
Freedom**