



EngageMedia



Featuring the methodology and guidance from

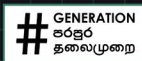


# Through The Looking Glass:

Digital Safety and Internet Freedom  
in South and Southeast Asia

JUNE 2022

Highlighting country reports by





**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.

**The OPTF** is a not-for-profit which supports and builds secure, privacy-enhancing technologies such as the Session messaging app. We also conduct research to inform the civil society community about emerging and ongoing issues in the digital rights space, as well as conducting outreach and education initiatives to support people and organisations to better understand, use, and implement secure and privacy technologies.

**Ranking Digital Rights (RDR)** is an independent research program at the policy think tank New America. RDR believes that transparency is the first step to accountability. RDR evaluates the policies and practices of the world's most powerful tech and telecom companies and studies their effects on people's fundamental human rights.

**The Cambodian Center for Independent Media (CCIM)** envisions a Cambodian society where everybody is well-informed and empowered to strengthen democratic governance and respect for human rights. CCIM believes that a well-informed Cambodian society will expect and demand good governance, and select leaders that will shape the society and economy in a way that will benefit the Cambodian people equitably.

**The Institute for Policy Research and Advocacy (ELSAM)** is a civil society organisation that works to enhance the democratic political order in Indonesia by empowering civil society. Founded in 1993, it actively participates in efforts to promote human rights through policy and legal research, advocacy, and training. ELSAM combines the working methods of human rights think tanks and those of human rights advocacy organisations

with the goal of creating a society that upholds the values of human rights, justice, and democracy, both as set out in laws and regulations, as well as in their implementation and institutionalisation.

**Society for Peace and Democracy** is a non-government organisation that empowers communities through awareness-raising and capacity-building to act and to participate in their own development. Through education and training, the organisation develops knowledge and skills, providing opportunities to advocate for improved policies to ensure human rights, inclusion and collective actions.

**Digital Rights Nepal (DRN)** is a not-for-profit initiative dedicated to the protection and promotion of digital rights in Nepal. It focuses on digital rights issues such as right to online freedom of expression and association, online privacy, access to information, internet governance, cyber laws/policies, and cyber security. DRN is engaged in policy research and advocacy, public awareness campaigns, capacity building initiatives, and creating platforms to provide technical support, in collaboration with relevant stakeholders.

**Out of The Box (OOTB) Media Literacy Initiative** is an educational nonprofit that creates innovative learning tools and experiences that foster media literate Filipinos. It was awarded First Prize in the 2021 Global Media & Information Literacy Awards of the UNESCO MIL Alliance.

**Hashtag Generation** is an antiracist, feminist movement led and run by a group of young, tech-savvy Sri Lankans working towards building a society where everyone has the skills, information, and tools to be active participants in making the decisions that affect their communities, technologies, and bodies. Hashtag Generation mobilises digital media tools to raise awareness and catalyse dialogue on important social justice issues.





## Project Lead

Vino Lucero, Digital Rights and Communications Manager, EngageMedia

## Lead Writer for Regional Report and Framework Designer

Sam de Silva, Oxen Privacy Tech Foundation (OPTF)

## Research Oversight

Egbert Wits, Network Development and Research Manager, EngageMedia

## Research Advisor

Leandro Ucciferri, Global Partnerships Manager, Ranking Digital Rights

## Report Editor

Katerina Francisco, Editorial Coordinator, EngageMedia

## Country Partner Reports

- Cambodia - Cambodian Center for Independent Media: Chhan Sokunthea (*Country Lead Researcher*); Sek Sophal and Mam Vibol (*Country Researchers*)
- Indonesia - Institute for Policy Research and Advocacy (ELSAM): Miftah Fadhli (*Country Lead Researcher*); Shevierra Danmadiyah and Parasurama Ardi Tri Pamungkas (*Country Researchers*)
- Maldives - Society for Peace and Democracy: Adam Shareef (*Country Lead Researcher*); Shimla Ahmed, Ahmed Shifaz Arif, and Mohamed Shumais (*Country Researchers*)
- Nepal - Digital Rights Nepal: Santosh Sigdel (*Country Lead Researcher*); Tanka Raj Aryal (*Country Reviewer*); Rukamanee Maharjan, Saurav Bhattarai, and Sanjina Kshetri (*Country Research Support*)

- Philippines - Out of The Box Media Literacy Initiative Inc.: Alex Valte, Ivanka Custodio, and Hoseia Ibanez (*Country Researchers*)
- Sri Lanka - Hashtag Generation: Harindrini Corea (*Country Research Lead*); Senel Wanniarachchi (*Country Reviewer*)

Published June 2022

This report has been produced by EngageMedia, in partnership with the Oxen Privacy Tech Foundation (OPTF), as part of the Greater Internet Freedom program work in South and Southeast Asia.



# TABLE OF CONTENTS

<b>Through The Looking Glass: Digital Safety and Internet Freedom in South and Southeast Asia</b>	<b>1</b>
Table of Contents	6
Context	9
Approach	10
Limitations	12
Findings	12
Digital Safety Capacity	12
Insights from At-risk Communities	15
Telecommunications Companies Policy Analysis	19
Internet Freedom Analysis	20
Recommendations	20
Strengthening Digital Safety Capacity	20
Addressing Internet Freedom Issues	21
Improving Policies of Telecommunications Companies	22
<b>ANNEX 1: Country Reports</b>	<b>23</b>
<b>Cambodia</b>	<b>25</b>
Digital Safety Capacity Analysis	26
Online Survey – Key Findings	26
At-risk Communities	27
Telecommunications Companies Policy Analysis	29
Metfone	30
Smart	32
Internet Freedom Context	34

<b>Indonesia</b>	<b>36</b>
Digital Safety Capacity Analysis	36
Online Survey – Key Findings	37
At-risk Communities	38
Telecommunications Companies Policy Analysis	41
Telkomsel and XL Axiata	42
Internet Freedom Context	44
<b>Maldives</b>	<b>46</b>
Digital Safety Capacity Analysis	46
Online Survey – Key Findings	47
At-risk Communities	48
Telecommunications Companies Policy Analysis	49
Dhiraagu	49
Ooredoo	51
Internet Freedom Context	53
<b>Nepal</b>	<b>55</b>
Digital Safety Capacity Analysis	56
Online Survey – Key Findings	56
At-risk Communities	58
Telecommunications Companies Policy Analysis	61
Nepal Telecom	62
Ncell Axiata	63
Internet Freedom Context	65
<b>Philippines</b>	<b>67</b>
Digital Safety Capacity Analysis	68
Online Survey – Key Findings	68
At-risk Communities	70
Telecommunications Companies Policy Analysis	74
PLDT/Smart Communications	75
Globe Telecom	76
Internet Freedom Context	78
<b>Sri Lanka</b>	<b>80</b>
Digital Safety Capacity Analysis	81
Online Survey – Key Findings	81
At-risk Communities	82

Telecommunications Companies Policy Analysis	84
Dialog Axiata	85
SLT Mobitel	86
Internet Freedom Context	87
<b>ANNEX 2: Research Framework</b>	<b>91</b>
Context	92
Objective	92
Research Activities	93
Part 1 - Evaluating Digital Safety Capacity	93
Part 2 - Mapping the Internet Freedom Landscape	96





## Context

Digital threats and attacks are impacting the work of human rights defenders and members of at-risk communities in South and Southeast Asia. Simultaneously, internet freedom is being undermined by cyber laws that limit or prohibit secure, safe, and private communications, and has been further eroded through practices and policies of telecommunications companies that fail to protect their customers' freedom of expression and privacy rights.

With the dramatic growth of mobile broadband penetration in South and Southeast Asia,<sup>1</sup> email, messaging apps, and social media have become invaluable tools for human rights defenders' communications and advocacy work. However, the same digital technologies and platforms have also been used to mount attacks against those who are protecting human rights and speaking out against injustices. Sophisticated strategies are being deployed by a range of actors to intercept communications and take over accounts. Cyber laws that are intended to improve safety online are often used to criminalise activities that criticise governments. Online harassment and cyber violence against human rights defenders and at-risk communities are on the rise, demoralising them and dramatically impacting the work they do.

There is an urgent need for civil society and organisations that support and strengthen democracy, including donors and policy influencers, to better understand how internet freedom restrictions and digital attacks impact the protection and promotion of human rights and democratic principles.

---

1. <https://www.geopoll.com/blog/mobile-penetration-asia-south-asia-southeast-asia/>

# Approach

This report is informed by local inputs from six countries – Cambodia, Indonesia, the Maldives, Nepal, the Philippines, and Sri Lanka. To gather these inputs, we commissioned country reports from the following leading digital rights organisations:

- Cambodian Center for Independent Media (Cambodia)
- The Institute for Policy Research and Advocacy – ELSAM (Indonesia)
- Society for Peace and Democracy (Maldives)
- Digital Rights Nepal (Nepal)
- Out of The Box Media Literacy Initiative, Inc. (The Philippines)
- Hashtag Generation (Sri Lanka)

This report synthesises the findings from the country reports, contains a summary of trends and offers recommendations. The bulk of the research in the country reports was gathered between November 2021 and January 2022, and was guided by a common research framework (found in Annex 2). Individual country reports are found in Annex 1.

The other key stakeholders participating in this report and its research are:

- EngageMedia – lead organisation responsible for the research and the report
- Oxen Privacy Tech Foundation (OPTF) – key partner responsible for designing and coordinating the research process and producing the high-level report, including the recommendations
- Ranking Digital Rights (RDR) – key partner responsible for assisting country partners with the analysis of telecommunications companies’ public policies in target countries

The research framework was designed to:

**1. Identify the gaps and needs related to digital safety capacity among human rights defenders and at-risk communities**

Country partners used online surveys, key informant interviews with at-risk communities, and desk research to produce specific country reports. They received a model online survey, guiding questions, and guidance from EngageMedia and OPTF; however, they were requested to provide input and contextualise research criteria based on their own understanding of the local situation. Country teams were also given flexibility in determining which at-risk communities to include in the analysis.

**2. Understand internet freedom contexts and issues**

Country partners were requested to use their own knowledge and desk research to provide further details about the internet freedom situation in their countries. Data gathering was structured by country partners commenting on internet access, censorship, online harassment and hate speech, disinformation, and use of circumvention technologies.

**3. Identify gaps in the public policies of telecommunications companies related to freedom of expression and privacy**

EngageMedia used Ranking Digital Rights' Corporate Accountability Index methodology,<sup>2</sup> adapting it to the regional context to evaluate the public policies of telecommunications companies. RDR provided guidance and materials to the country partners, facilitating the data collection and analysis of their findings.

More details about the research framework can be found in Annex 2.

---

2. <https://rankingdigitalrights.org/methods-and-standards/>

## Limitations

The research by country partners and the compilation of this report were conducted under less than ideal conditions.

COVID-19 was still having a high impact in the six target countries and on our partners during the research phase. It was difficult for many of them to conduct physical meetings and most research activities were conducted online. While most partners were able to fulfil the research as required, we experienced unforeseen delays which resulted in some gaps in research. Despite this, this report paints a comprehensive picture of the digital safety and internet freedom conditions in South and Southeast Asia.

## Findings

The overall findings of this report provide a pessimistic picture of the regional situation, with many human rights defenders and at-risk communities vulnerable to digital attacks. Research findings from each country partner tell a similar story:

- There is a significant skills and knowledge gap about digital safety among human rights defenders and at-risk communities;
- The high level of online harassment and hate speech has a detrimental impact on human rights defenders and at-risk communities;
- Cyber laws are not protecting human rights defenders against digital attacks – instead, they are often used against human rights defenders;
- Telecommunications companies do not have (or are not interested in having) adequate policies to protect subscribers' rights in terms of freedom of expression and privacy.

## Digital Safety Capacity

The digital safety capacity of human rights defenders is paramount in our increasingly digitally driven world. In order to evaluate digital safety capacity, country partners surveyed human rights defenders and interviewed at-risk communities to understand their use of

digital technologies and gaps in their digital safety practices. While the numbers, demographics, and at-risk communities surveyed and interviewed by each country partner differed, there is enough similarity to synthesise research results into meaningful findings about technology use and digital safety practice. The summary of the responses from the six partner countries to key topics from the online survey are documented below.

### **Use of communications apps (Email, Messaging, Collaboration, and Meetings)**

When it comes to **email**, more than 90% of respondents from each of the six countries indicated they used Gmail. There was some use of ProtonMail – a secure email platform – however, this was insignificant when compared to Gmail's dominance.

The most popular **messaging apps** were WhatsApp and Facebook Messenger, with Telegram also being frequently used in some countries. The Signal private messaging app, which is highly recommended by digital security trainers, has a low level of use. Human rights defenders, like ordinary users, are more likely to use platforms that are already popular with their networks, which could explain its low use. While Signal is slowly gaining traction, it has a long way to go when it comes to mainstream adoption.

For **online collaboration and meetings**, Zoom and Google Meet are the most used platforms. Jitsi, a video conferencing/meeting platform highly recommended by digital security trainers, is hardly used by survey respondents. More research is required to understand the reasons for this; however, it is likely that Jitsi is not used by a large enough critical mass to warrant its adoption by human rights defenders.

### **Digital attacks**

Majority of respondents indicated they were concerned by digital attacks that included account takeovers, malware attacks, online harassment, hate speech, doxing, and online gender-based violence.

The digital attacks that most respondents across the six countries experienced were online harassment, hate speech, and online gender-based violence.

Respondents recognised that both state and non-state actors perpetrate digital attacks. Across a number of countries, pro-government groups and religious fundamentalists were identified among the non-state actors that posed a threat to human rights defenders.

Respondents indicated that they had low levels of capacity to counter or protect themselves from digital attacks – both the attacks that they were most concerned about and those that they had directly experienced.

### **Passwords and Two-Factor Authentication (2FA)**

Respondents expressed a medium level of confidence regarding their password strength.

The use of 2FA varied across countries, with approximately 50% of survey respondents indicating they used it on some of their accounts. However, as indicated by the Sri Lanka report, 2FA may not be used or clearly understood by non-English-language human rights defenders.

### **Countering online surveillance**

Less than 10% of respondents indicated they had the ability to browse the internet anonymously without leaving a digital trail (e.g., Using TOR browser or a virtual private network).

### **Digital safety skills and digital safety training**

More than half of the respondents indicated that they had low levels of digital safety skills.

The vast majority of respondents did not receive any digital safety training in 2020 and 2021. However, for Cambodia and Indonesia, approximately 50% of respondents indicated that they had attended digital safety workshops.

Despite this, only 12% of respondents from Cambodia indicated they had a high level of digital safety skills, and none of the respondents from Indonesia. While more research is required to understand this phenomenon, it could be attributed to training curricula not aligned to participant needs, and to a tendency for trainers to assume higher levels of information and communication technology (ICT) skills and technical understanding among participants, resulting in them simply not fully understanding the training material.

## Insights from At-risk Communities

At-risk communities are often targets of concerted digital attacks. Country partners conducted key informant interviews with at-risk communities to further understand the type of digital attacks they faced, and their capacity to respond to such attacks. Representatives from the following at-risk communities were interviewed by country partners:

- Indigenous youth; university students (Cambodia)
- Civil society groups; journalists and media houses (Indonesia)
- Journalists (Maldives)
- Women journalists; LGBTIQ+ community (Nepal)
- Food security advocates (Maginhawa Community Pantry) and women activists; LGBTIQ+ community (Philippines)
- Muslim women activists/politicians; LGBTIQ+ community (Sri Lanka)

Responses from the interviews echoed the results of online surveys that were deployed by each country: digital safety skills are critically low, and at-risk communities need to have greater opportunities to participate in skills-strengthening programs.

The interviews also indicated that online hate speech and harassment were key issues that significantly affected the mental health and wellbeing of human rights defenders.

Below are some key takeaways that are important to highlight for each at-risk community.

## **Indigenous communities (Cambodia)**

- They are vulnerable to online discrimination and attacks, primarily because of the lack of education about social media and digital safety skills.
- Practising digital safety may not be a high priority for these communities. The reasons for this require further investigation.
- Other issues of concern include being asked to join offensive Facebook groups, forgetting account passwords, and social media accounts being hacked.
- The younger generation is interested in using smartphones to produce videos and news reports. They are also in a better position to practise digital safety than their elders, because they are more technology savvy and have grown up with mobile devices.

## **University students (Cambodia)**

- Students are highly concerned about Facebook hackings, sexual messages, and cyber bullying. They have also experienced other digital attacks such as requests by strangers for private information, impersonations, and requests to join dodgy chat rooms.
- There may be a lack of willingness to improve digital safety skills among this group. An interviewee indicated that if one's social media account is taken over by strangers, then the response is to create a new account.
- If students encounter problems, they turn to friends with better ICT skills to help solve these problems.

## **Journalists and media houses (Indonesia)**

- Journalists are highly vulnerable to digital attacks, equally from both state and non-state actors. They face a wide range of threats including hate speech and doxing.
- Media houses have experienced hacking and website defacing.
- Despite having a high level of ICT capacity, digital safety practice remains low among journalists. There is a reluctance to move away from familiar platforms to safer platforms such as ProtonMail, Signal, and Wire.



## **Journalists (Maldives)**

- Journalists face heightened risk of online intimidation and abuse. Greater risks will occur during politically charged times – for example, elections and religious tensions.
- Government conducts no investigations and offers no protection from these threats.

## **Women Journalists (Nepal)**

- The digital attacks women journalists experience include online harassment, threats, intimidation and bullying, hate speech comments, sexting, trolling, and online impersonation. Attacks are often aimed at both women journalists and their family members.
- Online gender-based violence, including sexting, is sometimes perpetrated by male journalists and colleagues in the newsroom. Other non-state actors digitally attacking women include religious, business, anti-feminist, and political groups.
- Newsrooms tend not to prioritise the digital safety of women, and do not provide them with support when they experience online harassment and other digital attacks.
- Women journalists generally lack the technical literacy and digital safety knowledge to assess risks and counter threats and attacks.

## **LGBTIQ+ community (Nepal)**

- The LGBTIQ+ community is generally at a heightened risk of digital attack, with the digital space reflecting and magnifying offline vulnerabilities, inequalities, and discrimination. Intra-community threats also need to be addressed.
- Incidents of online harassment, trolling, blackmailing, and doxing are on the increase.
- Digital attacks come from conservative members of the Nepalese society, but also from within the at-risk community itself.
- Digital platforms are important for LGBTIQ+ community members to find partners, but lack of technical know-how and digital safety skills put them at high risk.
- Understanding of the importance of digital safety is quite low within the community and it has not been a priority for them.

## **Food security advocates and women activists (Philippines)**

- Digital threats disproportionately affect both food security advocates and women activists, with threats including cyber bullying, online gender-based violence, hate speech, account takeovers, online impersonation, and doxing.
- Online and offline threats and harassment are coming from police, military, and non-state actors.
- Gender compounds the frequency and severity of digital threats – particularly of hate speech and gender-based violence. The use of Facebook’s built-in reporting tools have had no real impact.
- There is a strong willingness to practise digital safety; however, more focused capacity building is required.

## **LGBTIQ+ Human Rights Defenders, and the LGBTIQ+ Community (Philippines)**

- The LGBTIQ+ community and their supporters are highly vulnerable to digital threats, particularly online gender-based violence, bullying, and hate speech. They are targeted by both state and non-state actors who aim to demean and sow hate for the LGBTIQ+ community and their supporters.
- LGBTIQ+ defenders tend to have more digital safety skills than the broader LGBTIQ+ community; however, defenders are often attacked on social media, and accused of being communists and terrorists.
- There is a need for more training opportunities for both the broader LGBTIQ+ community as well as the LGBTIQ+ defenders.

## **Muslim female activists/politicians (Sri Lanka)**

- Women activists and politicians from the Muslim minority experience online attacks through social media platforms. These attacks include harassment, hate speech, and bullying.
- Muslim female activists experience derogatory and misogynistic comments online and their personal images are sometimes altered and shared. Their daily movements are also tracked and commented upon on social media, which can lead to further offline violence.
- Perpetrators may be established male Muslim politicians, but can also be conservative Muslim women, politicians from other parties, and ordinary people.

- Very few members of this at-risk community have high levels of ICT skills. Most are unaware of digital safety practices, although there is a willingness to learn.
- An enhanced system for reporting online hate speech and social media threats is needed.

### **Transgender people (Sri Lanka)**

- Transgender people face higher rates of online harassment, hate speech, trolling, and doxing than the general population.
- Digital attack perpetrators are often known to them. Digital attacks have a detrimental impact on their work and personal lives and can result in offline harm and violence.
- Transgender people have low levels of digital safety skills and limited awareness of the need to practise digital safety, as these skills are often perceived as 'too technical' or 'too difficult'.

## **Telecommunications Companies Policy Analysis**

Country partners used a subset of indicators selected from the Ranking Digital Rights (RDR) methodology to analyse the public policies of popular telecommunications companies in their countries, namely the Terms of Service (sometimes referred to as Terms and Conditions) and the Privacy Policies.

This was the first time such an analysis has been carried out in the region, and each country report presents key takeaways related to the findings that analyse privacy and freedom of expression indicators in the public policies of telecommunications companies.

It should be noted that rights-based advocacy aimed at the private sector is not heavily practised in the target countries, and feedback from the country partners suggest that there has been little or no interaction with the telecommunications sector about issues related to freedom of expression and privacy.

The findings from the RDR research is a useful first step in enabling civil society organisations to contact and engage private sector telecommunications companies to

improve their terms of service agreements and privacy policies, and to be transparent about their policies in relation to internet freedom.

## Internet Freedom Analysis

For this report, we requested country partners to tap into the research they conducted as well as their own experiences. They then analysed internet freedom in terms of access and censorship indicators, as well as other indicators, such as the impact of hate speech, surveillance, and false and harmful information flows that negatively affect internet freedom.

The general takeaway from the analysis is that there is a need to be vigilant about internet access and censorship. However, other factors such as hate speech and laws enacted to moderate and control content on the internet are also resulting in online self-censorship and restricting human rights defenders from confidently accessing and using the internet.

## Recommendations

The following recommendations are intended as action steps for civil society organisations (CSOs), including media support and training organisations, legal and policy organisations, and digital rights organisations. These recommendations aim to positively impact digital safety and internet freedom across South and Southeast Asia.

### Strengthening Digital Safety Capacity

- Responding to hate campaigns: There is an urgent need for dedicated training programs focused on addressing online harassment, hate speech, doxing, and other forms of attacks that target users by sending them messages and images through their social media channels. Such training programs must provide practical strategies that minimise the mental health impacts of defenders who are vulnerable to hate campaigns.

- Assessing needs: CSOs must invest more time and effort in understanding the requirements of at-risk communities, and designing digital safety program curricula that specifically address their needs.
- Localising training programs: Training program curricula must be designed and localised to better address participants' needs and concerns, using examples and case studies they can relate to. CSOs must avoid using generic digital safety programs that have not been customised to fit the local context.
- Maximising safety adoption: Training program design must take into account participants' varying levels of ICT literacy, and provide adequate time for participants to understand the concepts and put these into practice, and conduct follow up programs.
- Using appropriate trainers: Programs must be delivered by trainers who are best suited to effectively engage with the participants. This could mean trainers who speak participants' local languages, or women trainers for women participants. Specific training programs organised along gender and cultural/ethnic lines should also be considered.

## Addressing Internet Freedom Issues

- Communicate the futility of internet shutdowns and throttling: CSOs should form coalitions with the private sector, including tech companies and social media advertisers, and carry out campaigns to educate and improve awareness among parliamentarians and government officials about the negative impacts of blocking internet services.
- Access during shutdowns: CSOs should deliver training programs on using virtual private networks (VPNs) and other strategies to bypass internet shutdowns, throttling, and other forms of online censorship. They should consider investing in technologies such as satellite internet connections that facilitate internet connectivity without being dependent on local providers.
- Responding to hate speech: CSOs should leverage local and international laws to prosecute perpetrators.
- Advocate for improved cyber laws: Laws related to the internet, including social media, must not be ambiguous and must protect human rights defenders and at-risk

communities, especially in terms of freedom of expression, privacy, and preventing online hate speech and harassment. CSOs should form coalitions with the legal community to advocate for improved cyber laws.

## Improving Policies of Telecommunications Companies

- Pressure companies to increase transparency: CSOs should advocate for easy access to telecommunications companies' Terms of Use and Privacy Policy statements, along with versions adapted to local languages. They should strive to explain the provisions of these policies to non-technical audiences (using plain language and explaining technical concepts where needed).
- Strengthen relationships: CSOs should engage telecommunications management and board members to build and strengthen relationships. Most private sector organisations are interested in discussing their commitment to the United Nations Sustainable Development Goals, where Goal 16 has indicators that refer to freedom of expression<sup>3</sup> as well as the UN Guiding Principles on Business and Human Rights.<sup>4</sup>
- Align policies with local laws: CSOs should push to have companies' Terms of Use and Privacy Policy statements aligned with domestic laws on privacy rights. For example, data protection and consumer protection laws may restrict telecommunications companies from sharing user data with third parties.
- Educate and increase awareness of telecommunications companies: CSOs should engage the management and staff of telecommunications companies about the importance of respecting and protecting freedom of expression and having clear policies that protect user privacy, especially in the event of user data requests from government agencies.
- Institute ongoing assessments: CSOs should work with organisations such as RDR and donors to ensure regular engagement with telecommunications companies and assessments of their public policies and positions in relation to freedom of expression and privacy indicators.<sup>5</sup>

---

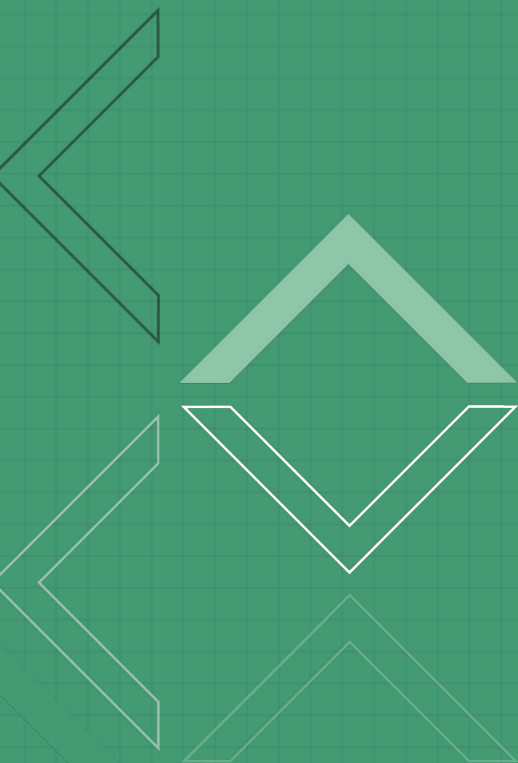
3. For more information, refer to <https://ifex.org/sustainable-development-goals-sdgs-what-role-for-freedom-of-expression/>.

4. For more information, refer to [https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr\\_en.pdf](https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf).

5. See the Annex for a list of the RDR indicators used in this report.



# **ANNEX 1:** **COUNTRY REPORTS**



From November 2021 to January 2022, the six country partners conducted research and produced reports on the digital safety capacity of human rights defenders and at-risk communities, as well as the internet freedom context of their countries. These reports include an assessment of popular telecommunications companies against a set of indicators that measure freedom of expression and online privacy.<sup>6</sup>


It should be noted that the research is presented for analysis by the reader. We have not included recommendations for each of the countries. A summary of the trends across the countries, along with key recommendations, can be found in the main section of this report.

This Annex contains edited versions of the six reports produced by the country partners.

---

6. See the Methodology section in the Annex 2 for more details.





# CAMBODIA

## CAMBODIAN CENTER FOR INDEPENDENT MEDIA (CCIM)

The past five years have seen a steady decline in freedom of expression. This has followed the coordinated crackdown on independent media in mid-2017, when over 30 independent radio stations were shut down by the Cambodian government.

With almost all independent media institutions eradicated, Cambodian people have been forced to rely largely on social media and other online platforms to access news and information.

The vulnerability of this reliance became apparent in early 2021, when the government issued a sub-decree to establish a National Internet Gateway (NIG) – a China-style firewall – which would create a single point of entry for all internet traffic under the government’s control. This poses a huge threat to internet freedom in Cambodia, and is yet another indication of the government’s intentions to suppress access to information and freedom of expression. Journalists, activists, and civil society organisations (CSOs) are particularly at risk, as are the vulnerable groups they support through their advocacy efforts surrounding human rights, media freedom, and democracy.

# Digital Safety Capacity Analysis

In response to declining internet freedom in Cambodia, the Cambodian Center for Independent Media (CCIM) conducted an online survey of internet users, with a focus on gauging the digital safety capacity of human and environmental rights defenders, including activists, journalists, media producers, policymakers and lawyers. Survey responses were received from 34 individuals with backgrounds primarily in media and journalism (56%), human rights (23.5%) and environmental issues (15%). Of the respondents, 60% identified themselves as male, 37% identified as female, and 3% indicated that they did not want to reveal their gender.

## Online Survey – Key Findings

- **Use of email platforms:** Gmail is by far the most popular email platform, used by 97% of respondents, while 12% of the respondents also indicated they had Outlook accounts.
- **Use of messaging apps:** The most popular instant messaging apps are Facebook Messenger and Telegram. Interestingly, usage of WhatsApp was low, with the use of Signal being slightly higher than WhatsApp.
- **Digital attacks:** The digital attacks that were of most concern to respondents were account takeover, online impersonation, online surveillance, online harassment, and hate speech. In terms of actual experiences, a high percentage of respondents indicated they have been harassed or subjected to hate speech and online gender-based violence.
- **Threat actors:** Respondents indicated greater concern over state actors compared with non-state actors. 44% indicated they had some or high levels of concern about state actor attacks, compared to 24% expressing some concern about attacks from non-state actors and 36% indicating they had no concern about attacks from non-state actors.
- **Protecting against digital attacks:** Over 60% reported having low capacity to protect themselves from the digital threats and attacks they highlighted as most concerning.

- **Passwords:** Only 50% of respondents are confident about the strength of the passwords they use to access important devices and accounts. However, 50% of them use two-factor authentication (2FA) on all or most of their accounts, with many reporting that it is one of the digital security skills they have learned from digital safety training programs.
- **Online censorship:** Over 64% of respondents have faced censorship and blocks on websites and apps they wished to access to some level. Only 1% of respondents indicated having high capability to access censored or blocked content.
- **Online surveillance:** Only 2% of respondents indicated they have a high level of capability to browse the web anonymously using TOR or a virtual private network (VPN).
- **Use of collaboration and online conference calling platforms:** Zoom and Google Meet are the most used platforms. Jitsi is used by a small proportion; however 52% indicated they never use it. 33% indicated they had a low level of confidence collaborating or participating in online conferences safely and securely.
- **Digital safety skills:** 12% of respondents indicated having a high level of digital safety skills, with a further 59% indicating they had a medium level and 29% indicating a low level of skills.
- **Digital safety training:** 59% of respondents indicated having attended a digital safety training in the last 24 months.

## At-risk Communities

To gain a deeper understanding of the specific vulnerabilities of at-risk communities to mounting digital threats, CCIM got in touch with youth representatives (aged between 17 and 22 years) from two at-risk communities: a group of indigenous people in Ratanakiri province, and a group of university students in Siem Reap province.

## **Indigenous communities**

Indigenous people in Cambodia are particularly vulnerable to online discrimination and attacks for three primary reasons:

1. Lack of sufficient education around social media and digital skills;
2. Lack of reliable, easily accessible, and comprehensible sources of information;
3. Their marginalised ethnic identity.

When asked to describe the level of ICT skill that their community has, responses from all nine of the young indigenous people interviewed ranged from “zero” to “poor”. They also all reported that, despite being more likely to fall victim to digital attacks, indigenous people seem not to be interested in learning tips that might improve their digital safety. While this was unanimously agreed upon, none of the interviewees were able to pinpoint the reason why this is the case.

Specific challenges reported anecdotally by the interviewees include being invited to join inappropriate or offensive Facebook groups, forgetting account passwords, social media accounts being hacked, and a general inability to use many phone applications properly.

The younger generation of indigenous people is in a better position than their elders in terms of digital safety, thanks to the proliferation of digital and media literacy trainings aimed at young people from CSOs, such as the Cambodian Youth Network (CYN) and Transparency International Cambodia (TI-Cambodia), and environmental activists. Still, interviewees declared that more specific training on using social media safely and responsibly are required. They also expressed a desire to learn how to use media as part of their freedom of expression advocacy efforts, reporting that many young people in the area are interested in producing videos and writing news reports using their smartphones.

## **University students**

Facebook hackings, sexual messages, and cyber bullying are the three most critical digital concerns for university students, according to the nine individuals involved in this

focus group discussion. These threats were thought to primarily come from friends on social media, strangers, scammers, and internet service providers.

Actual experiences of attacks reported by interviewees include requests by strangers for private information, impersonation, suspicious links, and requests to join dodgy chat rooms. All of these have the potential to be extremely dangerous.

Respondents suggested that university students are particularly vulnerable to digital threats and attacks for a range of reasons, including a lack of understanding and critical thinking, habits and behaviours surrounding social media, the society or community they live in, and poor ICT skills – which were reported as ranging from “low” to “medium”.

The primary reason given for such low skills and a lack of willingness to improve them was that university students simply do not care about their digital safety. For example, an informant indicated that if a student's social media account is hacked or taken over by strangers, they will simply create a new account.

When issues do arise, most university students tend to turn to someone who they think might be able to deal with them (i.e., friends with better ICT skills than their own).

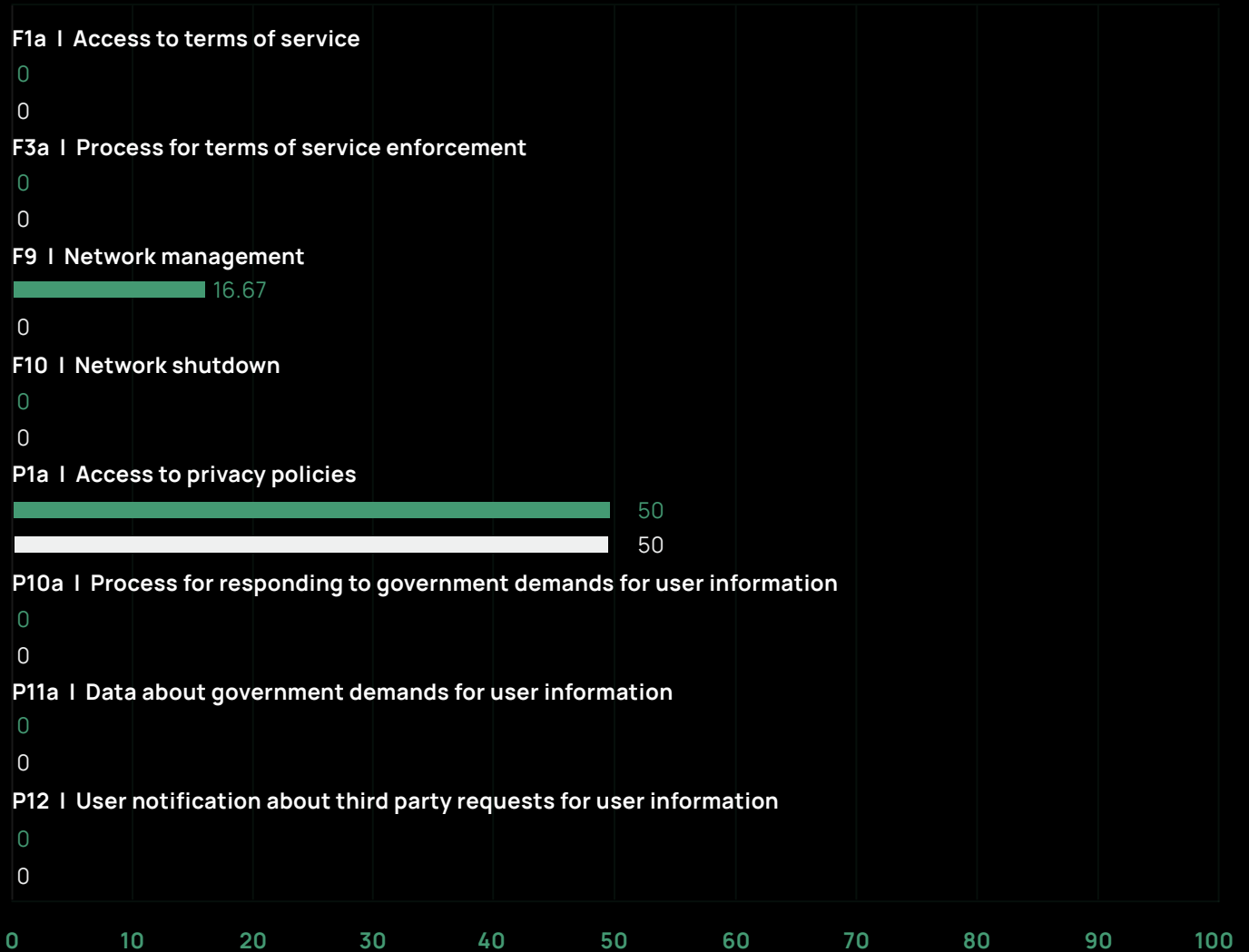
All nine of the university students interviewed had, at some point, attended a training on media literacy. All students reported being very interested in attending more training programs on this topic, in particular to learn about online safety and privacy, digital security, information verification, photography and photo-editing skills, and how to counter cyber bullying, hate speech, and sexting.

## **Telecommunications Companies Policy Analysis**

The two charts below are generated from data associated with the RDR indicators used in this research. The indicators measure the publicly available policies of the telecommunications companies in relation to freedom of expression and privacy. Please refer to Annex 2 for more information about the RDR indicators and the scoring process, or visit <https://rankingdigitalrights.org/2020-indicators>.

## Metfone | Cambodia

■ Mobile    ■ Fixed-line broadband



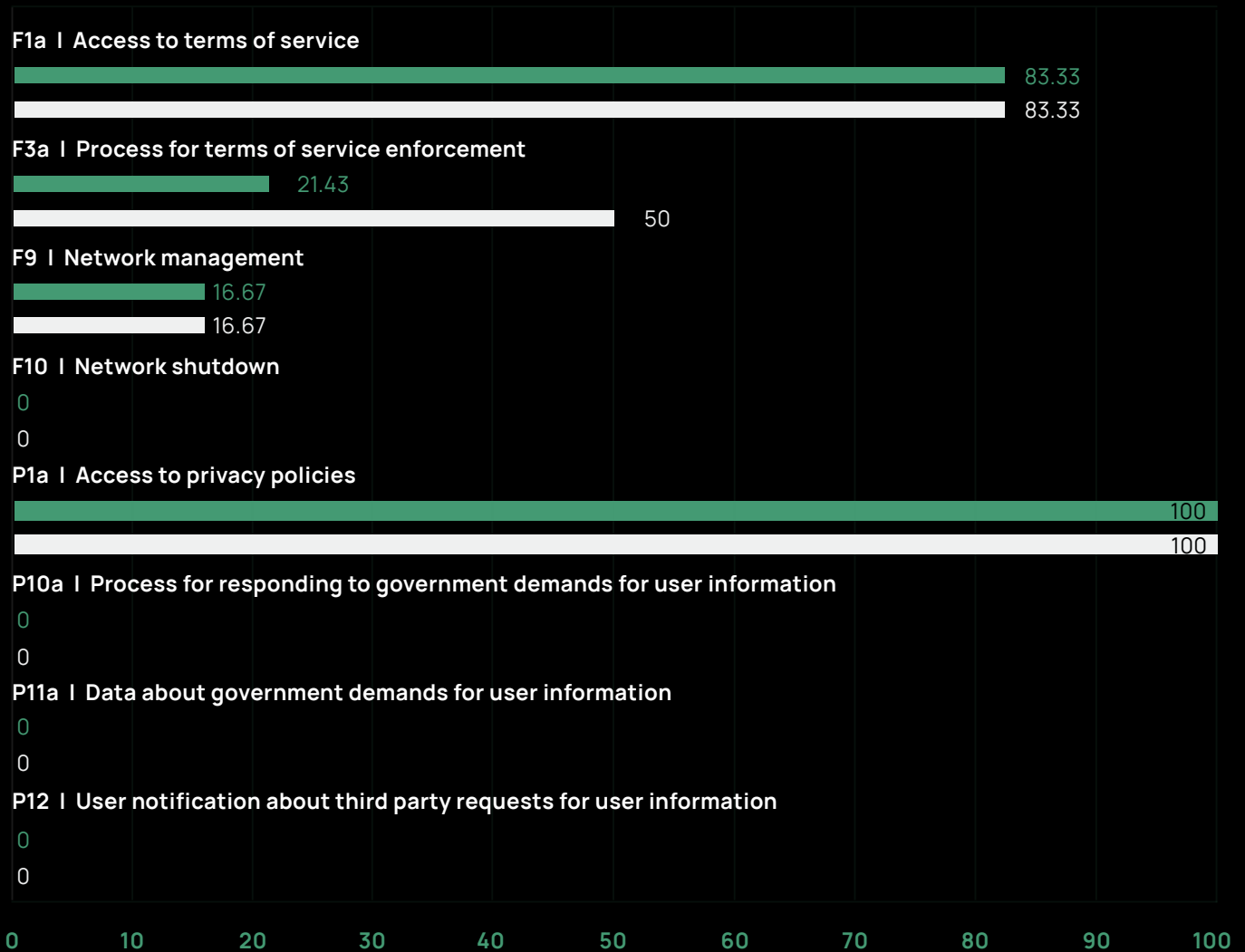
## Key takeaways

- Metfone does not have a Terms of Service policy that could be accessed; however, a short and broad Privacy Policy could be found only in English rather than in Khmer language for local people in Cambodia to read and understand.

- Since the disclosure of public policies in relation to Terms of Use is not available on the company's website, there is no information on how the company acts on government requests to flag content. Without mentioning clear processes on how the company will respond to such requests, Metfone has room to manoeuvre in response to government requests to shut down or block internet services.
- The company claims it will not pass private information about its users to third parties, including government authorities. However, the policies related to the proposed National Internet Gateway will enable the government to have full access to private information about all internet users in Cambodia.

## Smart | Cambodia

■ Mobile ■ Fixed-line broadband



### Key takeaways

- Smart Axiata’s Terms and Conditions are easy to find on its website and are available in both English and Khmer. However, it is difficult to understand due to the technical and legal terms used in presenting terms of services. It should also be noted that the Terms and Conditions state: “The English version will prevail over any translation.



The Subscriber acknowledges that it has had the opportunity to review a Khmer translation of the GTCs or to go to Smart website.”

- Privacy policies are easy to find on its website. The privacy policies are available in both English and Khmer and written in an understandable manner. In section 5 of the Privacy Policy, titled 'Disclosure of Personal Data', the company states: “We keep your personal data confidential and do not share it with any third party or government authority, except under the following circumstances: a) to meet our legal and regulatory obligations, including to prevent and/or detect crime; b) to enforce and/or safeguard our rights, usage terms, intellectual/physical property, our safety or of associated parties; c) if we are acquired by or merged with any other company; or d) for any legal claim, where we are required to do so.” However, the policy does not include information about the process the company follows to respond to non-judicial government demands or court orders. Equally important, there is no disclosure found related to international data transfer. In section 6 of the Privacy Policy, titled 'Cross Border Data Transfer', the company states: “We do not sell, trade, transfer or otherwise share your personal data, except: (...) b) as required by law, such as in conjunction with government inquiry, litigation or similar legal processes. However, the policy does not include information about the process that the company follows to respond to government demands from foreign jurisdictions.” Within this context, it is still possible that the company might pass the private information of its Internet subscribers to the government if required to do so.
- It should be noted that Smart will also be required to comply with the proposed government's National Internet Gateway policies, and in this context, user information will be directly accessible by government authorities.

## **Trends and Concerns for Reviewed Telecommunications Companies in Cambodia**

- Linguistic accessibility of terms and conditions for reviewed companies can still be improved further, to ensure that users from all backgrounds can fully understand the fine print of the terms.
- While in varying levels, both companies reviewed can also work on improving

disclosures on how they protect their users' privacy and data, especially amid concerns about government authorities requesting access to user data. It is imperative for the companies to clearly and thoroughly state their privacy policies and stances related to key privacy concerns so users can be fully aware of this when they use the companies' services.

- The impact of the government's internet gateway policies on the telecommunications companies' policies is of major concern for civil society. Further research can be done on how the companies' disclosures and action will be affected by the government's internet gateway policies as time goes by.

## Internet Freedom Context

Cambodia's internet freedom will be severely impacted when the NIG is implemented. The NIG not only enables authorities to control internet access and impose censorship, but will also assist in monitoring users and their online behaviour. Needless to say, it will have a detrimental impact on independent journalists, activists, and civil society organisations working on human rights, good governance, and democracy.

Even without a centralised NIG, there is ample evidence that there are tight controls over internet activities by government authorities. In March 2020, Cambodia's Ministry of Information established a Fake News Monitoring Committee that had the power to monitor social media as well as "block websites, accounts, or pages that promote false information that cause social unrest".<sup>7</sup> In April 2020, the government used the COVID-19 crisis as cover to pass laws that would give them the ability to censor the media.<sup>8</sup> During the same month, the popular online news channel TVFB was blocked and its editor-in-chief arrested for allegedly inciting social disorder after he shared comments made by the country's Prime Minister on informal workers and their hardships.<sup>9</sup>

There is no doubt that the proliferation of hate speech is a massive problem in the country. Research by Licadho indicates that the government itself is "one of the most

---

7. <https://opendevelopmentcambodia.net/announcements/decision-on-the-establishment-of-fake-news-monitoring-committee/>

8. <https://rsf.org/en/cambodia-hun-sen-uses-covid-19-crisis-tighten-his-grip>

9. <https://vodenglish.news/news-site-blocked-journalist-jailed-after-quoting-hun-sen/>

visible perpetrators of online harassment” in the country.<sup>10</sup> Laws related to ‘fake news’ have been weaponised against journalists and government critics, with Human Rights Watch documenting 30 arbitrary arrests in early 2020.<sup>11</sup>

The power and control over internet freedom that the NIG will give the government is deeply concerning, especially in the context of general elections earmarked for 2023. Critical voices are already restricted, and if the public are fearful that their online conversations can be easily monitored, there will be little debate or discussion about the future direction of Cambodia.

---

10. <https://www.licadho-cambodia.org/reports.php?perm=235>

11. <https://www.hrw.org/news/2020/04/29/cambodia-covid-19-spurs-bogus-fake-news-arrests>



# INDONESIA

## THE INSTITUTE FOR POLICY RESEARCH AND ADVOCACY (ELSAM)

Indonesia is ranked [48/100 in the Freedom on the Net 2021 report](#), which also categorises the country as 'partially free' in terms of internet freedom. Human rights defenders have continuously faced obstacles in the offline world and, increasingly, online through various forms of digital attacks by state and non-state actors. There have been numerous cases of internet throttling and shutdowns, including the use of cyber laws to stifle government criticism and freedom of expression.

### Digital Safety Capacity Analysis

In response to the rising cases of digital attacks in Indonesia, ELSAM conducted an online survey of internet users, with a focus on communities particularly at risk of digital attack, including journalists, civil society groups, and human rights defenders and activists. Survey responses were received from 18 individuals, 6 of whom identified as women and 12 identified as men. Their backgrounds are primarily in human rights, journalism, and digital rights. Two of the respondents indicated they were from rural areas.

## Online Survey – Key Findings

- **Use of email platforms:** Gmail is by far the most popular email platform, used by 93% of respondents.
- **Use of messaging apps:** WhatsApp was found to be the most popular messaging app. The majority of respondents indicated that encryption and anonymisation features were important considerations when choosing a communication platform. With this in mind, it is interesting that Signal and Wire were not popular choices among the respondents.
- **Digital attacks:** None of the survey respondents indicated they had experienced a digital attack. However, according to SAFEnet data, the most common form of digital attack among civil society groups is hacking (70%), predominantly by taking over WhatsApp and Instagram accounts. Meanwhile, doxing makes up approximately 13% of digital attacks.
- **Protecting against digital attacks:** The majority of respondents reported having low capacity to deal with digital threats. 46.7% of respondents also admitted that they rarely use software or strategies to improve their digital security. Meanwhile, 20% said they did not know, suggesting even wider rates of non-usage.
- **Passwords:** 60% of respondents reported rarely using password management applications.
- **Online surveillance:** Monitoring and surveillance was one form of digital threat of which respondents had significantly less knowledge and awareness. Just over half of respondents claimed to have adequate ability to use browsers anonymously.
- **Use of collaboration and online conference calling platforms:** WhatsApp, Zoom and Google Meet are the three most used applications for making conference calls.
- **Digital safety skills:** None of the respondents felt that they had high or very high digital security skills. The specific gaps they identified included their ability to access blocked digital content and use digital security features such as two-factor authentication (2FA).
- **Digital safety training:** The majority of respondents (60%) have not received digital security training in the past 24 months.

# At-risk Communities

## Civil society groups

““ What we can do is to be aware [that] the work is risky, then equip ourselves with skills and abilities, by changing behaviour. On the other hand, externally, the perpetrators of the attacks are getting more sophisticated.

ANTON MUHAJIR, SECRETARY GENERAL OF SAFENET

““ There is no secure system, there are always loopholes behind the system, so the safety of a system depends on the user. Our security lies with us, not with the system. But security is inversely proportional to convenience. The safer it is usually the less comfortable it is.

STAFF MEMBER FROM SETARA

Based on SAFEnet’s monitoring results, civil society groups experienced approximately 190 digital attacks throughout 2021 – a 129% increase from the year prior<sup>12</sup> – making them an at-risk community, especially in the context of digital safety.

To effectively analyse the threats facing civil society, ELSAM interviewed representatives from four institutions in Indonesia: Lembaga Bantuan Hukum (LBH) Jakarta, Indonesia’s first legal aid NGO for vulnerable groups; Indonesia Corruption Watch (ICW), a civil society organisation that actively voices criticism on sensitive national issues; SETARA Institute, a research and advocacy group focused on democracy, political freedom, and human rights; and SAFEnet, a network of digital rights defenders in Southeast Asia.

---

12. See: A. Ryan Sanjaya, et al., Indonesia Digital Rights Situation Report 2020: Digital Repression in the Midst of a Pandemic, SAFEnet, April 2020, <https://id.safenet.or.id/wp-content/uploads/2021/04/Report-Situation-Digital-Rights-2021-Daring-02.pdf> accessed on January 20, 2022.

Significant commonalities were found between their experiences or, in the case of SAFEnet, observations of digital attacks.

First, in line with SAFEnet data, the most common attacks reported by organisational representatives were hacking of institutional and staff accounts, Zoom-bombing, doxing, phishing, DDoS attacks, and counter-narratives often involving the negative framing of the organisation's work via traditional and social media, amplified sometimes through the use of influencers.

Second, civil society organisations (CSOs) are significantly more likely to face digital attacks than most other groups and individuals, and also more likely to be targeted by state actors. State-led attacks are difficult to prevent, respond to, or trace due to the inequality of digital security infrastructure between the state and civil society. SAFEnet also indicated that these attacks often coincide with specific demonstrations or periods of activism.

Third, even when an attack is actually or allegedly inflicted by a non-state actor, there is little to no support or acknowledgement for civil society from the government. The Ministry of Communication and Information (*Kemenkominfo*) does not view civil society as a priority group in regard to digital security issues, so no form of policy that protects them exists.

Fourth, CSOs usually concern themselves with the digital safety of the groups and individuals they represent. These groups are often vulnerable or marginalised, such as religious minorities and LGBTIQ+ communities, and more likely to be attacked by non-state actors, particularly when it comes to hate speech and doxing. This demonstrates the importance of CSOs themselves being aware of the importance of digital safety and how to mitigate harm so that they can better assist at-risk minority groups vulnerable to harassment, intimidation, and other digital threats.

Fifth, most CSOs have initiated some kind of digital security effort internally. The majority already have or are in the process of rolling out digital security standard operating procedures (SOPs), with varying degrees of success thus far. As such, an awareness of digital safety clearly exists among CSOs. However, comprehensive implementation of the SOPs is lacking, particularly at the individual level. Staff who are not consistent in

implementing digital security efforts can pose a major threat and increase the vulnerability of the entire organisation. Even the most secure system can be thwarted in this way, highlighting the importance of regular digital security training for staff. Additionally, the majority of institutions do not conduct regular digital security audits, with most either carrying them out only in response to specific threat instances or not at all.

## **Journalists and media houses**

Journalists and media houses form a group that is one of the most at-risk of digital attacks in Indonesia. The Alliance of Independent Journalists (AJI) Indonesia was interviewed to provide insights into the situation faced by journalists and media houses. Like CSOs, they are again more likely than individuals outside of the industry to face digital attacks for their online reporting.

Digital threats from state and non-state actors are considered equally concerning for journalists, meaning that danger is coming from both sides. As AJI put it, digital attacks on the media are a form of “unrelenting violence in Indonesia”.

Since the introduction of Indonesia’s notorious Information and Electronic Transactions Law (ITE Law) in 2008, digital threats to journalists have become more apparent. This law, which should focus on electronic transactions, threatens the freedom of increasingly digital-centric journalists with new, wide-ranging regulations surrounding hate speech, defamation, hoaxes, and misinformation.

One particular doxing case that became the focus of AJI Indonesia at the time was that of a journalist for detik.com, who had written an article about President Jokowi’s plan to open a mall in Bekasi in the middle of the COVID-19 pandemic. In addition to having his personal information shared online by unknown parties, the journalist had someone ordering food for him through a delivery app, an incident that resulted in the driver attacking the journalist



presumably for refusing to accept and pay for the food. The journalist also received death threats via WhatsApp.<sup>13</sup>

Media houses also experience frequent attacks, often in the form of hacking. In August 2020, Tempo's news portal was hacked and defaced. At first, the home page was blank and played the Indonesian patriotic song "Gugur Bunga". Subsequently, the words *Stop Hoaxes, Don't Lie to the Indonesian People* would appear.<sup>14</sup>

Beyond their written work, journalists were found to be at risk for digital attacks as a consequence of advocacy and solidarity efforts.

All in all, the range and prevalence of digital threats to journalists and the media mean that special attention must be paid to the digital security of this group. While the industry in general would have a higher level of understanding of ICT, in practice the digital safety capacity among journalists remains low. This capacity relates not so much to their ability to use this technology, but the ability to use it safely, and the wider habits and behaviours surrounding it – in particular, the inclination not to move away from what is known. As such, the use of safer platforms like Proton, Signal, and Wire remains rare.

## Telecommunications Companies Policy Analysis

The two charts below are generated from data associated with the RDR indicators used in this research. The indicators measure the publicly available policies of the telecommunications companies in relation to freedom of expression and privacy. Please refer to Annex 2 for more information about the RDR indicators and the scoring process, or visit <https://rankingdigitalrights.org/2020-indicators>.

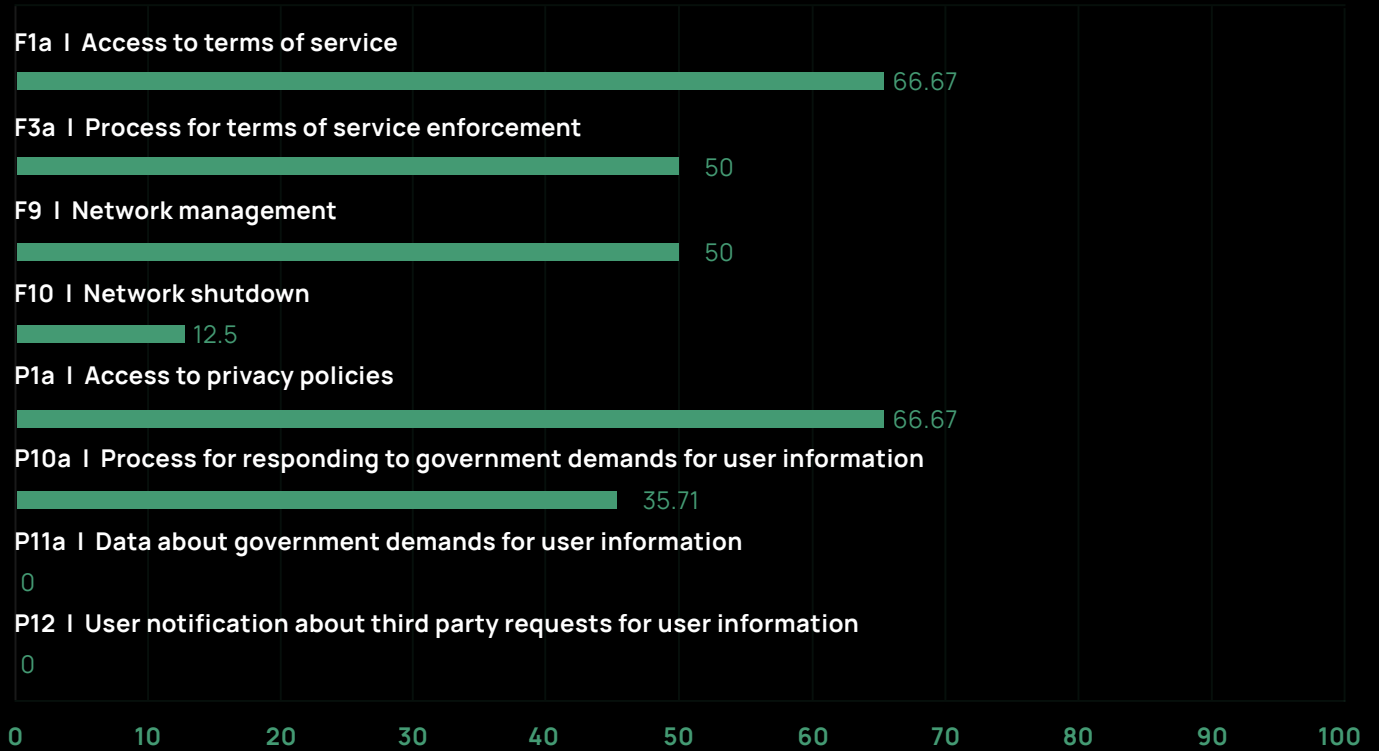
---

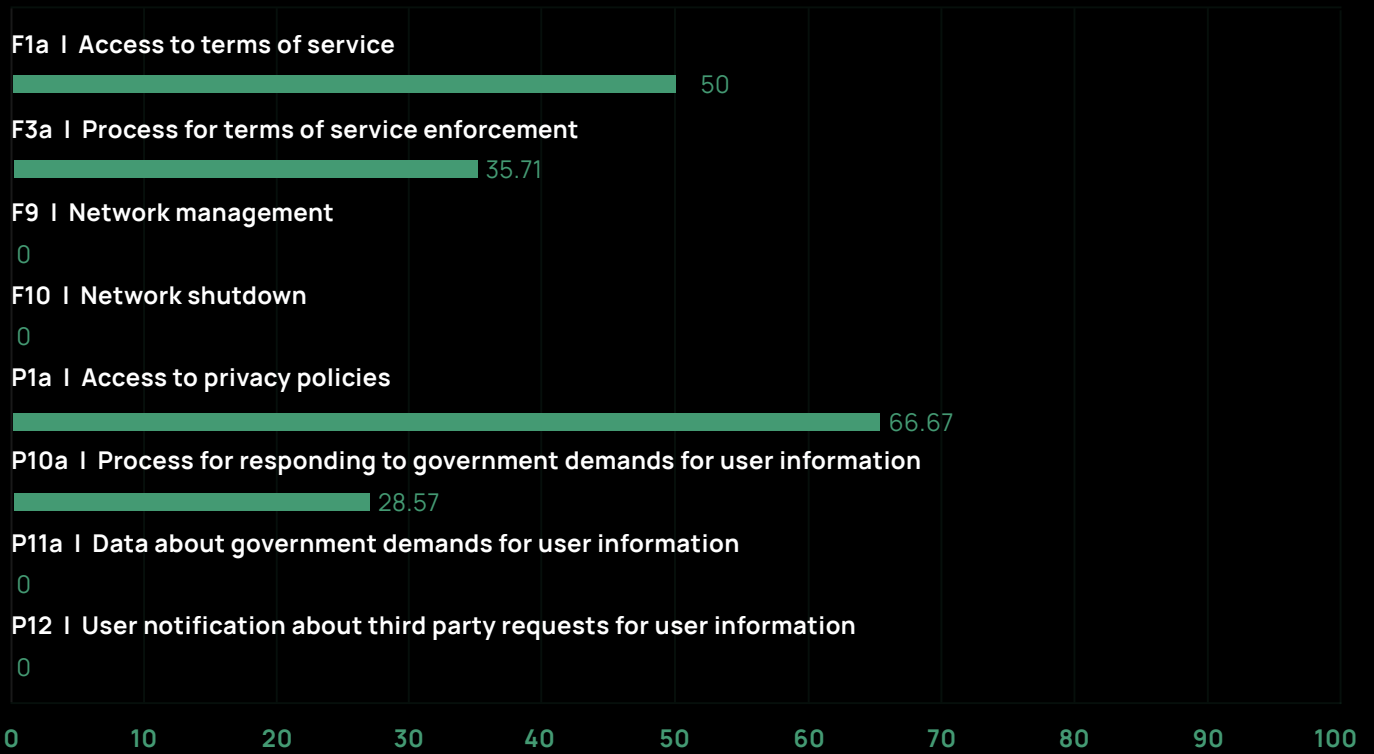
13. AJI Indonesia, "Journalists of Detikcom Experience Doxing, Intimidation, Death Threats", *AJI Indonesia*, 26 May 2021, <https://advocation.aji.or.id/read/data-kerasan/1829.html?y=2020&m=5&ye=2020&me=5> accessed on January 24, 2022.

14. Chronology of the hacking of the Tempo.co site <https://nasional.tempo.co/read/1377884/begini-kronologi-peretas-site-tempo-co> accessed on February 7, 2022

## Telkomsel | Indonesia

■ Mobile





### Key takeaways

- The Terms of Service and privacy policies of both companies are far from easy to read in terms of format and language.
- Both companies clearly describe the forms of prohibited content in their services, but neither fully describes the process taken to identify prohibited content. Neither company clearly outlines a remedy mechanism available to users if the imposition of sanctions for alleged violations causes them harm (e.g. due to mistargeted or misidentified sanctions).
- The mechanism for providing data to third parties, such as government agencies, is stated in both documents but the legal basis or process for data exchange is not clearly stated. Neither company elaborates on whether there is a possibility that it could refuse data requests from authorities.
- Neither company discloses data on complaints or content reporting by the government in their annual reports. However, XL Axiata does disclose the number

of reports handled in a mechanism called 'the whistleblowing system' – although it does not specify the types of reports handled.

## Trends and Concerns for Reviewed Telecommunications Companies in Indonesia

- While linguistic accessibility is already good in both companies reviewed, further details on key issues like the process on identifying prohibited content and government complaints need to be improved further as public interest concerns.
- Connecting the mechanisms for government data sharing with references to legal bases is important, so users can know the laws they can use in case of violations to privacy. Being more upfront on this will help users be fully aware of these companies' policies as they use their services.
- Monitoring and surveillance of online activity, especially by government authorities, is a key concern for Indonesian civil society. Telecommunications companies should keep this in mind when thinking of how to improve their terms and disclosures to its users and the general public.

## Internet Freedom Context

The survey's findings on digital safety capacity in Indonesia exist in a wider context in which internet freedom is in a state of decline. COVID-19 has played a contributing role in this and the acceleration of existing trends in digital authoritarianism. The necessity for increased usage of digital spaces has enabled the government to more effectively silence public criticism, in particular regarding the government's handling of the pandemic.<sup>15</sup>

There are also several laws in Indonesia which specifically enable the shackling of citizens' digital rights. The ITE Law is one of the most well-known, enabling restrictions on criticism in the online realm, surveillance of citizen activities, and content blocking. Such regulations have been increasingly manifesting into real life cases over the last few years.

---

15. <https://rsf.org/en/news/indonesia-used-covid-19-silence-criticism-government>

Last year, for example, *Kemenkominfo* blocked 565,449 pieces of content on the internet, citing the violation of laws and regulations, with minimal additional elaboration.<sup>16</sup> This is because the ITE Law allows for largely unrestricted content blocking by government agencies via Article 40, which is vague in language and does not leave room for complaint or recourse in response to any actions taken.<sup>17</sup>

Monitoring and surveillance of online behaviour, particularly on social media, is also increasing, supported by various regulations and programs issued by the government. There are two agencies in Indonesia that have the relevant online monitoring and surveillance powers: *Kemenkominfo* and the Indonesian National Police (POLRI). Under the relevant laws and regulations, these agencies can make demands on electronic service providers, including the submission of personal user data.

Monitoring and surveillance of online platforms is often justified by the prevention of pornography, hoaxes and/or “hate speech”, the definition of which is unclear in Article 28 of the ITE Law, which bans the practice. A virtual police force was created specifically to monitor such content, unilaterally determine its quality, and decide whether it should be restricted or taken down. Rather than protecting civilians from hate speech attacks, virtual police officers are more likely to target content criticising government policies. As such, it does not have any positive impact on efforts to protect marginalised groups, such as the LGBTIQ+ community and religious minorities, who are genuinely vulnerable to discrimination.

The regulation of disinformation is left similarly broad, with a lack of clear definitions around terms like “fake news” and “trouble”.

At a more fundamental and troubling level, 2020 saw several instances of disruption to internet access, including incidents thought to be government attempts to restrict communication channels in the province of Papua, where there is an ongoing struggle for independence from Indonesia.<sup>18</sup> There is a likelihood that government authorities will use a ‘national security’ argument to throttle or shut down internet access again in the future.

---

16. <https://en.antaranews.com/news/207145/kominfo-pushes-three-strategies-to-handle-negative-online-content>

17. <https://www.eastasiaforum.org/2021/04/02/the-uncertain-future-of-online-free-speech-in-indonesia/>

18. <https://freedomhouse.org/country/indonesia/freedom-net/2021>



# MALDIVES

## SOCIETY FOR PEACE AND DEMOCRACY (SPD)

Being a country with more than 1,190 islands scattered over approximately 90,000 square kilometres, telecommunication is very important. In recent years, the number of people using the internet has skyrocketed.

As more people, including human rights defenders, become dependent on online technologies, digital attacks have increased and are impacting those less familiar with digital safety practices.

### **Digital Safety Capacity Analysis**

The online survey was conducted in English. It was completed by 41 individuals, with 11 identifying as female, 24 identifying as male, 1 as 'intersex', and 5 not responding to the question about gender. 63% indicated they were based in the city (Malé), 31% in the islands and the remainder living in one of the resorts or under the sea. A majority of the respondents indicated that they work in the human rights field, in the media/journalism sector, or were involved in digital rights.

## Online Survey – Key Findings

- **Use of messaging apps:** WhatsApp was ranked the most popular, followed by Viber and Facebook Messenger. Signal use was very low. Only 5% of respondents indicated they had a high level of confidence using instant messaging platforms safely.
- **Digital attacks:** All respondents indicated that they were very concerned about digital attacks including account takeover, malware attacks, device confiscation, online monitoring/surveillance, online impersonation, online harassment, and hate speech. A majority of respondents indicated they do not have capacity to address these attacks. In terms of directly experiencing digital attacks, the majority of respondents indicated they had only been affected by online harassment and hate speech.
- **Threat actors:** State and non-state actors were considered equal threats by respondents.
- **Protecting against digital attacks:** Majority of respondents indicated they do not have the capacity to protect themselves from digital threats.
- **Passwords:** 39% of the respondents are confident about the strength of their passwords to access devices and accounts. 35% of respondents indicated they use two-factor authentication for most or all of their accounts.
- **Use of collaboration and online conference calling platforms:** Respondents indicated that they do not use collaboration or conference calling platforms regularly. However, of the platforms that they do use, Zoom, Google Meet, and Skype are the most commonly used apps. Only 17% of the respondents are confident about collaborating or participating in these calls in a safe and secure way. 37% are not confident about securely participating in online conferences.
- **Digital safety skills:** 63% of respondents indicated they had no or a low level of digital safety skills, while 12% indicated that they had a high level of digital safety skills.
- **Digital safety training:** 95% of respondents had not attended a digital safety training in the 24 months prior to the survey. Most believe there are no special institutions or available courses related to digital safety where they can learn more about digital threats.

Anecdotal evidence suggests that Maldivians also face growing Islamophobic content online. In March 2021, the United Nations Special Rapporteur on freedom of religion, Dr. Ahmed Shaheed, who himself is a Maldivian, noted the rise of Islamophobic incidents in the form of online hate and stigmatization.

(UNHRC, 2021)

## At-risk Communities

### Journalists

Journalists have long been at heightened risk of intimidation and abuse online in Maldives. The more politically charged the environment, the higher the risk becomes. This has been shown to be true in times of religious division, elections, and COVID-19.

One female journalist said she has been targeted and has been receiving harassing messages and threats that can be linked to her journalism. This forced her to work in social isolation from home.

The high levels of social media usage in the Maldives means platforms such as Facebook are often weaponised and used to target journalists and bloggers.

Another key informant, a blogger, expressed his grief after losing two journalist friends – one had disappeared, while the other was murdered following death threats.<sup>19</sup> He further added that there was no government protection even when they reported said threats.

---

19. <https://maldivesindependent.com/crime-2/rilwan-killed-by-maldives-group-linked-to-al-qaeda-presidential-commission-reveals-147705>



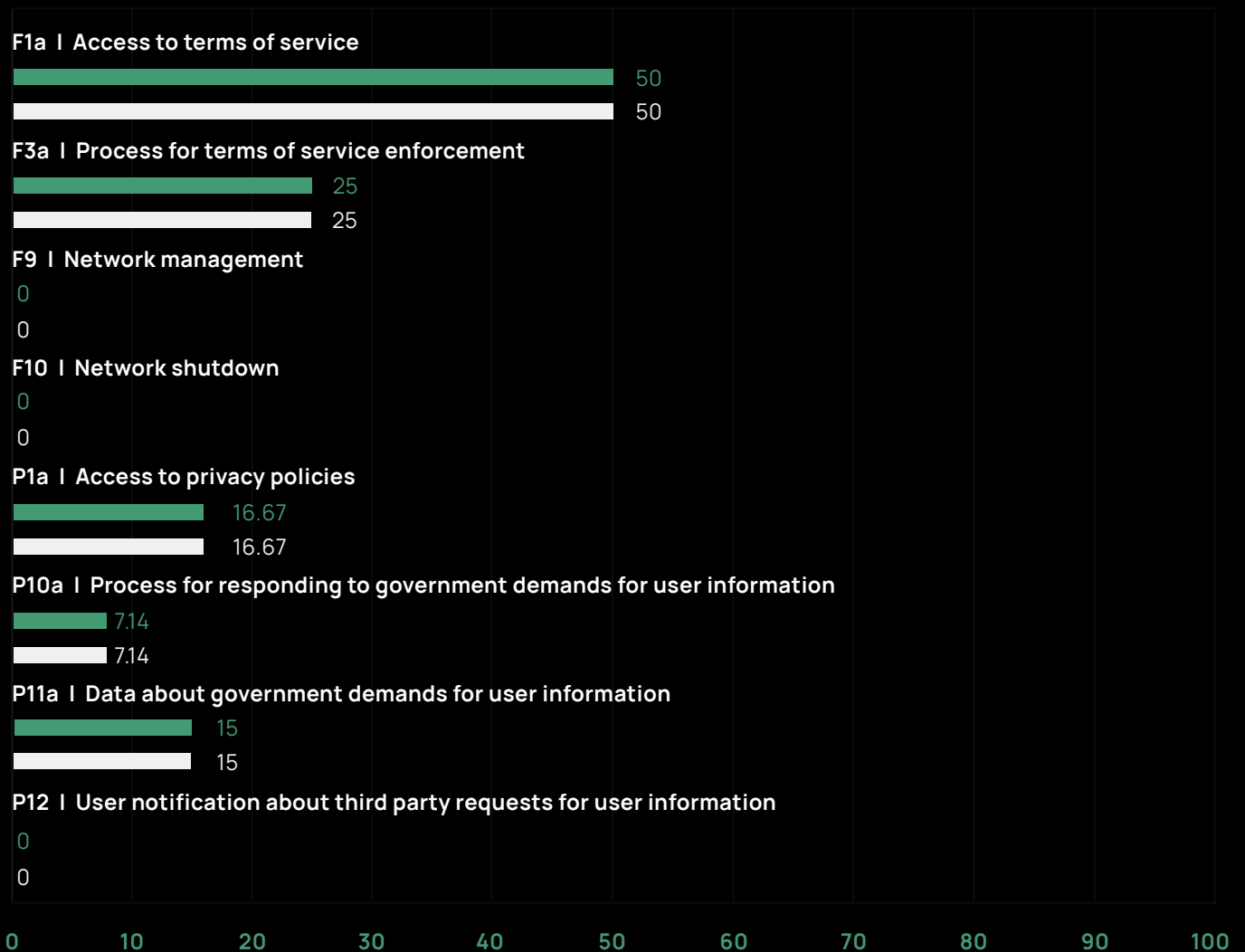
# Telecommunications Companies Policy Analysis

The two charts below are generated from data associated with the RDR indicators used in this research. The indicators measure the publicly available policies of the telecommunications companies in relation to freedom of expression and privacy. Please refer to Annex 2 for more information about the RDR indicators and the scoring process, or visit <https://rankingdigitalrights.org/2020-indicators>.

## Dhiraagu

### Dhiraagu | Maldives

■ Mobile    ■ Fixed-line broadband

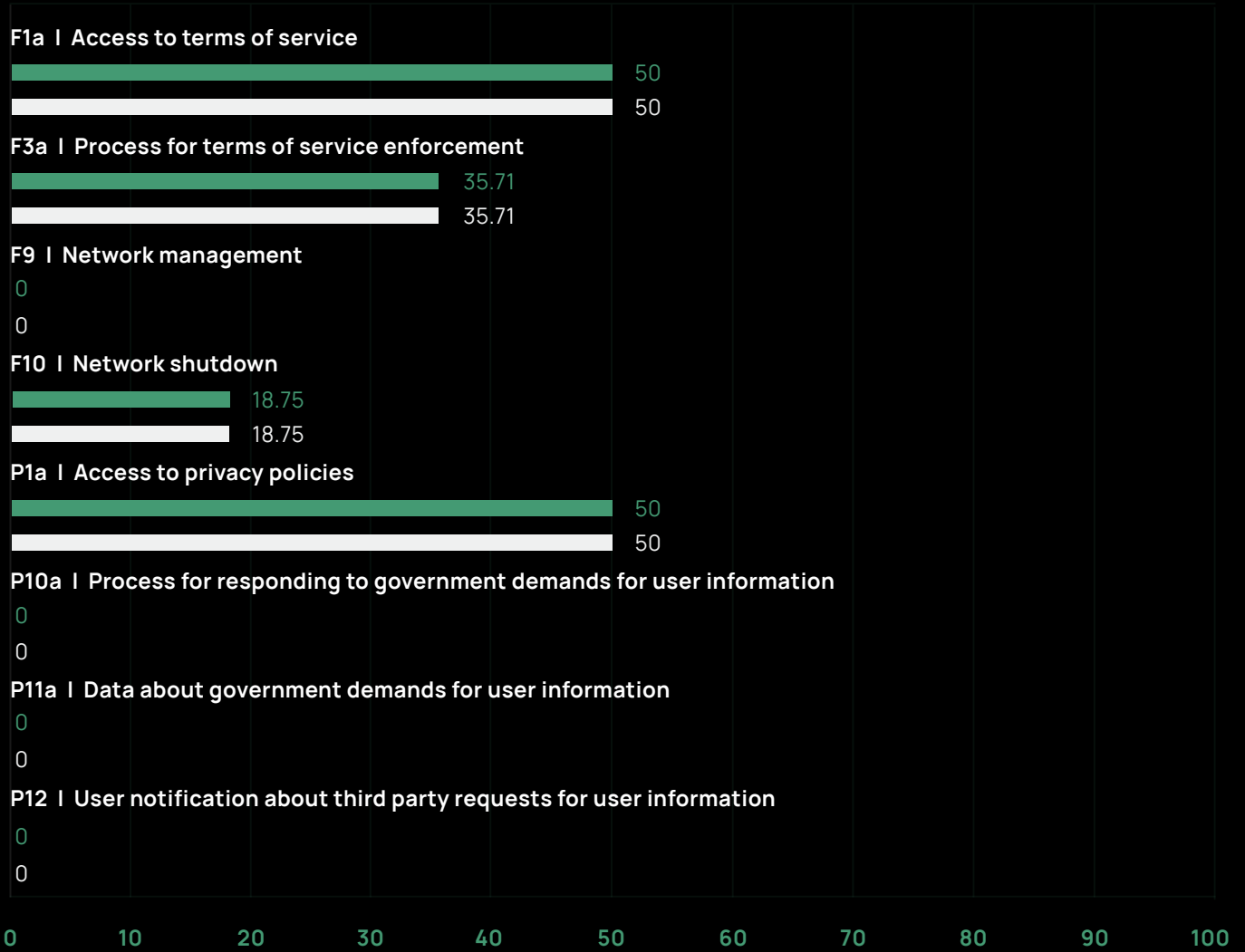


## Key takeaways

- Terms and Conditions are available only in English, which makes it difficult for non-native English speakers – namely Maldivians and the sizable community of Bangladeshi expatriates – to understand the substance of the document.
- Dhiraagu prioritises requests of government authorities, including requests to restrict access to a customer if it is required to do so under any applicable laws or regulations, or as required by necessity of an emergency situation. Dhiraagu can terminate a service with or without notice at any time and without exposing itself to any liability.
- There is no separate Privacy Policy; however, within the Terms and Conditions it states that unless expressly prohibited by law or regulations, Dhiraagu takes the position that customers have authorised them to use or disclose information or data relating to any service number or account. It further states that Dhiraagu may disclose personal information to research organisations for the purpose of surveying users' opinions.

Ooredoo Maldives | Maldives

■ Mobile ■ Fixed-line broadband



Key takeaways

- Similar to Dhiraagu, Ooredoo's Terms and Conditions and Privacy Policy documents are only available in English, preventing Maldivians and the sizable Bangladeshi expatriate community from being able to access them.
- Ooredoo prohibits customers to call, message or send, upload, download, use or re-use any material that is offensive, abusive, indecent, defamatory, obscene, or

menacing, a nuisance or a hoax, in breach of any rights or privacy or otherwise, fraudulently in connection with a criminal offence, or in breach of any law or statutory duty. These terms are broad and vague, and there is no detail on the process of enforcement related to these terms.

- Ooredoo may give 7 to 30 days advance notice to a customer prior to disconnecting their account; however, there is no information on how Ooredoo responds to third-party demands for user information. The Terms and Conditions state that Ooredoo may have sole discretion to terminate an agreement to provide a service to a customer if requested by government authorities. Ooredoo also does not disclose whether it carries out due diligence on such demands before deciding how to respond, or what the process is more broadly.
- The company's Privacy Policy states that, to the extent permitted by law, certain non-public information about customers may be disclosed to comply with a request or order of a governing authority. However, there is no information about obligations to inform the customer about such requests.

### **Trends and Concerns for Reviewed Telecommunications Companies in Maldives**

- Translating their terms and policies to locally used languages should be an urgent priority for the reviewed companies. This will help users and the general public better understand the companies' policies as they use their services, including their rights and privileges as users.
- Privacy and content regulation policies for the reviewed companies need to provide more specific details and scope in their disclosures. If users are not given details about these topics, grievance mechanisms for related user concerns would not have clear pathways for resolution.
- The companies also show, through the terms and disclosures, how they balance peoples' data privacy and their compliance (or openness to comply) with government authorities. A good re-examination of this balance is recommended, considering public interest and people's digital rights.

# Internet Freedom Context

In 2021, the citizens of Maldives did not experience any deliberate or publicly announced restrictions to internet access. However, there were minor incidents of temporary outages and slowing down of services, which were attributed to technical difficulties due to increased internet demands of home schooling and remote work caused by COVID-19. It is unlikely that any politically motivated restrictions to internet access will be made in the near future.

Censorship is also not a primary issue in Maldives compared to other Asian nations. The biggest threat to free speech is hate speech, threatening speech, instigation of violence, and misinformation from third parties – very few of which have been acknowledged, addressed, or prosecuted by government authorities. This may trigger self-censorship by journalists and critical voices. According to Human Rights Watch, online harassment of human rights defenders continued “to have a chilling effect on civil society in 2020”.<sup>20</sup>

In an attempt to address hate-related crimes, in November 2021 the President signed a bill on how public spaces are defined in the law, including online media such as online forums. Clause 124 (a3) states that if someone harms or encourages harm to someone based on ethnicity, country of birth, race, political views, or religion, it is considered an offence.<sup>21</sup> What is not defined or mentioned is what constitutes harm. This non-specificity increases the vulnerability of the victims to attack.

Misinformation has also posed a persistent problem in Maldives. On March 19, 2020, the Maldives Broadcasting Commission conducted an investigation following numerous complaints from the general public on the broadcasting of certain channels, which contained inaccurate and misleading information concerning the COVID-19 situation in the country. The police warned the public against commenting untrue information in the comment sections of online news sites. In December 2020, the Ministry of Foreign Affairs expressed concern over spreading hatred, misleading information, and false allegations regarding bilateral ties with India. It further stated that all parties and political leadership should act responsibly and refrain from spreading false information.

---

20. <https://www.hrw.org/world-report/2021/country-chapters/maldives>

21. <https://presidency.gov.mv/Press/Article/25879>

From a state censorship perspective, discussions regarding the restriction or blocking of irreligious, pornographic sites and/or sexually explicit webpages have been ongoing in informal circles for as long as internet services have been made available in Maldives. However, concerns have never been formally acted upon. The Communications Authority of Maldives (CAM) is reported to maintain an unpublished blacklist of blocked offending websites. Anecdotal evidence suggests that the CAM monitors websites for content breaches proactively; however, it does accept requests to block websites from government ministries and public authorities. In the past, the CAM has blocked six websites disseminating anti-Islamic views. The grounds for blocking such websites can be found in the Religious Unity Act of Maldives, which prohibits “encouraging violence; inciting people to disputes, hatred and resentment; and any talk that aims to degrade a certain sex and gender in violation of Islamic tenets”.<sup>22</sup>

On November 30, 2021, Times of Addu Online News stated that the criminal court of Maldives had given the Maldives police service 21 hours to shut down all internet mediums used to promote religions other than Islam.<sup>23</sup> The order was made under the Religious Unity Act, which prohibits the practice by citizens of any religion other than Islam. However, no sites have been blocked to date. It is uncertain whether there will be any changes in the year ahead.

There remains little to no restrictions surrounding the use of virtual private networks (VPNs) and circumvention technologies, which has increased during the COVID-19 pandemic as organisations installed and used Wide Area Virtual Networks for extending workspaces to homes. People also routinely use circumvention technologies to access region-locked content on web services such as Netflix and YouTube. We do not envisage that any restrictions on such technologies will be made by the government in the next couple of years.

---

22. New Religious unity regulation: English (<https://minivannewsarchive.com/society/new-religious-unity-regulations-english-6877>)

23. <https://timesofaddu.com/2021/11/30/isps-ordered-to-shutdown-content-promoting-religions-other-than-islam-within-72hrs/>

# NEPAL

## DIGITAL RIGHTS NEPAL (DRN)

In Nepal, COVID-19 has further increased the reliance and use of the internet and digital platforms. While certain benefits have been profound, recent data from the Cyber Bureau of Nepal Police show that cybercrimes are increasing daily, with over 3,900 cases recorded in the fiscal year 2020/2021 alone.<sup>24</sup> While it is difficult to get a breakdown of these cases, there are concerns that many of them are related to freedom of expression. Human rights defenders are worried about emerging cyber laws that will curtail online freedoms further.

Nepal, which is categorised as 'partially free' by the Freedom in the World 2021 report,<sup>25</sup> does not have adequate laws to protect freedom of expression online, with a number of individuals arrested during 2020 for criticising members of the government and their policies.<sup>26</sup>

---

24. 3,906 cases of cybercrime registered in fiscal year 2020/21, 22 January 2022, available at <https://theannapurnaexpress.com/news/3-906-cases-of-cybercrime-registered-in-fiscal-year-2020-21-4056>

25. <https://freedomhouse.org/country/nepal/freedom-world/2021>

26. [https://www.apc.org/sites/default/files/Nepal\\_12.05.pdf](https://www.apc.org/sites/default/files/Nepal_12.05.pdf)

# Digital Safety Capacity Analysis

In response to growing digital safety challenges faced by human rights defenders, DRN conducted an online survey and key informant interviews with at-risk communities in the country. The online survey garnered responses from 59 human rights defenders with backgrounds in fields such as law, media, and human rights. 25% of the respondents identified themselves as female, while the remainder identified as male. 89% were from urban areas, and the majority of respondents fell into the 25 to 49 age group. To gain insights into the digital safety of at-risk communities, interviews were conducted with women journalists and representatives of the LGBTIQ+ community.

## Online Survey – Key Findings

- **Use of email platforms:** Gmail is by far the most popular email platform, used by 98% of respondents. 34% of the respondents also indicated they had Outlook accounts.
- **Use of messaging apps:** The most popular instant messaging apps are Facebook Messenger, SMS, WhatsApp and Viber. Signal use was extremely low. Only 7% indicated they were very confident communicating using instant messaging apps safely and securely.
- **Digital attacks:** There was a high level of concern about most forms of digital attacks including account takeovers, malware attacks, online harassment, hate speech, and gender-based violence. Interestingly, concern with 'being doxed' was lower. The top three digital attacks experienced by respondents included malware attacks, hate speech, and online harassment.
- **Threat actors:** Respondents reported a fairly even level of concern over digital attacks from state actors and non-state actors (including online pro-government groups and IT companies, anti-feminist groups, political and religious groups, and hackers) at 48% and 43% respectively.
- **Protecting against digital attacks:** The vast majority of respondents are not in a strong position to protect themselves from digital threats and attacks; however, responses suggested that they had a better capacity to deal with online harassment, gender-based violence and hate speech than the other types of listed attacks.



- **Passwords:** Most respondents have a medium level of confidence regarding their passwords, but more than a third of respondents use a password manager. Two-factor authentication (2FA) is used by 50% of respondents.
- **Online censorship:** Over 40% of respondents have faced censorship and blocks on websites and apps they wished to access. Only 5% of respondents indicated that they have high capabilities to access censored or blocked content.
- **Online surveillance:** Less than 10% of respondents indicated having a high-level of ability to browse anonymously.
- **Use of collaboration and online conference calling platforms:** Zoom, Messenger rooms, Microsoft Teams, and Google Meet are the most commonly used collaboration and online/conference calling platforms in Nepal. Almost 93% of the respondents had never used Jitsi.
- **Digital safety skills:** 7% of respondents reported having high digital safety skills and 47.5% respondents have medium skills. The remaining respondents have low skills or are unable to comment.
- **Digital safety training:** An overwhelming 91% of respondents have not attended any digital safety training programs/workshops in the past 24 months.

As one respondent pointed out:

“ Different messaging apps use different security standards. I cannot simply choose a secured one, because I need to go with the platform where most people in my network are connected.

One respondent said:

“ I am slowly switching to Signal but still a large number of people contact me via Facebook Messenger.

Another commented:

“ “I know it is not safe but I don't know how to be safe.”

The above comments show that respondents are generally concerned about the safety of messaging apps; however, many lack the knowledge required to act on this.

One respondent reported:

“ “I used to do end-to-end encryption for sensitive emails while working on human rights violation case documentation. Now I no longer use email encryption.

The majority of respondents neither use Pretty Good Privacy (PGP) encryption nor know how to use PGP encryption, indicating that encryption involves technical aspects that make it difficult for public use.

## At-risk Communities

### Women journalists

The most common forms of digital attacks found for this at-risk group are online harassment, threats and intimidation, hate speech comments, online impersonation, and bullying – including sexting and online defamation, aimed at both women journalists and their family members.

Instances where sexual violence in the workplace also manifested online in the form of sexting or unwanted messaging were not uncommon, and caused significant psychological harm to women journalists.

Their journalism work also attracted digital attacks. One interviewee said: “Harassment or bullying in cyberspace is mainly faced by women journalists based on what they write and what they stand for. This might not necessarily be as violent as physical bullying, but still it is faced by many women journalists.”

In one incident, a woman was trolled extensively on Twitter and discredited as a journalist for writing about the political situation in Nepal. Male journalists covering the same issue did not face similar backlash.

In another incident, a woman journalist received hateful, demeaning, and demotivating comments online after posting a controversial story related to marriage.

Defaming and assassinating the character of women journalists have become easier now that their personal information is widely available on social media platforms. One strategy carried out by those who want to discourage women journalists from doing their work is to threaten to link their name with politicians in a way that discredits them, attacking their reputation and creating an environment of mistrust among their families.

The digital threat to women journalists from non-state actors, including religious, anti-feminist, and political groups, are greater than those from state actors. However, if women journalists write about government issues, the digital threats from state actors increase.

Women journalists in Nepal do not have the capacity to sufficiently protect themselves in the digital space because they generally lack the technical literacy, digital safety knowledge, and the ability to assess risks. The patriarchal structure of society and newsrooms, combined with a lack of professional unity, means that women do not get the support they need if online harassment and bullying happens. Furthermore, there is a general unwillingness among newsrooms and media houses to consider digital security issues a priority concern for women.

“ Many of us do not know about the privacy settings of social media platforms. We don't have basic knowledge on ICT, online privacy, and data protection.

## **LGBTIQ+ community**

The Nepalese LGBTIQ+ community includes a wide spectrum of people with diverse sexual orientations, gender identity, gender expression, and sex characteristics. The community in general is at heightened risk of digital attack, with the digital space not just reflecting but magnifying existing vulnerabilities, inequalities, and discrimination in the offline world. Transgender and intersex communities face particularly amplified public discrimination and threats online.

A prominent LGBTIQ+ rights activist interviewed for this survey said: “In terms of connecting with the LGBTIQ+ community or finding a partner or sexual relation or revealing gender identities, the digital space is more convenient and feasible than physical space. But, without formal education and technical know-how, these people will not be able to use digital platforms in a safe way, therefore they are at high risk.”

In one example, a gay male was blackmailed by his former partner, using a private photograph that was shared during their relationship, with threats to reveal his gender identity to his family if he did not comply with his demands.

Media interviews of LGBTIQ+ activists are not well received and attract a disproportionate number of negative comments, hateful criticism, and harassment, which can significantly affect the self-esteem and mental health of targeted individuals.

This issue raises questions around the wider social acceptance of the LGBTIQ+ community, with a prominent activist adding: “Nepalese society has been deeply rooted in sexual discrimination and stigmatisation, which is being expressed on social platforms. There

are homophobic and transphobic contents being circulated on both digital and physical platforms. It is just a reflection of Nepalese society.”

The LGBTIQ+ community tends to promote privacy and anonymity over the internet. In Nepal, a certain LGBTIQ+ group encourages its members to create anonymous accounts, revealing only their gender identities to connect safely with other members of the community. Some members have been exposed to blackmailing, as they are unaware of basic privacy settings or knowing how to make their phone numbers private.

It is important to note that the Nepalese LGBTIQ+ community is not homogenous. As one interviewee pointed out: “A person from an urban area may have high ICT capacity. But people who are deprived of education, opportunity, and are mostly from rural areas have low ICT capacity.”

Additionally, while certain members of the community may know about safety related to Facebook, TikTok, email, and website access, they may not know how to protect themselves when using the latest digital platforms. They may also be unaware of password protection practices and the importance of updating mobile applications.

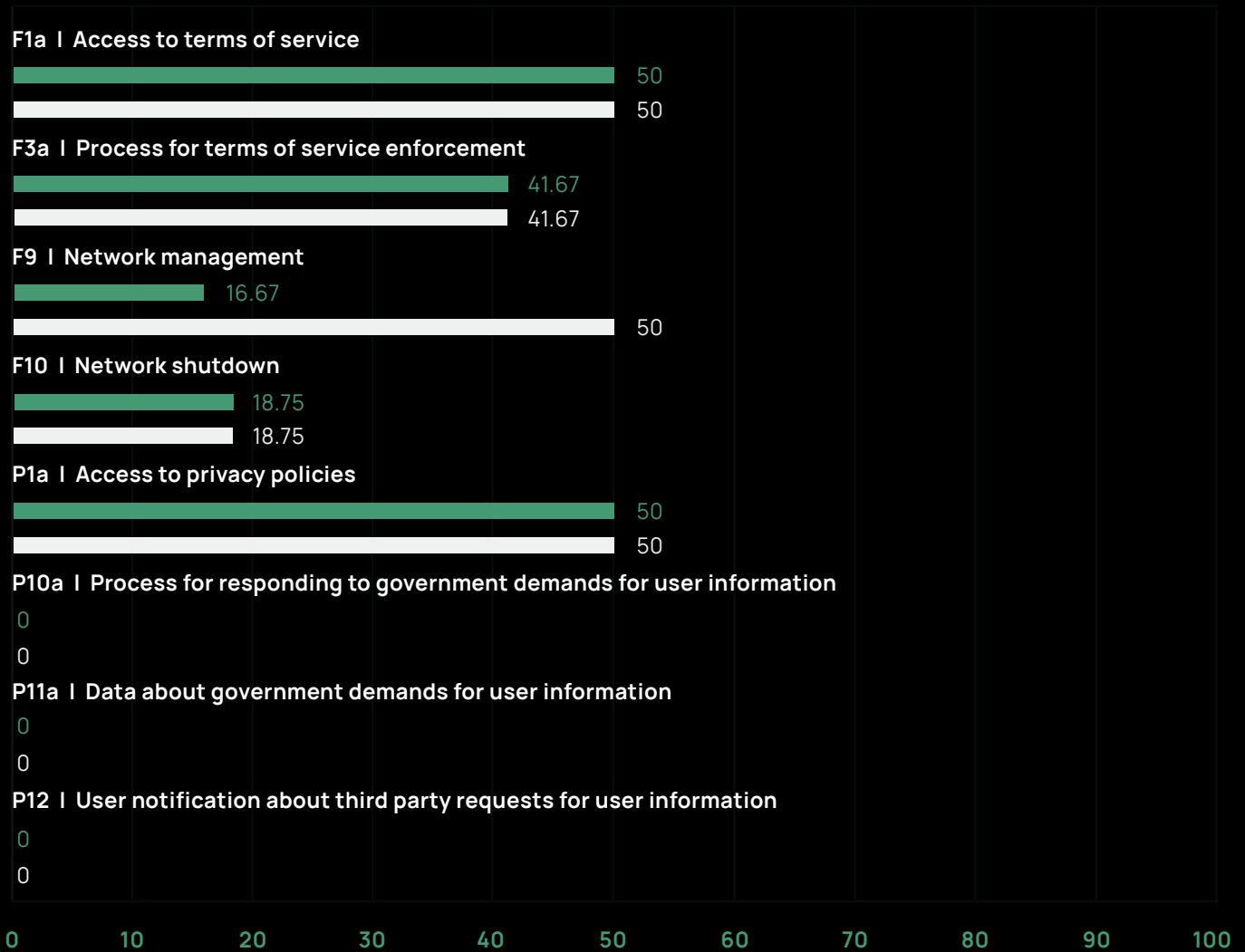
According to the representatives we interviewed, incidents of harassment, bullying, trolling and blackmailing within this community are on the rise, as are breaches of privacy and doxing. Several media houses are also complicit in digital attacks, posting news or content about the LGBTIQ+ community in a derogatory and discriminatory way.

## **Telecommunications Companies Policy Analysis**

The two charts below are generated from data associated with the RDR indicators used in this research. The indicators measure the publicly available policies of the telecommunications companies in relation to freedom of expression and privacy. Please refer to Annex 2 for more information about the RDR indicators and the scoring process, or visit <https://rankingdigitalrights.org/2020-indicators>.

## Nepal Telecom | Nepal

■ Mobile ■ Fixed-line broadband



### Key takeaways

- While the company's Terms of Use and Privacy Policy statements are well-formatted and easily available through the website, these are not available in the local Nepali language. Majority of the population may not be able to access or understand the content of these statements.
- There is no information related to the processes for responding to government

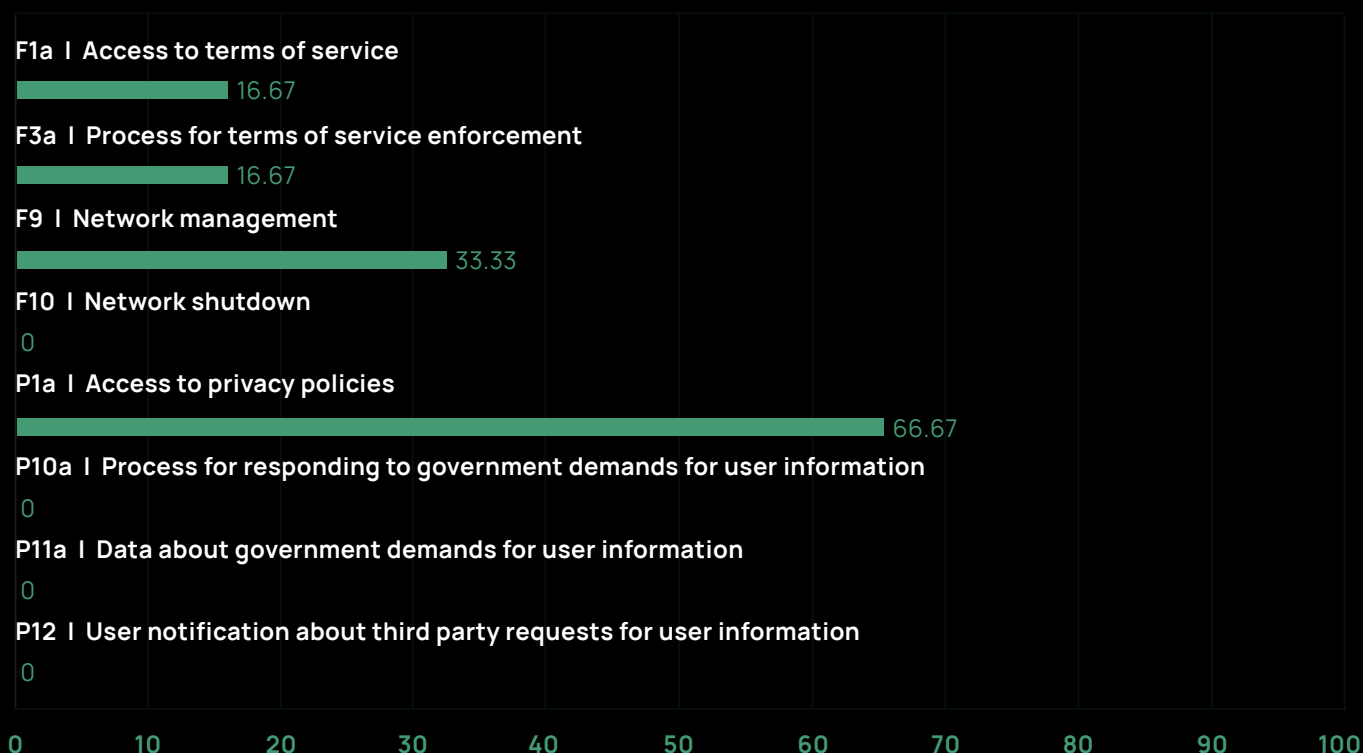
requests for user information, or documenting and notifying subscribers of such requests. Nepal Telecom has not disclosed whether it sends notifications to subscribers when there is a third-party request for their user information.

- The company offers free ('zero-rated') access to certain government websites, including the government's Nagarik app<sup>27</sup> – but does not have a broad zero-rating policy nor explanations about how it decides which sites to offer for free.

## Ncell Axiata

### NCell | Nepal

Mobile



27. <https://nagarikapp.gov.np>

## Key takeaways

- The company's Terms of Service are not available on its website. Although it can be found once the mobile application is installed, it is not available in Nepali language and does not include any definitions for technical terms used. Its Privacy Policy can be easily found through the website; however, it is also not available in the Nepali language.
- The company website does not mention what activities are not permitted using its services. Ncell's mobile application does mention this, so this information can be found if the application is installed.
- Ncell engages in practices that prioritise network traffic. The company made access to two of the government hotlines free, as well as the Nagarik app, which provides access to government services. Ncell has clearly mentioned its purpose to engage in network prioritisation beyond assuring quality of service – to support the government to fight against COVID.
- Regarding the network shutdown issues of telecommunications companies, Ncell has not disclosed any circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network.
- Ncell's website does not disclose information on the process for responding to government demands for user information, nor any published data about such government demands. The company has also not disclosed whether it sends notification to users when a third party requests for user information.

## Trends and Concerns for Reviewed Telecommunications Companies in Nepal

- There is ample room for improvement in ensuring the linguistic accessibility and easy and uncomplicated access to both companies' terms and conditions. A first step to attaining this would be to ensure that all terms and disclosures are available in the local languages.
- As monitoring of users' online activities is a key concern for civil society, improving disclosures about government requests related to user data should be made a key priority as well. This is to ensure that users have the avenue to read these disclosures



and be informed as they use the companies' services.

- Disclosures related to internet shutdowns should be improved as well, especially given concerns about government authorities cutting off services.

## Internet Freedom Context

A newly proposed IT bill in Nepal is causing concerns over internet freedom as specific provisions may restrict or prohibit citizens' use of encryption services and enable the monitoring and potential censorship of online behaviour. The lack of clarity and detailed definitions in the draft bill would enable significant space for the government to encroach on citizens' freedom of expression and the right to privacy.

While censorship does not appear to be as much of a pressing concern in Nepal as in other Asia-Pacific nations, there are legal frameworks in place that would enable censorship if the government so wished. There is evidence that the government is blocking certain games and pornography sites, demonstrating that they have the necessary mechanisms to block political critique. A more recent development has seen the Nepal Telecom Authority (NTA) initiate the introduction of internet filtering technology in Nepal to regulate content. The NTA has allocated a budget of NRs. 1 billion (USD 8 million) to act on this project. If they are to roll out this technology in Nepal, the government would be easily able to further curtail freedom of expression and press freedom.

Among non-state groups, hate speech and disinformation are a dominant concern. Hate speech can lead to self-censorship, and disinformation has been shown to contribute to its propagation. According to a recent poll conducted by the Centre for Media Research Nepal (CMR-Nepal), 95.5% of internet users in Nepal are exposed to false material, primarily through social media sites such as YouTube, Facebook, and Twitter.<sup>28</sup>

Hate speech related to religious groups has particularly inflamed as a result of COVID-19. During the early days of the pandemic, Muslims were blamed for deliberately attempting to spread the virus.<sup>29</sup> This misinformation was aided and abetted by social media


---

28. <https://research.butmedia.org/95-percent-nepali-internet-users-exposed-to-disinformation/>

29. <https://tkpo.st/2XSTsJg>

and some online news portals. Homophobia has also been particularly rife, with various meme pages and social media handles posting homophobic content which has further spread and incited hatred.

On top of all these challenges to internet freedom, internet access itself is at risk because the state-owned Nepal Electricity Authority (NEA) has previously disconnected internet and TV cable wires over financial disputes with Internet service providers (ISPs). The NEA monopoly, combined with the fact that it is state-owned and controlled, means that it can also play a role in future internet shutdowns in the country. A dispute between ISPs and the government on tax and royalty issues can also create uncertainty on uninterrupted access to the internet; mistrust and misunderstanding between these agencies may put people's access to the internet at risk.



# PHILIPPINES

## OUT OF THE BOX MEDIA LITERACY INITIATIVE, INC.

In 2018, the Philippines was tagged as the most dangerous place for activists, with state actors being some of the primary perpetrators of rights violations despite their legal obligation to protect and uphold human rights.<sup>30</sup> This can largely be attributed to the fact that dissent is vilified under the Duterte regime.<sup>31</sup>

Media houses, journalists, and human and environmental rights defenders increasingly fear for their security. Far from being restricted to the offline world, the internet is increasingly a place of anxiety and uncertainty as digital freedom shrinks. COVID-19 has seen the government leverage fake news surrounding the health crisis to crack down on broader dissent. Existing laws such as the Cybercrime Prevention Law and the Anti-Terror Act also hold the potential to threaten the right to freedom of expression and dissent online.

---

30. Global Witness, “Defending the Philippines”, September 2019 (version 2), <https://www.globalwitness.org/en/campaigns/environmental-activists/defending-philippines/> (accessed February 28, 2022)

31. United Nations Human Rights Council, “Situation of human rights in the Philippines: report of the High Commissioner for Human Rights”, A/HRC/44/22 (June 29, 2020), <https://undocs.org/en/A/HRC/44/22>.

# Digital Safety Capacity Analysis

In response to shrinking internet freedom, Out of The Box conducted an online survey and interviews with at-risk communities to better understand specific digital threats facing individuals in this environment, as well as the digital safety practices already being deployed. Survey responses were received from 43 individuals, with a majority of respondents identifying themselves as human rights activists, trainers and educators, and environmental rights defenders.<sup>32</sup> Two-thirds were between 25 and 34 years old, with another one-fifth under 24, providing a largely young professional outlook on the digital safety environment in the Philippines.<sup>33</sup> The gender breakdown was 39.5% male, 32.6% female, and 14% queer/non-binary. A small minority identified as transgender female (2.3%) and lesbian (2.3%), while 9.3% others chose not to answer.

## Online Survey – Key Findings

- **Use of email platforms:** Gmail for daily communications was used by 95% of the respondents. Importantly, 14% also reported using ProtonMail on a daily basis. Many believe that email safety is compromised regardless of the platform. Just one respondent reported being confident about the security and privacy of their email communications.
- **Use of messaging apps:** Facebook Messenger is the most popular communication app, used more than once a day by the majority of the respondents, followed by Signal and Instagram. Respondents noted that, while they are aware that some messaging apps are more secure than others and that they are generally more trusting of independently-owned messaging apps, they often forget to use them and revert back on more popular platforms. This is particularly apparent in the use of

---

32. The majority of the survey respondents are based in the Philippines (95.3%) with a very small minority of them coming from Filipino Americans based in the United States (4.7%). Most of the respondents spend their time working in urban areas (76.7%) with less than half (23.3%) being spread out in semi-urban (11.6%), semi-rural (9.3) and rural (0.4%) locations.

33. 62.8% are between 25 and 34 years old. 20.9% are between 18 and 24. The remaining are broken down as follows: 40-49 (7%), 35-39 (4.7%) and 60+ (4.7%).

Facebook, which is at once the most widely-used platform and, based on comments from respondents, the most distrusted.

- **Digital attacks:** The majority of respondents are very concerned about online monitoring and surveillance, followed by malware attacks and online gender-based violence, hate speech, bullying and harassment, online impersonation, and device confiscation. However, the digital attacks that most respondents have experienced are online hate speech, bullying, and harassment.
- **Threat actors:** The majority of respondents are more concerned about digital attacks by state actors, with approximately one-third of respondents indicating that non-state actors were also of concern.
- **Protecting against digital attacks:** Respondents particularly struggle to protect themselves against doxing, device confiscation, monitoring/surveillance, and online impersonation.
- **Passwords:** 21% of respondents indicated that they are very confident with their password strength. Just over half the respondents are not making use of password management platforms to store passwords.
- **Online surveillance:** Online monitoring/surveillance was found to be the issue of most concern among respondents. This finding is paired with average-to-no capacity to browse the web anonymously among the majority (74.5%). When asked if they believe they were in a location where their browsing and online behaviour is monitored, the majority (60.5%) responded that they were not sure or did not know.
- **Use of collaboration and online conference calling platforms:** Zoom is the most popular platform used by respondents, followed by Google Meet and Jitsi. Almost 40% of respondents indicated that their level of confidence in securely collaborating and joining online conference calls was average.
- **Digital safety skills:** 9% of respondents reported a high capacity in digital safety skills.
- **Digital safety training:** Just under one-third of respondents have attended digital safety training programs or workshops in the last two years.

## At-risk Communities

### **Food security advocates and women activists**

Through the lens of the Maginhawa Community Pantry (MCP) in Quezon City, it is clear that digital threats disproportionately affect both food security advocates and women activists. Particular threats include bullying, gender-based violence, hate speech, account takeover, online impersonation, and doxing.

MCP's founder is at the intersection of both groups, starting the Pantry in 2021 following extended community quarantines that saw many Filipinos lose their livelihoods. While the government allocated aid budget for low-income residents of these areas, the distribution had not been fast enough to ensure food for poor communities. This prompted the MCP founder to action, inspiring a country-wide movement to make up for the inadequacies of government relief via mutual aid.

The MCP founder and the entire movement were soon being linked to communist groups by government officials from the National Task Force to End Local Communist Armed Conflict (NTF-ELCAC), rendering them the targets of threats and harassment both online and offline by the police, military, and non-state actors. Unfortunately, the MCP founder was forced to temporarily suspend the operations of the Maginhawa Community Pantry as a result.



Photo by Kunokuno, CC BY-SA 4.0 <<https://creativecommons.org/licenses/by-sa/4.0/>>, via Wikimedia Commons

The MCP founder shared that she and her entire family were the subject of fake news at the height of the community pantry movement. Red-tagging was the primary form of disinformation she faced.

“ The [perpetrators] would stalk me, grab my pictures, and use those as propaganda against me. They would link me to various people and organisations, and make up stories about me. There was even one news article featuring a person who claimed they knew me as a member of the New People’s Army. This was on YouTube.

She also was the victim of doxing:

“ Someone released my number online, and what non-state actors did was to order a huge volume of food online and had it delivered to me, and which I had to pay for.

The founder of the Kalabasa Project and food security advocate also faced bullying because of her work, including being accused of conducting advocacy for money, fame, and clout.

Gender compounds the frequency and severity of digital threats for women defenders and advocates in the food security and wider human rights space, particularly when it comes to hate speech and online gender-based violence.

Both the MCP founder and the Kalabasa Project founder have used Facebook’s built-in reporting tools in attempts to tackle said threats. However, they found Facebook’s response lacking, with little to no action on such reports once filed.

While ICT/technology skill levels are generally high among advocacy communities, more focus is required towards improving digital safety capacity and media literacy, with many in particular struggling to gauge if a piece of news is real or fake.

“ When I was being red-tagged, some members of the community were doubting me. They really believed what other people were saying about me. But when they got to know me, that’s when they realised who I really am.

THE MCP FOUNDER



Fortunately, there exists strong willingness to practise digital safety, aided by the prevalence of young people in the community who use technology daily and are generally more aware of online threats. As such, there have been efforts to promote digital literacy within the movement already, including holding discussions on how to identify and filter out fake news, particularly around COVID-19 and other health-related information.

## **LGBTIQ+ Human Rights Defenders and Community**

The pervasiveness of transphobia and homophobia in Filipino society is reflected on online platforms, making LGBTIQ+ people more vulnerable to digital threats – in particular online gender-based violence, bullying, and hate speech.

An example provided by a member of the organization Camp Queer centred on online discussions around the 2019 Senate interpellations on the SOGIE Equality Bill – a legislative measure that aims to provide redress for discrimination based on Sexual Orientation, Gender Identity and Expression (SOGIE):

“ There were a lot of comments that claim that when the bill gets passed, LGBT people would face backlash from the church and people who are against the bill. There were even comments and posts urging people to look into the laws of Brunei that criminalise LGBT people and even going so far as to recommend that the [Philippine] government does not pass laws like [the SOGIE bill]. These really impacted the passage of the bill – until now, the bill hasn't been passed yet.

Anti-LGBTIQ+ rhetoric is deployed by both state and non-state actors to demean and sow hate for LGBTIQ+ individuals, as well as political figures who may not identify as LGBTIQ+ but have expressed support for the movement. The Filipino word 'bakla' and the term 'tomboy' are being used as slurs to shame political opponents, even by President Rodrigo Duterte himself.

Apart from SOGIE-based attacks, LGBTIQ+ human rights defenders also face the risk of being tagged as communists and terrorists.

Non-activists in this community tend to have a low capacity to protect themselves against digital threats due to the absence of digital security training in the school curriculum and beyond. Further, the marginalisation of LGBTIQ+ people means they are more likely to be excluded from accessing formal education altogether.

LGBTIQ+ activists, however, tend to have high levels of digital safety capacity as they are more likely to have been exposed to digital security training opportunities. There are several organisations in the Philippines that offer such classes for LGBTIQ+ organisations and activists.

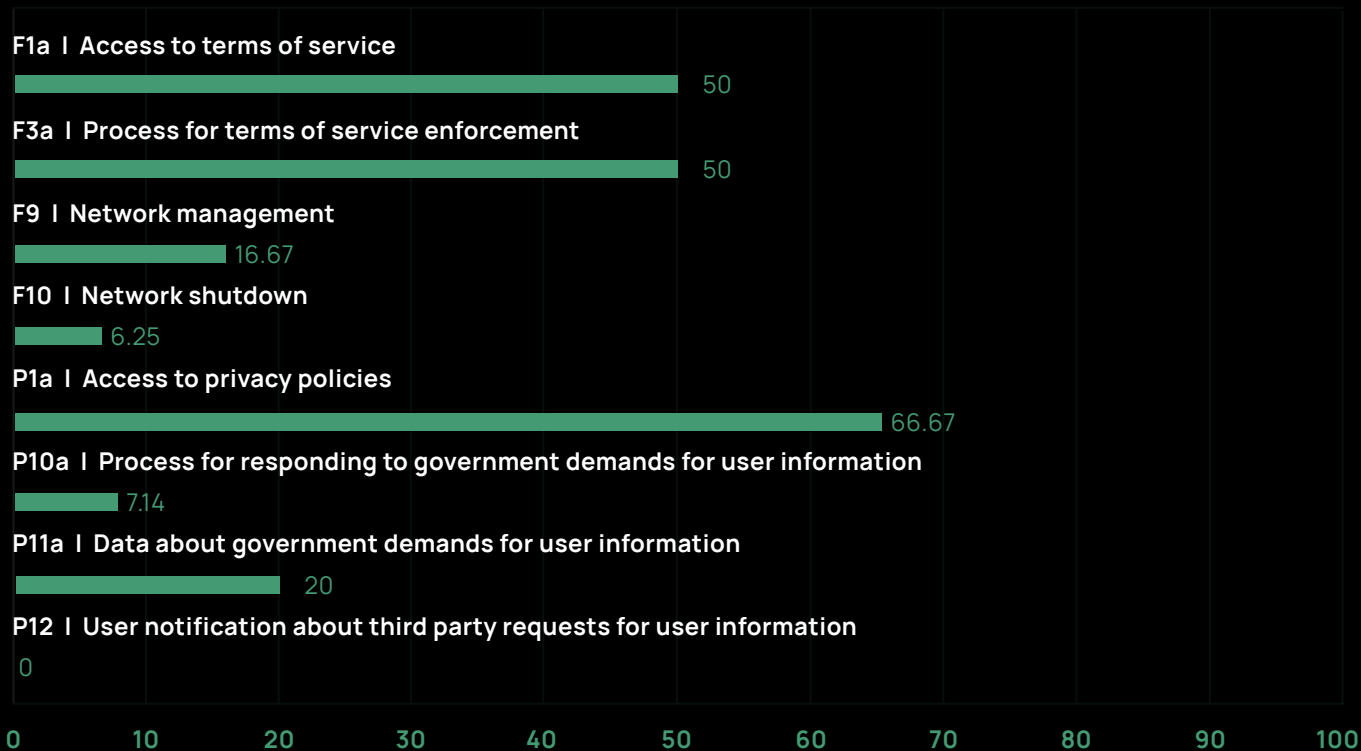
There also appears to be relatively high interest in learning about and improving digital safety capacities among the LGBTIQ+ community. Ensuring equitable access to relevant tools and training will be essential to meet this interest moving forward. This must involve addressing the discrimination faced by LGBTIQ+ people in education.

## **Telecommunications Companies Policy Analysis**

The two charts below are generated from data associated with the RDR indicators used in this research. The indicators measure the publicly available policies of the telecommunications companies in relation to freedom of expression and privacy. Please refer to Annex 2 for more information about the RDR indicators and the scoring process, or visit <https://rankingdigitalrights.org/2020-indicators>.

## PLDT/Smart | Philippines

Mobile



## Key takeaways

- The Terms of Use statement and Privacy Policy are not available in most people's first language: Filipino. Information on how they monitor and flag accounts that violate the company's rules remains undisclosed.
- PLDT/Smart Communications does not specify any policies on net neutrality or when they block or restrict users to particular websites.
- Circumstances that might lead to PLDT/Smart Communications shutting down their network are not clearly outlined.
- PLDT/Smart Communications does not disclose the number of shutdown demands received from legal authorities and government agencies; how they provide user

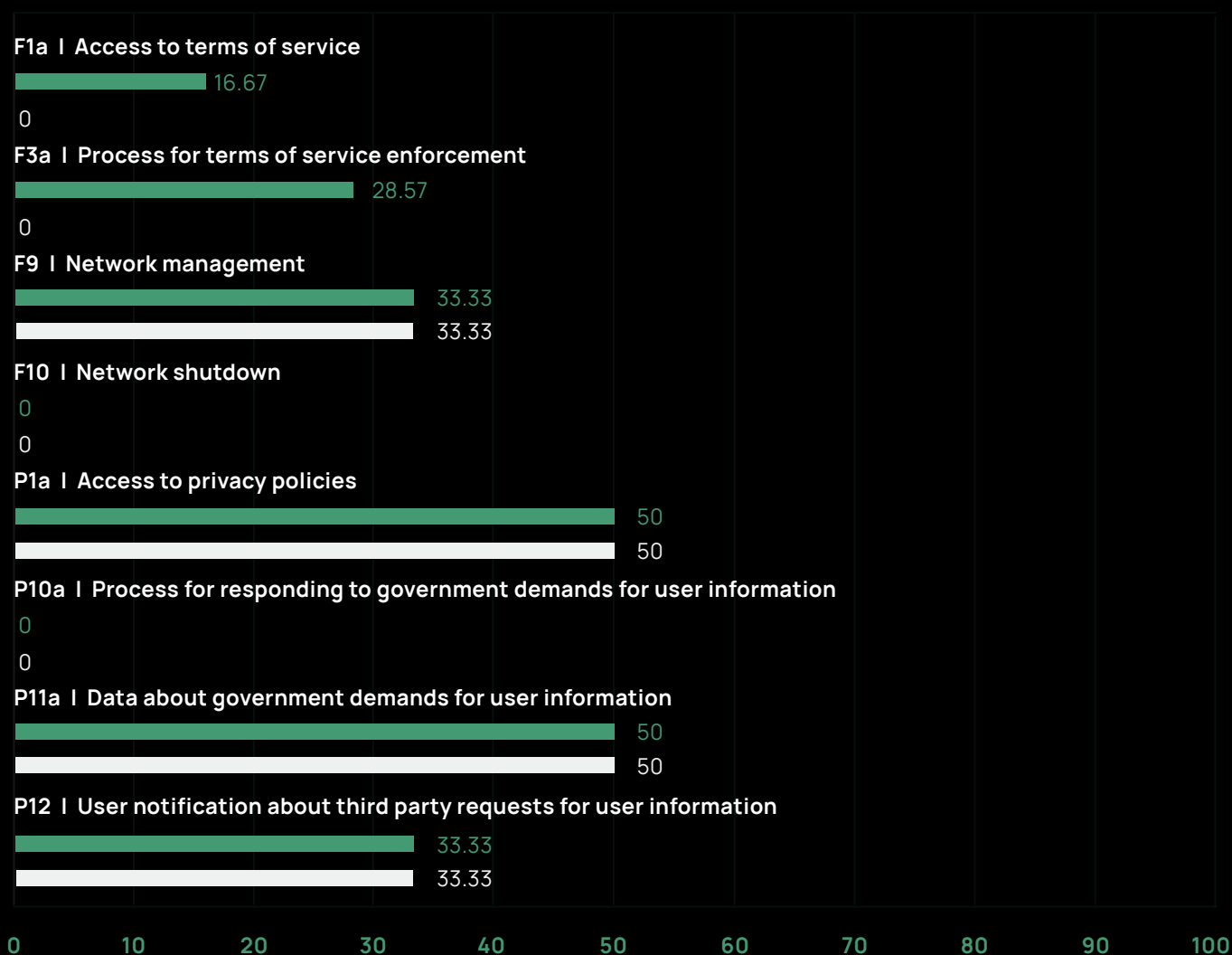
information and other data as requested by court orders, law enforcement or government agencies; and how they decline such demands.

- There are no details on how the company will notify their users if third parties, including government authorities, request their information.

## Globe Telecom

### Globe Telecom | Philippines

■ Mobile ■ Fixed-line broadband



## Key takeaways

- The Terms and Conditions of Globe Telecom for mobile are not easily accessible. The user needs to download the GlobeOne app in order to view them. There are also no Terms and Conditions available for fixed-line broadband on the Globe Telecom official website.
- Globe Telecom does not disclose any information on how they monitor, identify, and flag accounts that violate their rules. The company does not provide any justification as to why they block or delay content for reasons beyond assuring quality network or service.
- There is no information provided in Globe Telecom's reports around which government demands for user information were complied with. While Globe notifies its customers that their user information is being requested, there is no disclosure as to who is requesting such information or why.

## Trends and Concerns for Reviewed Telecommunications Companies in the Philippines

- Making terms of use and other disclosures easily accessible and understandable to its users should be given further priority by both companies reviewed. This can be done by ensuring that these terms and disclosures are easy to find and that these are available in locally used languages other than English.
- Processes and systems about informing users when third parties, like government authorities, request for their information should be specified and made accessible, especially amid concerns about privacy and government surveillance among civil society.
- Content and website-blocking policies should also be specified and developed further, keeping in mind people's right to access information and freedom of expression while also balancing other relevant legal policies and digital rights.

## Internet Freedom Context

From an access perspective, the Philippines suffers from slow, expensive internet, largely thanks to the duopoly of telecommunications service providers Philippine Long Distance Telephone (PLDT) and Globe Telecom. This situation is unaided by strict government regulations inhibiting the entrance of new players. For example, in 2021, the National Telecommunications Commission asked Horizon Gateway Corporation – a small-scale provider of fibre internet services – to shut down its operations because it had failed to obtain a government licence.<sup>34</sup>

Government authorities are also actively involved in restricting freedom of speech via the controversial Anti-Terrorism Act of 2020,<sup>35</sup> which has been left largely intact following a Supreme Court ruling, despite calls from human rights activists that the law is broadly unconstitutional. There are well-founded fears that it could be used to further clamp down on political dissent online.<sup>36</sup>

The government is now using more modern methods like Facebook groups to monitor citizens' activity and compliance. Most notably, Joint Task Force COVID-19 created a Facebook channel with the purported aim of facilitating complaints against netizens who are violating Inter-Agency Task Force (IATF) guidelines on quarantine protocols. It is monitored by the Philippine National Police (PNP) Command Centre personnel and has led directly to arrests.<sup>37</sup> While there is scope for such a group to be useful in the context of a health crisis, it is a form of monitoring and reporting that is broadly problematic due to its reliance on social media – a space often lacking in adequate context.

Tech companies themselves are also frequently involved in the mining of data and tracking of online behaviour, which inspired much anxiety among survey respondents.

---

34. <https://business.inquirer.net/332151/ntc-asked-to-shut-down-internet-provider-accused-of-having-no-license>

35. <https://www.npr.org/2020/07/21/893019057/why-rights-groups-worry-about-the-philippines-new-anti-terrorism-law>

36. <https://thediplomat.com/2021/12/philippine-supreme-court-upholds-majority-of-controversial-anti-terror-law/>

37. <https://www.philstar.com/headlines/2021/03/17/2084988/police-still-monitoring-social-media-quarantine-violations>

The government does not systematically order the removal of online content. There are certainly instances of information being removed in recent years in response to government requests by parties such as telecommunications providers and media houses, but these are often justifiable under important protection laws such as the Anti-Child Pornography Act. That said, there have been some reports of the government forcing public apologies for social media posts critical of its COVID-19 response, leveraging the amended Bayanihan to Heal As One Law, which punishes the spreading of fake and alarming information.<sup>38</sup>

The more common form of content restriction is self-censorship in response to, or in mitigation of, cyber attacks, hate speech, and allegations of disinformation or libel. Such attacks, particularly on media and activists, can intimidate these important information providers and discourage them from future advocacy. For example, media houses Bulatlat, AlterMidya and Karapatan all experienced cyberattacks mid-2021 following reports/statements on the designation of 19 individuals as terrorists by the Anti-Terrorism Council and the arrests of activists and elderly peasant leaders in Northern Mindanao. The Computer Emergency Response Team (CERT-PH) reported that the cyberattacks originated from IP addresses linked to the Philippine Army.

Red-tagging is another common form of harassment whereby targets are accused of having links to local communist groups.<sup>39</sup> In April 2021, community pantries trended all over the country to address gaps in COVID-19 relief. However, the community pantry volunteers and organisations were red-tagged as communists in social media pages handled by local police. The posts have since been deleted and the police have apologised, with the national police even offering to help the Maginhawa Community Pantry founder after she received death and rape threats online.

The general intensification of information disorder in the country post-COVID-19 has seen the government weaponise misinformation to shame, discredit, and intimidate activists, journalists and government critics. There is a widespread sense of mistrust among users of more popular and mainstream tech platforms like Facebook, Twitter, Google, and TikTok.

---

38. <https://www.rappler.com/nation/256256-sanctions-fake-news-bayanihan-act-most-dangerous/>

39. Human Rights Watch, "Philippines: End Deadly 'Red-Tagging' of Activists", January 17, 2022, <https://www.hrw.org/news/2022/01/17/philippines-end-deadly-red-tagging-activists> (accessed March 1, 2022).



# SRI LANKA

## HASHTAG GENERATION

Threats to freedom of expression in Sri Lanka – both online and offline – intensified throughout 2021, resulting in a climate of increasing fear and self-censorship among activists and critics of those in power.

A significant part of this has been the State's crackdown on dissent, frequently under the guise of combating 'fake news' in the COVID-19 era.

Sri Lanka's internet freedom status remains a vital concern. There exists a broad level of awareness of digital safety as an issue of importance, and acknowledgement that more needs to be done, yet there are significant gaps in capacity and practice – both at an individual and organisational level.

On top of this, there is a lack of clarity among telecommunications service providers surrounding shutdown protocols and the sharing of user information with third parties, including government authorities.



# Digital Safety Capacity Analysis

Hashtag Generation deployed an online survey to better understand the capacity and gaps related to digital safety among human rights and environmental defenders in Sri Lanka. We also conducted key informant interviews with representatives of communities particularly vulnerable to digital threats: Muslim women activists and politicians, and transgender people.

The online survey attracted 70 responses in total – 21 from the English-language survey (7 female, 8 male, 6 other), 44 from the Sinhala-language survey (15 male, 23 women, 6 other) and five from the Tamil-language survey. A majority of respondents identified themselves as being human rights defenders and working in the media. The key findings below present combined results, with clear notes on any distinctions or differences occurring.

## Online Survey – Key Findings

- **Use of email platforms:** Gmail dominates when it comes to email platforms, with 95% of respondents across the three language groups having accounts on the email service.
- **Use of messaging apps:** WhatsApp is the most used instant messaging platform, followed by Facebook Messenger and Instagram. SMS is used more than once a day by approximately 30% of respondents. Signal is also used more than once a day by 25% of the English-language survey respondents. In comparison, the use of Signal by Sinhala-language respondents is very low.
- **Digital attacks:** A majority of English-language respondents indicated high levels of concern about account takeovers, malware attacks, online impersonation, online harassment and hate speech. However, those who responded to the local language surveys indicated that hate speech, doxing, and gender-based violence were the most concerning forms of digital attacks. Importantly, the handful of respondents to the Tamil-language survey also indicated a high level of concern about online surveillance.
- **Threat actors:** English-language respondents indicated that state actors were slightly more likely to perpetrate digital attacks than non-state actors. Sinhala-

language respondents identified non-state actors as being slightly more likely to commit digital attacks. Non-state actors that were mentioned in the survey response included pro-government citizens and violent Buddhist and Islamist extremist groups.

- **Passwords:** Approximately 45% of all respondents indicated a high level of confidence in the strength of their passwords. 65% of English-language respondents and 20% of Sinhala-language respondents use two-factor authentication (2FA) for most or all of their accounts. A significant 60% of Sinhala-language respondents indicated they were not sure or did not know if they were using 2FA.
- **Online surveillance:** 30% of English-language respondents indicated a high level of ability to browse the web anonymously (using TOR or a virtual private network for example), compared with just 3% of Sinhala-language respondents.
- **Use of collaboration and online conference calling platforms:** Zoom was the most daily used conference calling platform that averaged across all respondents, followed by WhatsApp and Google Meet. The use of Jitsi – promoted by some digital security trainers as a preferred conference calling platform – was almost completely non-existent.
- **Digital safety skills:** Only 10% of all respondents indicated that they had a high level of digital safety skills.
- **Digital safety training:** 73% of all respondents indicated that they had not attended a digital safety training program during the past 24 months.

## At-risk Communities

### Muslim women activists and politicians

As Muslim women activists and politicians become prominent in the public sphere, many of them also become increasingly vulnerable to digital threats. Online attacks are especially intense when in direct relation to rights-based advocacy. For example, those who supported legal reforms that would see an increase in the minimum age of marriage under the Muslim Marriage and Divorce Act experienced significant levels of online attacks through social media platforms.

Harassment, hate speech, bullying, and online monitoring were identified as key digital threats to this particular community. Derogatory and misogynistic online comments and the altering and sharing of personal images contribute to the cycle of intimidation faced by Muslim women. Their daily physical movements are sometimes tracked and shared on social media, which can lead to offline safety risks. The perpetrators may be established male Muslim politicians, but can also be other more 'conservative' Muslims, politicians from other parties, clerics, or laypeople.

Very few members in this at-risk community have high skill levels in ICT or technology. Many of them are therefore unaware of how to best respond to the digital security threats they face. However, there is willingness to learn about digital safety practices, suggesting scope for future improvement.

“ I think less than 10% of the women have that knowledge. They may not even have basic ICT knowledge, so when they face threats or issues, they don't know what to do or how to complain. Some may even overlook or ignore it.

ANONYMOUS SURVEY RESPONDENT

The Muslim women we spoke with also highlighted the need for better reporting procedures for incidents of hate speech and social media threats. They suggested having civil society representatives in every district of the island who would be responsible for monitoring and reporting digital security attacks on social media that were experienced by people living in that district. This way, quicker and more effective action could be taken against such attacks.

## Transgender People

Transgender people in Sri Lanka face high rates of harassment, hate speech, trolling, and doxing. Perpetrators of such attacks are often those who know them and have 'found out' their gender identity, and wish to expose or 'out' them to others as being transgender. This

can have a significantly detrimental impact on their work and personal life as an individual – including social stigma, and offline violence and harm – as well as on the broader transgender population.

Technology skill levels of transgender people range from low to medium. Many transgender people use smartphones and social media, but their understanding of how to respond to digital attacks is low. Several respondents indicated that the process of reporting attacks on social media platforms appeared complicated and daunting.

According to one interviewee, the willingness and ability of transgender people to practise digital safety is 'debatable', as levels of tech confidence is low. Transgender activists who have attended digital security training workshops will have some knowledge about the topic; however, this has generally not been shared with the wider community.

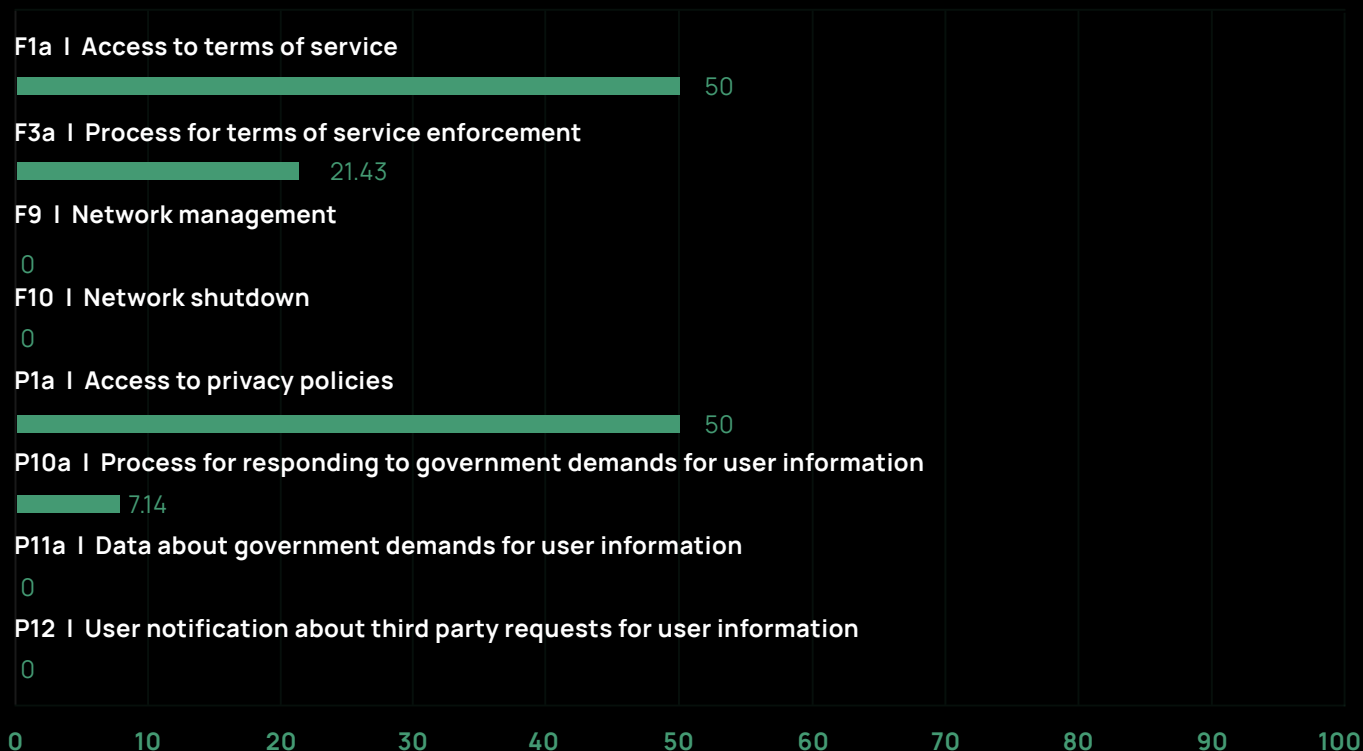
The same interviewee cited that there is awareness of ProtonMail and Signal as more digitally secure platforms, but that these tools are still not always used. Activists may also perceive digital security practices as requirements of 'projects', but not general skills to be acquired and practised regularly. As a starting point, simple awareness sessions on digital safety skills looking at the basics of digital security would be of use.

## **Telecommunications Companies Policy Analysis**

The two charts below are generated from data associated with the RDR indicators used in this research. The indicators measure the publicly available policies of the telecommunications companies in relation to freedom of expression and privacy. Please refer to Annex 2 for more information about the RDR indicators and the scoring process, or visit <https://rankingdigitalrights.org/2020-indicators>.

## Dialog | Sri Lanka

Mobile



### Key takeaways

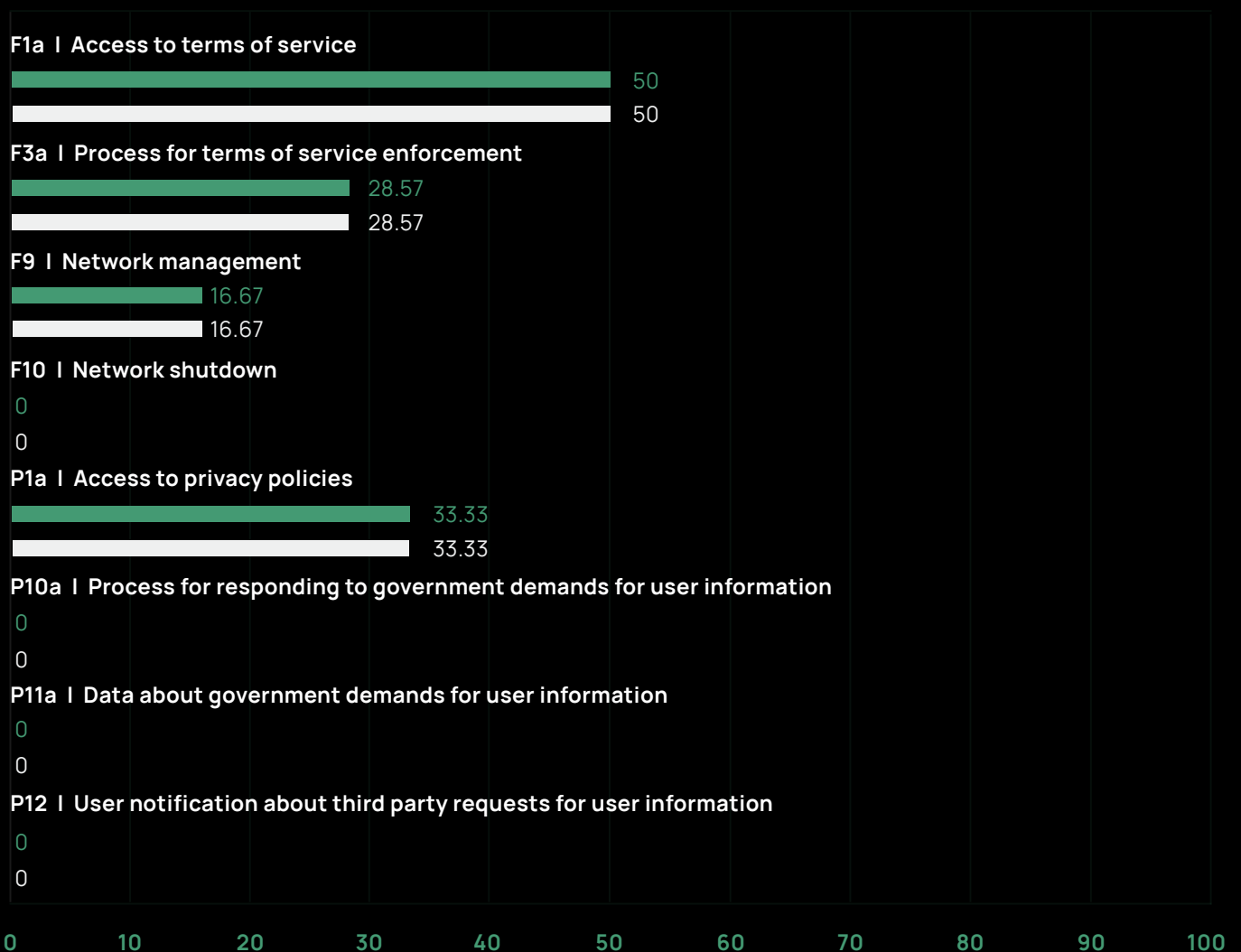
- Dialog discloses Terms of Service and privacy policies only in English and not in local languages of Sinhala and Tamil, excluding a majority of the country's population from understanding the terms and conditions related to using the service.
- Dialog does not clearly disclose the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network; or disclose the number of network shutdown demands it receives; or the number of demands it has complied with.
- Dialog engages in practices, such as offering zero-rating programs, that prioritise network traffic for reasons beyond assuring quality of service and reliability of the network.

- Dialog does not clearly disclose data about government demands for user information. The Privacy Notice states that the company may disclose customers' personal data "to third parties when disclosure is necessary or reasonable to protect our rights, protect your security, investigate fraud or respond to a law enforcement request".

## SLT Mobitel

### SLT Mobitel | Sri Lanka

■ Mobile ■ Fixed-line broadband



## Key takeaways

- SLT Mobitel discloses Terms of Service and privacy policies only in English and not in the local languages of Sinhala and Tamil.
- SLT Mobitel does not clearly disclose, with regard to mobile or fixed line broadband services, the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network.
- SLT Mobitel does not clearly disclose data about government demands for user information, and states publicly that they will “cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity. SLT reserves the right to disclose customer information to such external parties as law demands.”

## Trends and Concerns for Reviewed Telecommunications Companies in Sri Lanka

- Like with companies from other countries reviewed under this research, the Sri Lanka telecommunications companies reviewed here need to put in the work as well in improving linguistic accessibility of their terms and other disclosures.
- Government requests on user data should also be made clear and specific for the users to review. Especially given concerns on monitoring and surveillance, keeping users informed about these policies as they use the services provided by reviewed companies should be made a priority.
- Network shutdowns are also a key concern for Sri Lanka. With this, specific disclosures about this topic should be prioritised as well, so that advocates know how to assert digital inclusion and access based on the companies’ policies and local laws.

## Internet Freedom Context

Over the last two years, Sri Lanka has witnessed the rise of several problematic trends, including militarisation of civilian government functions, reversal of constitutional safeguards, political obstruction of accountability for crimes and human rights violations,

majoritarian and exclusionary rhetoric, surveillance and obstruction of civil society, shrinking democratic space, and new and exacerbated human rights concerns.<sup>40</sup>

Broadly, these developments have seen freedom of expression come under threat. A climate of fear and censorship is festering<sup>41</sup> under enhanced surveillance and intimidation, and has naturally bled into the online world, which has become dominant in daily life since the outbreak of COVID-19.

While internet use is expanding, internet freedoms are not, with increasing constraints observed throughout 2021.<sup>42</sup>

One form this has taken is content restrictions and censorship. Several websites have been blocked or restricted in 2020 and 2021, including news sites critical of the government.<sup>43</sup> In many circumstances, such censorship has directly involved collaboration with the telecommunications industry. For example, July 2021 saw the Telecommunications Regulatory Commission (TRC) ordered by a magistrate to ban all harmful websites. While this order was made in the context of a human trafficking and sexual abuse case and may be seen as a move to 'protect vulnerable communities', there is a need to move away from ad hoc responses and establish a more sophisticated and accountable approach to cyber policies that protects vulnerable communities, while ensuring that critical voices of journalists and human rights defenders are not censored.

Major telecommunications company SLT is also blocking torrent sites, peer-to-peer applications, VPNs, and Telegram on its unlimited data plans. This suggests that the telecommunications companies have the capacity to block or throttle other applications on demand. However, SLT offers a number of packages that offer unlimited YouTube and social networking access. Interestingly, these plans would have assisted subscribers to stream information and videos related to the country's economic crisis.

---

40. "Promotion reconciliation, accountability and human rights in Sri Lanka", Report of the Office of the High Commissioner for Human Rights, 27th January 2021.

41. "Old ghosts in new garb: Sri Lanka's return to fear", Amnesty International, 17th February 2021.

42. "Freedom on the net 2021", Freedom House, 2021.

43. <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>



Another form of censorship is the intimidation and punishment of those engaging in dissent, with a number of individuals, including journalists,<sup>44</sup> arrested in 2020<sup>45</sup> and 2021<sup>46</sup> following social media posts containing government criticism. This also indicates that online spaces are being actively surveilled, and the activities of individuals on platforms such as Facebook closely monitored. Trends indicate that authorities will become progressively less tolerant to government criticism on social media platforms, and monitoring and surveillance will increase in tandem. The weaponisation of laws such as the International Covenant on Civil and Political Rights Act No. 56 of 2007 against those dissenting and from minority communities has also been noted.<sup>47</sup> The major telecommunications companies have also stated in their public policies that they will cooperate with and disclose user information when demanded by government and law enforcement agencies.

Social media analysis carried out by Hashtag Generation during 2021 has also identified significant levels of anti-Muslim and anti-Christian hate and dangerous speech, produced in the majority language of Sinhalese largely by users who identified themselves as 'male' on Facebook. These hate speech trends are driven by a political climate of ethno-nationalism that emerged in the aftermath of the conflict between government forces and the Liberation Tigers of Tamil Eelam in 2009. These trends are continuing under Sri Lanka's current political climate, with certain ethnonationalist actors, including those who are aligned with the state, driving hate and dangerous speech in online spaces.<sup>48</sup>

The outbreak and spread of the COVID-19 pandemic in Sri Lanka intensified anti-Muslim narratives<sup>49</sup> that claimed the minority community were "super spreaders" of the virus.<sup>50</sup>

---

44. <http://www.fmmsrilanka.lk/mfrmd/>

45. <https://www.cipe.org/wp-content/uploads/2020/09/Due-Process-during-COVID-19-in-Sri-Lanka.pdf>

46. <https://www.themorning.lk/criminalising-dissent-free-speech-in-online-spaces/> and <https://monitor.civicus.org/updates/2021/10/05/sri-lanka-authorities-crack-down-protests-stifle-critics-and-accused-torturing-detainees/>

47. <https://srilankabrief.org/wp-content/uploads/2019/09/HRCSL-letter-to-Acting-Inspector-General-of-Police.pdf> and <https://www.amnesty.org/en/documents/asa37/2357/2020/en/>

48. <https://www.amnesty.org/en/wp-content/uploads/2021/10/ASA3748632021ENGLISH.pdf> and <https://blogs.lse.ac.uk/southasia/2021/12/06/reframing-the-debate-the-state-disinformation-in-sri-lanka/>

49. 'Sri Lanka: Compulsory Cremation of COVID-19 Bodies Cannot Continue, say UN Experts', (Office of the High Commissioner for Human Rights, OHCHR 25 January 25 2021) <<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26686&LangID=E>> accessed 17 May 2021.

50. Meenakshi Ganguly, 'Sri Lankan Officials Stoke Covid-19 Communal Hate,' Human Rights Watch, (19 May 2020), <<https://www.hrw.org/news/2020/05/19/sri-lankan-officials-stoke-covid-19-communal-hate>> accessed 17 May 2021.

Prominent Muslim women have also been targeted, especially in relation to their advocacy surrounding marriage and divorce laws.<sup>51</sup>

Hate speech and disinformation – both of which can prompt self-censorship among victims and ignite further discrimination, online and offline – are expected to continue to increase over the next two years in scale and sophistication.

---

51. Groundviews, 'An Uneven Playing Field: Bisliya Bhutto', at: <https://groundviews.org/2018/05/08/an-uneven-playing-field-bisliya-bhutto/>

The image features a dark green background with a fine grid pattern. In the top right corner, there are several overlapping, stylized geometric shapes in white and light green, resembling chevrons or arrows pointing in various directions. In the bottom left corner, there are similar overlapping geometric shapes in white and light green, also pointing in various directions. The main text is centered in the upper half of the page.

# **ANNEX 2:** **RESEARCH FRAMEWORK**

## Context

Digital threats are increasingly impacting the work of individuals and organisations working on human and environmental rights issues, and those who are members of at-risk communities.

Simultaneously, internet freedom is being eroded through policies and legal mechanisms that limit or prohibit secure, safe, and private communications, and through weak corporate policies and practices by telecommunications companies, which often lean towards the wishes of the state.

This project aims to take a deeper look at six countries in the South Asian and Southeast Asian regions, to better understand their digital safety needs and the internet freedom landscape.

## Objective

*To improve the capability of EngageMedia and Partners to address gaps and challenges in relation to 1) the digital safety of human rights defenders and at-risk communities, and 2) internet freedom issues in target countries.*

We have provided the following descriptions of the terms used in the objective:

- *Digital safety*: Digital safety refers to being safe from digital threats and attacks. Examples of these include phishing attempts, communications interceptions, email account hacking, social media monitoring, online harassment, and hate speech.
- *At-risk communities*: These are communities that are known to be vulnerable or are experiencing digital attacks. Examples include female journalists, LGBTIQ+ members, and members of marginalised religious or ethnic groups.
- *Internet freedom*: Internet freedom refers to our rights and freedoms to access the internet and participate freely in the digital world. This includes freedom of expression online, using the internet and digital platforms to organise civil

society activities, conducting advocacy, and communicating injustices to external audiences.

## Research Activities

### Part 1 - Evaluating Digital Safety Capacity

Individuals and organisations defending and promoting human rights and environmental issues have always been vulnerable to attacks because their work is often against the interests of those in positions of power. Defenders are increasingly becoming vulnerable to digital attacks and cyber violence. In this context, digital safety practices are paramount. This research activity will enable EngageMedia and its partners to design programs that improve the digital safety capacity of individuals and at-risk communities.

#### Research Participants:

- Human and environmental rights defenders – including activists, journalists, media producers, policymakers, and lawyers. We are interested in understanding the digital safety gaps and needs of individuals.
- At-risk communities who may or may not be human and environmental rights defenders, but are vulnerable to digital attacks. Members of these communities are often subjected to cyber violence including online hate, harassment, and targeted digital attacks.

#### Research Approach:

An online survey will be used to discover details such as existing vulnerabilities, the nature and sources of digital threats, digital safety capacity and confidence levels, and digital safety tool use. Key informant interviews with at-risk communities will be conducted to find out about threat actors, and the nature of perceived and real threats. Participants will also be asked about their views on how digital safety levels can be improved.

## **Human rights defenders**

Country Partners should deploy the online survey to at least 80 to 100 human and environmental rights defenders. Depending on the country, the exact numbers in each group will differ. It is recommended that the survey deployment is targeted, ensuring that at least 40% are women or gender minorities, and 20% of the overall participants are from non-urban areas. It is further recommended that the survey is localised, or is conducted manually using local languages. Given the research timeframe, Country Partners are not expected to conduct key informant interviews with human rights defenders. Country Partners should consider security implications when sharing the online survey and requesting participants to complete it. Responses to the online survey questions can be submitted anonymously, or using a pseudonym. If there are any security concerns, please discuss with EngageMedia or OPTF.

The online survey can be created using Google Forms or another online survey platform. The questions for the online survey aim to inform the following areas:

- Digital threats and attacks faced by participants, including preparedness levels and sources
- Digital safety practices and issues when accessing the internet and web

## **At-risk communities**

Country Partners should prioritise two to four at-risk communities to include as research participants. Examples of at-risk communities include ethnic minorities and LGBTIQ communities. It is recommended that at least one at-risk group composed of women or gender minorities be included – for example, female journalists.

Key informant interviews with representatives of these communities will be conducted to gain deeper insights into their digital safety. The online survey can also be deployed to at-risk communities if possible, to ensure that respondents will only be from at-risk communities.

If, due to security concerns, it is not possible to directly interview representatives of at-risk communities, then it is recommended that individuals familiar with the situation faced by at-risk communities are consulted.

Guiding questions for at-risk communities include:

- What are the top three digital threats faced by your community?
- What are the sources of each of these threats? Are they coming from state or non-state actors? Can you be specific about the source?
- Why is the at-risk community so vulnerable to digital threats and attacks?
- How would you describe the ICT/technology skill levels of your community? (None, Low, Medium, High, Very High, Not Sure / Don't know). *Researchers should follow up to better understand 'why' the interviewee responded the way they did.*
- How would you describe the willingness of your community to practise digital safety? (None, Low, Medium, High, Very High). *Researchers should follow up to better understand 'why' the interviewee responded the way they did.*
- How would you describe the current level of digital safety capacity by your community? That is, how well can your community use digital safety practices to protect themselves? (Responses can be non-existent, poor, medium, good, strong). *Researchers should follow up to better understand 'why' the interviewee responded the way they did.*
- Can you share one or two examples of threats faced by members of your community and what the outcome was? *The aim of this type of question is to enable researchers to provide narratives of real threats experienced by communities.*

## Part 2 - Mapping the Internet Freedom Landscape

Internet freedom levels are generally determined by external actors including telecommunications companies (TCs) and state agencies.

### Research Approach

There are two areas of research:

1. Investigate policies of TCs that are related to key internet freedom issues
2. Assess internet freedom impacts, including cyber laws that affect internet freedom

A bulk of the research associated with this activity can be desk-based. This includes looking into the policies of TCs and documented incidents of internet freedom impacts.

#### **2.1) Policies of Telecommunications Companies (TCs)**

The country partners will use indicators from [RDR's 2020 Corporate Accountability Index methodology](#) to assess the internet freedom related policies of TCs in their countries. TCs are entities that provide the public with internet access, and can include mobile telecommunications companies, internet service providers, and other providers of connectivity such as free wifi services. The following indicators from RDR measure the TCs' policies, especially in relation to internet freedom issues.



## Indicators

<p><a href="#">F1(a). Access to terms of service</a></p>	<p>The company should offer terms of service that are easy to find and easy to understand.</p> <ol style="list-style-type: none"><li>1. Are the company's terms of service easy to find?</li><li>2. Are the terms of service available in the primary language(s) spoken by users in the company's home jurisdiction?</li><li>3. Are the terms of service presented in an understandable manner?</li></ol>
<p><a href="#">F3(a). Process for terms of service enforcement</a></p>	<p>The company should clearly disclose the circumstances under which it may restrict content or user accounts.</p> <ol style="list-style-type: none"><li>1. Does the company clearly disclose what types of content or activities it does not permit?</li><li>2. Does the company clearly disclose why it may restrict a user's account?</li><li>3. Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?</li><li>4. Does the company clearly disclose how it uses algorithmic systems to flag content that might violate the company's rules?</li><li>5. Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?</li><li>6. Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?</li><li>7. Does the company clearly disclose its process for enforcing its rules once violations are detected?</li></ol>

<p><a href="#">F9. Network management (telecommunications companies)</a></p>	<p>The company should clearly disclose that it does not prioritise, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network.</p> <ol style="list-style-type: none"> <li>1. Does the company clearly disclose a policy commitment to not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?</li> <li>2. Does the company engage in practices, such as offering zero-rating programs, that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network?</li> <li>3. If the company does engage in network prioritization practices for reasons beyond assuring quality of service and reliability of the network, does it clearly disclose its purpose for doing so?</li> </ol>
<p><a href="#">F10. Network shutdown (telecommunications companies)</a></p>	<p>The company should 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.</p> <ol style="list-style-type: none"> <li>1. Does the company clearly disclose the reason(s) why it may shut down service to a particular area or group of users?</li> <li>2. 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?</li> <li>3. Does the company clearly disclose its process for responding to government demands to shut down a network or restrict access to a service?</li> </ol>

	<ol style="list-style-type: none"> <li>4. Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?</li> <li>5. Does the company clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service?</li> <li>6. Does the company clearly disclose the number of network shutdown demands it receives?</li> <li>7. Does the company clearly disclose the specific legal authority that makes the demands?</li> <li>8. Does the company clearly disclose the number of government demands with which it complied?</li> </ol>
<p><a href="#"><u>P1(a). Access to privacy policies</u></a></p>	<p>The company should offer privacy policies that are easy to find and easy to understand.</p> <ol style="list-style-type: none"> <li>1. Are the company's privacy policies easy to find?</li> <li>2. Are the privacy policies available in the primary language(s) spoken by users in the company's home jurisdiction?</li> <li>3. Are the policies presented in an understandable manner?</li> </ol>
<p><a href="#"><u>P10(a). Process for responding to government demands for user information</u></a></p>	<p>The company should clearly disclose its process for responding to government demands for user information.</p> <ol style="list-style-type: none"> <li>1. Does the company clearly disclose its process for responding to non-judicial government demands?</li> <li>2. Does the company clearly disclose its process for responding to court orders?</li> <li>3. Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?</li> </ol>

	<ol style="list-style-type: none"> <li>4. Does the company commit to push back on inappropriate or overbroad government demands?</li> <li>5. Does the company provide clear guidance or examples of implementation of its process for government demands?</li> <li>6. Does the company commit to push back on inappropriate or overbroad government demands?</li> <li>7. Does the company provide clear guidance or examples of implementation of its process for government demands?</li> </ol>
<p><a href="#"><u>P11(a). Data about government demands for user information</u></a></p>	<p>The company should regularly publish data about requests for user information that come through private processes.</p> <ol style="list-style-type: none"> <li>1. Does the company list the number of government demands it receives by country?</li> <li>2. Does the company list the number of government demands it receives for stored user information and for real-time communications access?</li> <li>3. Does the company list the number of accounts affected?</li> <li>4. Does the company list whether a demand sought communications content or non-content or both?</li> <li>5. Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?</li> <li>6. Does the company include government demands that come from court orders?</li> <li>7. Does the company list the number of government demands it complied with, broken down by category of demand?</li> <li>8. Does the company list what types of government demands it is prohibited by law from disclosing?</li> </ol>

	<p>9. Does the company report this data at least once per year?</p> <p>10. Can the data reported by the company be exported as a structured data file?</p>
<p><a href="#">P12. User notification about third-party requests for user information</a></p>	<p>The company should notify users to the extent legally possible when their user information has been demanded by governments and other third parties.</p> <ol style="list-style-type: none"> <li>1. Does the company clearly disclose that it notifies users when government entities (including courts or other judicial bodies) demand their user information?</li> <li>2. Does the company clearly disclose that it notifies users when they receive requests for their user information through private processes?</li> <li>3. Does the company clearly disclose situations when it might not notify users, including a description of the types of government demands it is prohibited by law from disclosing to users?</li> </ol>

## Evaluation and scoring

The evaluation includes an assessment of disclosure for every element of each indicator, based on one of the following possible answers:

- “Yes”/ full disclosure. Company disclosure meets the element requirement.
- “Partial.” Company disclosure has met some but not all aspects of the element, or the disclosure is not comprehensive enough to satisfy the full scope of what the element is asking for.
- “No disclosure found.” Researchers were not able to find information provided by the company on their website that answers the element question.
- “No.” Company disclosure exists, but it specifically does not disclose to users what the element is asking. This is distinct from the option of “no disclosure found,” although both result in no credit.
- “N/A.” Not applicable. This element does not apply to the company or service. Elements marked as N/A will not be counted for or against a company in the scoring process.

### Points

- Yes/full disclosure = 100
- Partial = 50
- No = 0
- No disclosure found = 0

N/A excluded from the score and averages.

## **2.2 ) Internet Freedom Impacts**

The following indicators can be used to evaluate the real impacts on internet freedom. Country partners should use their own knowledge and/or tap local experts to provide internet freedom contexts for their countries.

Accessing the internet and internet services	Restrictions to internet and internet services through throttling or shutdowns
Content restrictions or blocking (censorship)	Websites, videos or other content that has been restricted or blocked
Monitoring and surveillance of online behaviour	Monitoring and surveillance of online behaviour especially on social media, and related laws
Hate and dangerous speech	Prevalence of hate and dangerous speech, especially against human and environmental rights defenders, and policies and laws that aim to counter it