SOCIETY FOR
PEACE&DEMOCRACY

Digital Safety in Maldives

Country: Maldives
Author: Adam Shareef

Executive Summary

The study evaluates digital security in the Maldives and analyses digital safety analysis of risk communities, policies of telecom companies, and internet freedom impacts. For evaluation of digital safety, an online survey was carried out in December 2021. The survey revealed that there is a lack of familiarity with digital protection. There is a lack of understanding of the tools available and the training opportunities. Most of the respondents who use social media are often in online groups, and they can be in vulnerable situations to bullying and hate speech.

To understand the digital threats and digital safety at risk communities, key-informant interviews were conducted with twenty-five individuals in December 2021. Respondents believe they are not mentally strong to fight against those threats and lack of protective laws and lack of support system in the constitution, including no separate online privacy policy law to investigate.

Internet freedom impacts were analysed on accessibility to the internet, content restrictions, use of privacy-enhancing and circumvention technologies, monitoring and surveillance behavior, hate and dangerous speech, disinformation, and net neutrality breaches. As the analysis reveals, during 2021, the residents of Maldives did not have any deliberate restriction to the internet. Although there have been discussions on blocking of irreligious, pornographic, and sexually explicit sites, as of date, it is not known if any formal action has been taken. Lack of a cybercrime legal framework is a key challenge to effectively tackling cyber crimes that have actually increased since the pandemic began, and as more people became dependent on digital means for various services because perpetrators take advantage of the people that are less familiar with digital safety. Other issues include people becoming victims of hate speech and disinformation that have also increased as more people use social media.

Evaluations of the telecom policies reveal that important documents such as terms and conditions and privacy policies are not available in the native Maldivian language. There is also a lack of transparency in disclosing the processes in which the companies restrict content or share information on customers upon demands of government, courts, security agencies, and foreign jurisdictions.

In order to improve digital safety and transparency, there is a need to improve the legal framework, empower people with knowledge and training opportunities for increasing their capacity to protect themselves and their families. Moreover, it is crucial that communities that are at particular risk be given special attention. There is a need to have policies to tackle online bullying and the spread of fake information. There is a need for independent institutions to monitor and help those vulnerable to digital safety issues. The role of such independent institutions can be to make standards and facilitate a safe digital environment. The telecom companies also need to be transparent about their policies, and what information they share about customers, and the issues they deal with based on the demands of third parties, including the government. The telecom companies could publish information in the form of lists or statistics. This can help policymakers such as the parliamentarians, civil society to understand the seriousness of the issues and for the public to take precautions.

Digital Safety Analysis of Defenders (1.1)

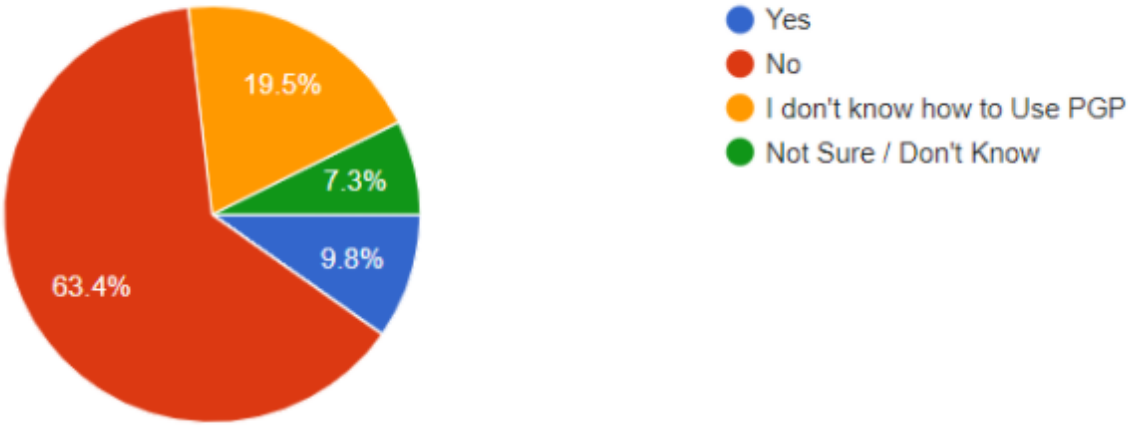
To understand digital safety issues in the Maldives, an online survey was carried out in December 2021. Among the 43 people who responded, 63 % were from the urban areas, and 31.7% came from the outer islands. Among the rest, 2.4% of the respondents were from tourist resort islands.

Being a country with more than 1190 islands scattered over about 90,000 square kilometers, telecommunication has been very important since its inception. The Maldives has one of the world's longest microwave links over the water. A 65 km long microwave link connects a long channel between Huvadhoo and Fuvahmulah in the Southern Maldives (ITU, 2011). In recent years the number of people using the internet has also increased. The Maldives has the highest internet usage in South Asia, with 54.46% of the population having connectivity to the internet (PSM, 2016).

When asked about the multiple devices used to access the internet, 85.3 percent of respondents mentioned using mobile phones. 4.8% of them use laptops, while 7.3% of them use desktops. A further 2.5% of the people use tablets.

When asked about the device they use most on a daily basis, 82.2% responded they use mobile phones, followed by laptops as responded by 9.8% and desktops as noted by 7.3% of the respondents.

The results reveal that there is a lack of familiarity with digital safety. For example, 63.4% of the respondents do not use PGP encryption software when sending sensitive information. Among them, 19.5% do not know how to use it, while only 9.8% mentioned using it.



People were asked if they had given additional thoughts or insights into the security and privacy of email communication. One of them mentioned that there is always a risk. Another respondent noted that one of his social media accounts was hacked, and he has no access to it. He says, "I have no idea how it happened. I don't have access to it anymore". Another mentioned that it is not always secure. However, more than 50% of the respondents mentioned that they do not have an opinion.

With regard to most concerning issues, the respondents identified potential malware attacks, bullying, and harassment. Similarly, based on the actual personal experiences of survey respondents, the most common issues have been bullying, harassment, and hate speech. Other issues in the order of occurrence were: malware attacks, account takeover, and online impersonation. This is followed by being doxed, online gender-based violence, and device confiscation. Online monitoring was noted to be the least occurring issue.

As per the crime statistics for 2020, that was last published by the Maldives Police Service, credit card fraud and hacking are the most common cases of online crimes that have been investigated by the police.

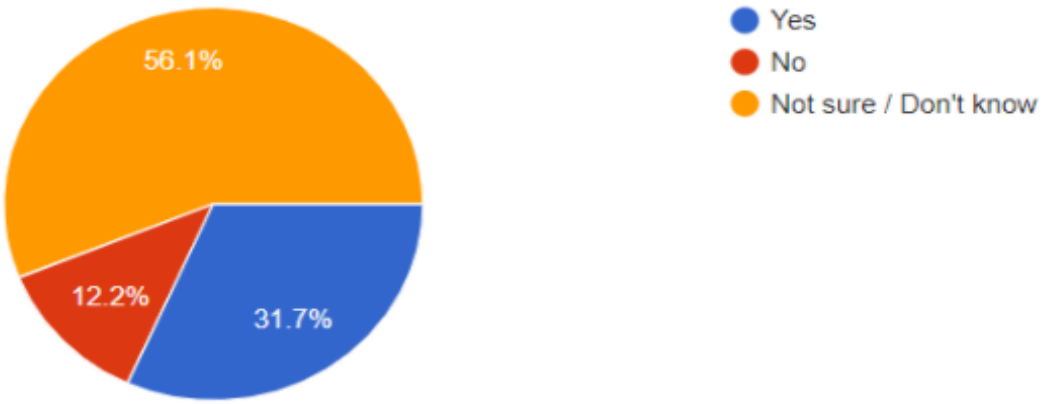
Type of crime	Cases
Credit card fraud	56
Hacking	29
Identity theft	9
Other cyber crimes	8

Source: Maldives Police Service (2020-2021).

Most of the respondents indicate that they do not have the capacity to protect themselves from such threats. Only 12.5% of the respondents indicate that they use software tools and strategies that can potentially improve digital safety. Only 39% of the respondents are confident about the strength of passwords to access devices, laptops, and other vital accounts. Only 34.4% of the respondents indicate they can browse the web anonymously by using Tor or a VPN. Moreover, only 12.2% of respondents indicate they can do encryption for files that they store on hard-drive or cloud, respectively. For example, only 9.8% of the respondents use PGP encryption software when sending sensitive information.

On the sources of digital attacks, respondents are most concerned about actions of non-state actors, including hackers and scammers, those who do online bullying, and those with political motives. However, the views of 37.5 percent of respondents on non-state actors and 41.5% of respondents' views on state actors are not clear as they ranked a midpoint between concern and no concern. This can be an indication of the unfamiliarity with regard to sources and types of digital threats. Those concerned about digital threats from the government comprise 24% of the respondents. A slightly more number of respondents, or 27.5 percent of them, view non-state actors as sources of digital threats. From the survey, however, it is not identified any information on actors from abroad as the respondents did not point anything related to it.

In relation to access to the privacy of the internet and apps, most of the respondents or 56.1% are not sure if they are in a location where the browsing and online behavior is monitored or not. However, 31.7% of the respondents think their online behavior is monitored. Another 12.2 percent of the respondents do not think that their online behavior has been monitored.



On the experience of coming across censorship or restrictions to access sites or apps, 51.2% of the respondents indicate that they have experienced some level of censorship or blocks on websites and apps that they have wanted to excess. 29.3% of the respondents are unsure or do not know if they have faced censorship, while 19.5% indicate they have not encountered such experiences.

There is also a possibility that the reason for not being able to access is not due to blocking by the authorities in the country, but it could happen due to technical matters. For example, there was a concern raised on social media that in Maldives, a social media app called "Clubhouse" was not accessible in December 2021. The Communications Authority of the Maldives (CAM) denied that CAM had blocked it (MNN, 2021). According to Nash Rafeeq, an IT professional from the private sector, it is unclear on the exact nature of the issue faced by Clubhouse users but that it may be likely that there is an outage in edge services or a routing issue, of which the latter is the more likely scenario.

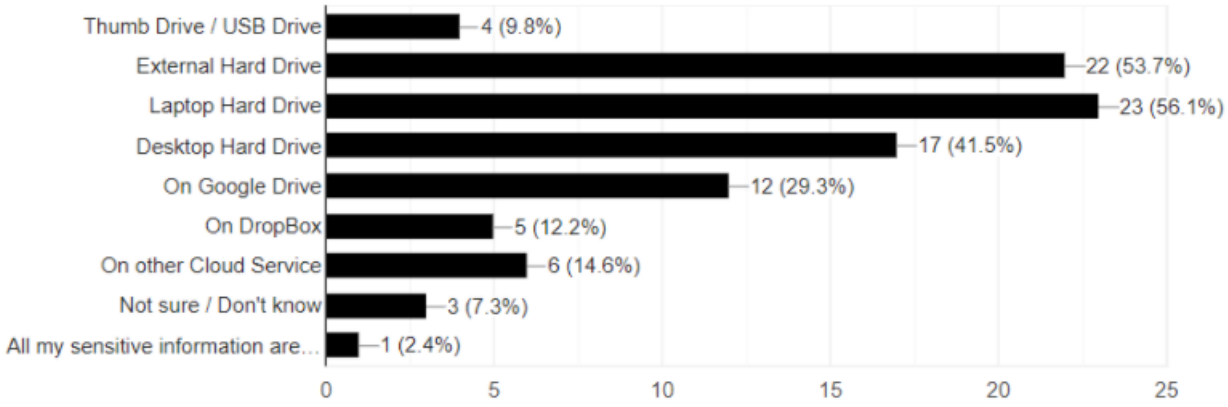
In some other circumstances, restrictions are also experienced due to policies of website operators that restrict or geofence content, or allow content and services based on location. For example, based on the experience of a Maldivian student at a Korean university, Korean Broadcasting Corporation (KBS) YouTube offers some videos that are accessible in the Maldives but not accessible in Korea. On the other hand, there are also contents that are restricted if attempting to view in the Maldives.

When asked about the digital safety capabilities, skills, and practice skill level, only 29.3 percent of the respondents mentioned they have a medium or high level of skills. That means the majority of internet users lack the skills to protect themselves. The survey also reveals a lack of opportunities for training. The vast majority, or 95% of the respondents, indicated that they had not attended a digital safety training/workshop in the past 24 months. The vulnerability of the respondents can be further understood as only 12.5% of the respondents indicated that they make use of software tools and strategies that improve digital safety. Moreover, only 39% of the respondents are confident in the strength of passwords that they use to access their devices, laptops, and other important accounts. Only 34.4% of the respondents indicated they have the capability to browse the web anonymously, for example, using Tor or a VPN. In comparison, only 12.2% of the respondents indicated that they have the capability to encrypt files that are stored on a hard-drive or cloud.

Regarding the daily use of instant messenger apps, most of the respondents use instant messaging / communications apps, with WhatsApp followed by Viber as the most popular apps. The majority or 43.9%, of the respondents, indicated that they belong to groups with an average number of people ranging between 20 and 49 people. This was followed by 31.7% of the respondents belonging to groups with an average number ranging from 5 and 19 people. However, only 24.4%

of the respondents are confident in using an instant messaging platform in a safe way. The majority, or 43.3% of the respondents, ranked 3 out of 1 and 5, representing no confidence or confidence. On the other hand, 31.7% of the respondents indicated they were not confident. Some respondents mentioned that photos were stolen and used in some other websites with wrong information and that there is a need to educate on digital safety matters.

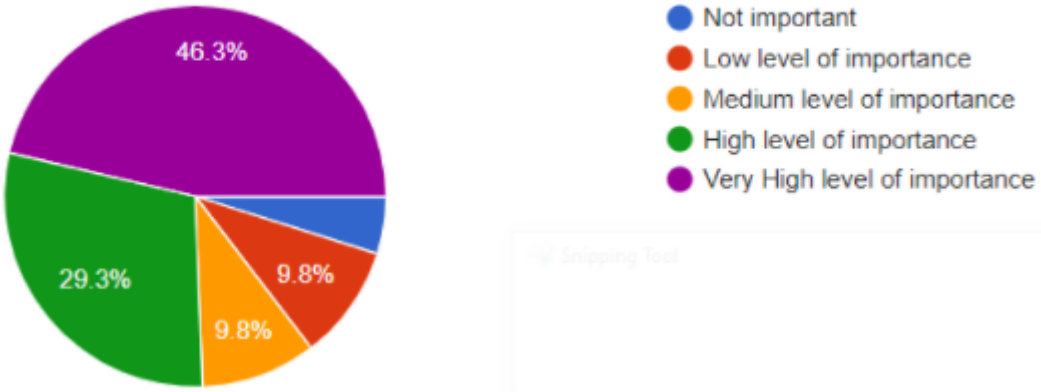
With regard to storing files and data, among the respondents, only 12.2% indicate that their computer (laptop or desktop) storage is encrypted. In comparison, only 22% indicate that mobile device (smartphone) storage is encrypted. 56.1% of the respondents indicated that sensitive information is stored in laptop hard drives, while 53.7% of the respondents store sensitive information in external hard drives. As for online storage facilities, google drive was most popular because 29.3% of the respondents indicated its use.



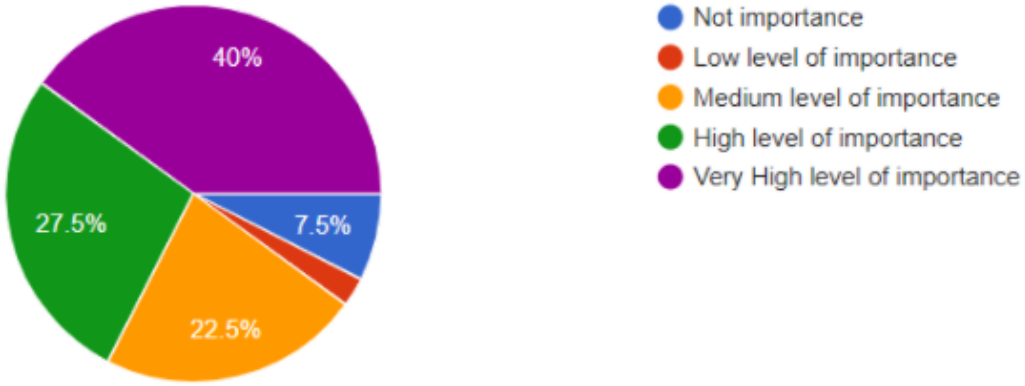
Most of the respondents do not use any software such as PGP Encryption, Veracrypt, Bitlocker, Cryptomat, or other software that can increase the security of files/data. Only 17% of the respondents are confident about storing files securely against access by unwanted parties or through digital attacks. Few respondents gave comments such as keeping a backup on an external drive and that there is a need to protect. One respondent mentions a video on YouTube that belonged to the respondent but cannot be accessed, as it was uploaded on YouTube before YouTube was taken over by Google, and currently, there is no way to use the old login details.

For collaboration and online/conference calling platforms, google meet, zoom, skype, and WhatsApp are the most commonly used apps. However, only 17.1% of the respondents are confident about collaborating or participating in online conference calls in a way that they feel safe and secure. On the other hand, 36.6% are not confident about securely participating in online conferences.

When asked about the importance of communicating anonymously as a measure of safety, except for 4.9 percent of the respondents, all agreed on the importance. On the level of importance, 29.3% indicated it was of high importance, and 46.3% indicated it was of very high importance.



When asked about the importance of implementing encrypted communication for safety and to ensure that the content of messages are not revealed, except for 7.5% of the respondents, the others indicated it was of importance. 27.5% of the respondents indicated it was of high importance, while 40% indicated it is very high importance.



Only 17.1% of the respondents are confident about collaborating or participating in online conference calls in a way that they feel safe and secure, while 36.6% are not confident.

When asked whether the respondents have additional feedback regarding private communication needs, there was only one comment saying that securing is needed. When asked if the respondents have any additional feedback regarding digital security practices, it was mentioned that they are not familiar or understand digital safety tools, and thus more information is needed. It was also mentioned that people need to be aware of privacy and online tools for their protection.

One of the things that is missing in the survey is how the respondents, as Maldivians, have felt in the country or outside the country when accessing the internet. Similarly, from the survey, it is noticeable that the respondents answered from a local point of view. However, the internet and social media is wider than that. Anecdotal evidence suggests that Maldivians also face content due to growing Islamophobia online. In March 2021, the United Nations Special Rapporteur on freedom of religion, Dr. Ahmed Shaheed, who himself is a Maldivian, stated about the rise of Islamophobic incidents in the form of online hate and stigmatization (UNHRC, 2021).
Another gap in the survey is on the digital safety issues related to COVID 19. One of the respondents in the survey was one of the first Maldivians who was suspected of COVID19. According to him, both government authorities and the news media published wrong information. As the identity was revealed, the respondent and respondent's family received hate messages online. Following that, Dr Nazla Rafeeq of the Health Protection Agency requested the public not

to spread misinformation. However, during 2020 and 2021 cases of hate increased. In order to counter this, a training programme was organised for social media influencers from Maldives and Sri Lanka, to sharpen skills to counter online hate (Hamza, 2021).

In the survey, it is found that a large percentage of respondents were indifferent in their answers to some questions. It is possible that many respondents are not familiar with the concepts. This is evident from the answers that most participants do not have the capacity to protect themselves from online threats or do not use technologies that can help to protect. Therefore, there is a need for increasing awareness.

Another part missing in the survey is the opinions of expatriates and their experience in the Maldives. Documentation is lacking on their difficulties in accessing services online or their experience on digital safety.

The survey revealed that there is a lack of familiarity with digital protection. There is a lack of familiarity with the tools available, and the training opportunities. Most of the respondents who use social media are often in online groups and they can be in vulnerable situations to bullying and hate speech. There is a need to have policies to tackle online bullying and spread of fake information. There is a need for independent institutions to monitor and help those who are vulnerable to issues in digital safety. The role of such independent institutions can be to make standards and facilitate a digital safe environment.

References

Hamza, M. (2021) Sri Lanka, Maldives youth to get new skills to counter hate speech in social media, EconomyNext, https://economynext.com/sri-lanka-maldives-youth-to-get-new-skills-to-counter-hate-speech-in-social-media-77789/ Accessed 8 January 2022

ITU (2011) Moving up the development ladder, International Telecommunication Union, https://www.itu.int/net/itunews/issues/2011/06/22.aspx, Accessed 7 January 2022

MNN (2021) CAM: Clubhouse not blocked, facing technical issues, https://www.maldivesnewsnetwork.com/2021/12/16/cam-clubhouse-not-blocked-facing-technical-issues/, Accessed 7 January 2022

Maldives Police Service (2020-2021) Crime Statistics, https://www.police.gov.mv/#casestat, Accessed 10 January 2022

PSM (2016) Maldives has highest internet usage in South Asia, Public Service Media, https://psmnews.mv/en/17048, Accessed 10 January 2022

UNHRC (2021) Islamophobia is a Result of Structural Discrimination Stemming from Negative Stereotypes, United Nations Human Rights Council Geneva, https://www.ungeneva.org/en/news-media/meeting-summary/2021/03/morning-special-rapporteur-freedom-religion-or-belief-human, Accessed 8 January 2022

Part 1.2 - Evaluating Digital Safety Capacity

For the purpose of understanding the digital threats and digital safety at risk communities, key informant interviews were conducted with twenty-five individuals in December 2021. This includes female / Male journalists, politicians, bloggers, actors/ actress and civil society representatives. The importance of conducting this interview is to gain deeper insights into their digital safety, as members of these communities are often subject to cyber violence including online hate, harassment, and targeted digital attacks.

Findings revealed, the top ranked threat by fifteen key informants responded that people are using social media under a fake ID and pretending to be someone and harassing them. However, there are other threats like harassment, Death threats, cyber bullying, black mailing, misleading to wrong information, circulating personal chat logs and betraying and other forms of threats are documented from the interview.

Three informants responded that there were unethical behavior images, inappropriate messages, videos and pictures of them that has gone viral in the social media, due to hacking of their social media accounts. They believe it happened due to lack of secure digital knowledge and carelessness.

Key informants believe primary sources of these threats are coming from non-state actors and made by anonymous. They also consider people who might know them and jealous of their profession are also part of these threats. Few informants highlighted there are threats coming from state actors and are coming from different state institutions.

Several reasons have been identified by the key informants of their vulnerability to digital threats. Respondents believe they are not mentally strong to fight against those threats and lack of protective laws and lack of support system in the constitution, including no separate online privacy policy law to investigate were addressed during the interview. Some of them are also concerned that if they talk about the threats there might be other consequences.

Lack of protective laws and lack of support system in the constitution, including No separate Online privacy Policy

It is also highlighted that most of the interviewees need legal advice and knowledge on certain laws that can be related to privacy online issues and they need civil societies to conduct workshops on digital safety and online well-being workshops and seminars.

Around Sixty percent (60%) of key informants responded that lack of knowledge and skills on information technology in the community is a concern. However, some respondents believe that the community has general knowledge on some software components, but lack in security tools and security features. Many key informants recognized it is important to work with digital safety and practice internet safety for better protection. They believe necessary training will empower them to meet their needs.

Most of them believe that there are no special institutions or available courses related to digital safety and to learn more about digital threats. Fifteen key informants respond there is an urgent need for digital capacity building and skill developing in the community to meet the demands of the digital world and need to understand the defense mechanism for many types of security threats such as cyber-attacks and stealing data. Interviewees included that the community doesn't

understand much about digital safety and people are not aware of how-to use of security tools and its features.

There is an urgent need for digital capacity building and skill developing in the community to meet the demands of the digital world

Creating fake ID's and pretending to be someone, sharing unappropriated pictures and blackmailing, bullying and death threats, physically and physiologically harming are common threats experienced by the key informants and their friends. Among all black mailings have been reported by several key informants as the highest threat faced by their community.

One Female journalist believes that writers are under threat. She said she has been targeted and received a number of threats after she published an article online. With pressure, harassment and harm, she moved her media station to somewhere safer and worked from home and social isolation. Because of fear, most of her staff who worked there stayed at home and later they resigned.

Journalist believe that writers are under threat

Another key informant, a blogger expressed his grief after losing his two journalist friends who was murdered and enforced disappearances after received numerous death threats. He further added that there was no protection from the government institutions even when they reported about their threats.

The government of Maldives should consider ways to support media sustainability through capacity-building and training activities and to conduct more programs / training related to cybersecurity and online privacy issues for protection and internet security.

For the mental wellbeing of risk community at risk from digital threats, access to mental health programs and mental health services are essential to protect their human rights and dignity.

It is also important for providing an outreach mechanism for increased access to self-expression for the risk community. The long-term sustainability of community media must be encouraged through supportive policies and strategies, including legal recognition.

People need to be educated on being wary of interacting with anonymous sources, as such sources can be abusive, such as chat logs, photos and videos to blackmail cyber users.

The urgency of the situation needs the engagement at the political level, on the safety of the journalist and media actors. Effective measures should be put in place to end attacks on journalists and others protecting the right to life, freedom of expression and associated rights. All the crimes against journalists must be properly and effectively investigated and be to bring those responsible to justice.

RDR Research- Telecoms Company policies (2.1)

DHIRAAGU

Dhivehi Raajjeyge Gulhun Public Limited (Dhiraagu) was established in 1988 as the sole telecommunication service provider in the Maldives. The two substantial shareholders of Dhiraagu are, BTC Islands Limited (Batelco) holding 52% of the shares, and the Government of the Maldives holding 41.8% of the shares. The remaining 6.2% of shares are held by the general public of the Maldives. Currently it is one of the two companies that have the license to provide telecommunication, and one of the three companies that have the license to provide internet.

KEY TAKEAWAYS:

Access to Terms of Service and Privacy Policy

Currently, the terms and conditions of Dhiraagu's service are provided only in English. This means it may not be easy to understand for those who do not speak English. The content is not available in Maldivian language. There is also a sizable Bangladeshi expatriate community in the Maldives and tourists visiting from many countries.

There is no specific document on the privacy policy on mobile service or broadband. However, there is a small section on privacy in the terms and conditions for smartphone devices and plans. In the general terms and conditions, there is no separate section on privacy policy, except what is related to disclosure of information.

Process of service enforcement

Dhiraagu prohibits customers actions that are defamatory, annoying, threatening, abusive, offensive, obscene, menacing or illegal, fraudulently or in connection with any criminal activity, and actions that may lead to anxiety, inconvenience, or infringes the rights of other persons, and what is prohibited by law or regulations, and international conventions.

According to the terms and conditions, Dhiraagu will give an opportunity to rectify the situation prior to termination of an agreement between the customer and Dhiraagu. However the actual processes on how the decisions are made are not disclosed.

In the published Annual Report 2020, it mentions that Dhiraagu renewed the membership with the GSMA Mobile Alliance Against Child Sexual Abuse Content to block child sexual abuse content on Dhiraagu's network. However no information is disclosed on the way it is monitored and implemented.

Network management and shutdown

Dhiraagu currently prioritizes the requests of the government authorities. However, there may be situations in which a customer is suspected while being innocent. Currently there is no disclosure on the procedures taken to not block, or delay certain types of traffic, applications, protocols, or content, or the network.

On network management, there is no information if Dhiraagu engages in practices, such as offering zero-rating programs, that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network.

Dhiraagu discloses that the company is required to restrict access to a customer if it is required to do so under any applicable laws or regulations, or under any other regulatory requirements, or upon request by government or regulatory or security or other competent authorities, or is required by necessity of an emergency situation.

However, there could be situations in which a customer is suspected while being innocent. Currently there is no disclosure on the procedures taken to push back on government demands to shut down a network or restrict access to a service. Dhiraagu also does not disclose information, such as the type and amount demanded by legal authorities and the extent to which Dhiraagu has complied with the requests of the government.

There is an indication that customers will be informed to rectify a situation prior to termination. However, as per the terms and conditions, Dhiraagu may terminate the service, with or without notice and without exposing itself to any liability at any time. Therefore there is no certainty that the customer will be informed or not.

Process for responding on user information

In the terms and conditions, it is mentioned that the basis for responding to government demand, is the law of the Maldives. However, the Telecommunication Act 2015, does not adequately address issues related rights of the customer, and user information. Currently there is no cyber law in the Maldives.

Currently there is no information disclosed by Dhiraagu on how it responds to demands by government, non judicial, court orders or foreign jurisdictions, for user information.

Dhiraagu also does not disclose that it carries out due diligence on such demands before deciding how to respond. There is also no information whether Dhiraagu can take decisions at its sole discretion in responding to demands by authorities.

This is relevant because there can be inappropriate or overbroad government demands as well. Dhiraagu does not provide clear guidance or example of implementation of its process for government demands.

Currently there are no lists or statistics on how it has responded to demands for user information.

Data about government demands and user information

Dhiraagu does not disclose any list or statistics on the number of requests it receives. Therefore it is unknown on the demands that come from the government, court orders, law enforcement and national security.

There is also no information that explains what types of government demands it is prohibited by law from disclosing. Dhiraagu has not published any such data. The annual report is generally on the corporate development and economic performance of the company, and thus has no relevant information on government demands on user information.

User information about third party requests

According to the terms and conditions it is stated that, unless expressly prohibited by law or regulations, Dhiraagu regards that customers authorize them to use or disclose information or data relating to any service number, any account, or any other information and data from customers. It

is also mentioned that Dhiraagu may also disclose personal information to research organizations for the purpose of surveying our customers' opinions. If customers do not wish Dhiraagu to use the data for these purposes customers are required to notify Dhiraagu in writing. This indicates that all the responsibility is on the customer and not on Dhiraagu. However, there is no disclosure on the type of data that is collected.

There is no disclosure on the type of information that is collected, and whether customers are informed to the extent legally possible when their user information has been demanded by governments and other third parties, when government entities (including courts or other judicial bodies) demand their user information, or through private processes.

Recommendations

It is important that Dhiraagu provide terms and conditions and privacy policy in local Maldivian language and in other commonly spoken languages, in addition to the current version in English.

It is recommended for Dhiraagu to increase transparency, and disclose the processes of service enforcement such as termination of service for a customer. It is also important to disclose the process for monitoring activities such as child sexual abuse and inform the public.

It is important that Dhiraagu reveal the procedures that are followed in responding to requests by the government to verify the content before termination of service to a customer. Currently a customer's service may be terminated with or without informing the customer.

It is recommended that Dhiraagu publishes a clear and transparent shut down policy, and promotes the rights of a customer with the premise that a customer may be innocent at times of suspicion.

There is a need for amending the Telecommunication Act 2015 to promote user information rights. Dhiraagu should cooperate with the government in improving the legal context on digital good governance.

There is a need for Dhiraagu to clearly disclose the procedure it takes in responding to demands for user information from government, non judicial, court orders or foreign jurisdictions

There is also a need for Dhiraagu to disclose what it can do at its sole discretion and the policy on due diligence it follows in responding to demands for user information from authorities.

There is a need to disclose the statistics on the number of requests it receives from the government, court orders, law enforcement and national security.

It is important that Dhiraagu disclose information on the type of data that is collected about customers, and shared to third parties.

Terms and Conditions for Smartphone Devices and plans
https://www.dhiraagu.com.mv/clients/Dhiraagu_CA2BB809-3A22-485B-A518-DA6B6DE653A5/contentms/img/document/tnc/DhiraaguGeneralTnC.pdf

OOREDOO

Ooredoo Maldives is a member of Ooredoo Group, headquartered in Qatar. The Company

launched its operations in the Maldives on August 01, 2005 as Wataniya Telecom Maldives Private Limited. The Company is the second licensee to be issued with a mobile telecommunications service provider license in the Maldives, and is one of the three companies that have the license to provide internet services. The Company changed its name to Ooredoo Maldives Private Limited on December 22, 2013. The Company changed its legal status to that of a public limited company on 6th October 6, 2016 and was accordingly re-registered as Ooredoo Maldives Public Limited Company. Majority shareholder Wataniya International FZ-LLC holds 90.5% and the Maldives Pension Administration office holds 5.64% of the issued shares of the Company, while the remaining 3.86% of the shares are held by other public shareholders

KEY TAKEAWAYS:

Access to Terms of Service and Privacy Policy

Ooredoo has two separate documents for the terms and conditions of Ooredoo's service, and the privacy policy. However both of these are provided only in English. This means it may not be easy to understand for those who do not speak English. TThe content is not available in Maldivian language. There is also a large Bangaldeshi expat community in the Maldives, tourists from many countries.

Process of service enforcement

Oooredoo prohibits customers to call, message or send, upload, download, use or re-use any material which is offensive, abusive, indecent, defamatory, obscene or menacing, a nuisance or a hoax in breach of any rights or privacy or otherwise, and fraudulently in connection with a criminal offense, in a breach of any law or statutory duty.

Individuals or private entities can raise an issue if they have been threatened by a customer. However, currently there is no information on the processes in which the contents are identified, except when the government authorities inform and request that a customer's account be terminated.

According to the terms and conditions, Ooredoo may give 7 to 30 days advance notice prior to disconnection. However, if this is how it is implemented is not known.

Network management and shutdown

Ooredoo currently prioritizes the requests of the government authorities, but does not disclose that it does not always block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network.

On network management, there is no information if Ooredoo engages in practices, such as offering zero-rating programs, that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network.

It is not clear the internet shutdown policy for particular areas or groups. However, under the privacy policy states internet access might not be available due to maintenance, repairs and unforeseen situations, such as disasters. Moreover, according to the terms and conditions, if Ooredoo may delay connection or disconnect services to devices, if Ooredoo suspects that there has been an application with false particulars. Ooredoo will connect or reconnect services if it is found that the suspicions prove to be groundless. However, It is further stated that the customer cannot claim against the company in respect of any delay or disconnection caused as a result of

the operation of this condition. That would mean that the company will take no responsibility for any damages a customer has even when the shutdown was done by false suspicion. The customer may not even know that the disconnection happened because of that, as there is no indication that the customers are informed.

Moreover, there is no information if Ooredoo has a procedure to push back on government demands to shut down a network or restrict access to a service. Ooredoo also does not disclose demands by specific legal authorities and number of demands it has complied.

Process for responding on user information

The process in which Ooredoo responds to government demands for user information is not clear. In the terms and conditions, it is mentioned that the basis for responding to government demands, is the law of the Maldives. However, the Telecommunication Act 2015, does not adequately address issues related rights of the customer, and user information. Currently there is no cyber law in the Maldives.

Currently there is no information disclosed by Ooredoo on how it responds to demands by government, non judicial, court orders or foreign jurisdictions, for user information. However, In the terms and conditions, it is mentioned that Ooredoo may, in its sole discretion, terminate an agreement to provide a service to a customer, at any time if Ooredoo is requested to terminate, bar, suspend or revoke the dustomer's use of the service by relevant Government authority. It is not clear why Ooredoo used the term sole discretion in this context.

Ooredoo also does not disclose that it carries out due diligence on such demands before deciding how to respond. Currently there is no information on the extent to which Ooredoo can take decisions with sole discretion, when faced with demand by a government authority.

This is relevant because there can be inappropriate or overbroad government and may vary based on the government institute that demands it. Ooredoo does not provide clear guidance or example of implementation of its process for government demands.

Data about government demands and user information

Ooredoo does not disclose any list or statistics on the number of requests it receives. Therefore it is unknown on the demands that come from the government, court orders, law enforcement and national security.

There is also no information that explains what types of government demands it is prohibited by law from disclosing. Ooredoo has not disclosed any such data. The annual report is mainly on corporate development, and the economic performance.

User information about third party requests

According to the privacy policy, the company may supplement the information that is collected about customers with information the company receives from other sources, public registers such as the electoral roll.

It is not clear on all the type of information that is collected about the customers. But it is disclosed that without limitation, data may be collected by Ooredoo website, App, on name, contact information such as email addresses and telephone numbers; demographic information such as post code, preferences and interests; and activity on the website and the App, and the site that is excited to exit to; and and “other information applicable”, the meaning of which is not explained.

It is stated that Ooredoo does not knowingly collect personal data from children. We do not take specific steps to protect the privacy of children who disclose their personal data to us.

In the privacy policy it is stated that to the extent permitted by law, certain nonpublic information about customers may be disclosed to comply with a request or order of a governing authority; to provide information to affiliates of the firm and non-affiliated third parties who perform services or functions for us in conjunction with our services to customers, if Ooeredoo have a contractual agreement with the other party that prohibits them from disclosing or using the information other than for the purposes for which it was disclosed.

There is no disclosure whether customers are informed to the extent legally possible when their user information has been demanded by governments and other third parties, when government entities (including courts or other judicial bodies) demand their user information, or through private processes. The customers therefore do not know the type of information and the extent that is shared about them.

Recommendations

Ooredoo needs to provide terms and conditions and privacy policy in local Maldivian language and in other commonly spoken languages, in addition to the current versions in English.

It is recommended for Ooredoo to increase transparency and disclose the process of service enforcement, such as termination of service for a customer.

It is also important to disclose the process for monitoring activities, when an individual or private entity informs of being threatened, and how Ooredoo responds to government requests.

It is important that Ooredoo reveal the procedures that are followed in responding to requests by the government to verify the content before termination of service to a customer.

As an ethical practice, it is important that the customers be informed when his/ her service is disconnected for investigation purposes. Therefore a clear shutdown policy is needed to be disclosed to the public.

There is a need for amending the Telecommunication Act 2015 to promote user information rights. Dhiraagu must cooperate with the government in improving the legal context on digital good governance.

There is a need for Ooredoo to clearly disclose the procedure it takes in responding to demands for user information from government, non judicial, court orders or foreign jurisdictions

There is also a need for Ooredoo to disclose what it can do at its sole discretion and the policy on due diligence it follows in responding to demands for user information from authorities.

There is a need to disclose the statistics on the number of requests it receives from the government, court orders, law enforcement and national security.

It is important that Ooredoo disclose information on the type of data that is collected about customers, and shared to third parties.

Our Privacy Policy | Ooredoo Maldives
Terms and Conditions | Ooredoo Maldives

Internet Freedom Impact (2.2)

2.2.1 - **Accessing the internet and internet services** - during 2021, the citizens of Maldives did not have any deliberate restriction to the internet, or, restrictions that were announced and/or publicized. However, there were minor incidents of temporary outages and/or slowing down of internet and internet services which were attributed to technical difficulties from service providers. Some challenges include access to remote learning during early 2020, covid-19, Effective capacity to learn from internet-based packages (Google Classroom, Google-Meet) and by Viber was reportedly challenged by insufficient bandwidth, the need for access to shared devices, data download limits, and effective connection speeds[1]. It is unknown whether these events were due to acts of malfunction. It is not foreseeable that any such restrictions will be made in 2022 or 2023, due to the presence of civil society organizations such as transparency Maldives who advocate freedom of expression and rights in the Maldives.

2.2.2 - Content restrictions of blocking (censorship) - 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 the Maldives, however, this has never been formally enacted upon. The Communications Authority of Maldives (CAM) is reported to maintain an unpublished blacklist of blocked offending websites. It has not been suggested that the CAM monitors websites for content breaches proactively, however, it does accept requests to block websites from government ministries and public authorities. In 2014 Communication Authority of Maldives blocked six websites disseminating anti-Islamic view. The leading grounds for such blocking are alleged violations of Religious Unity Act of Maldives, 6/94, **under chapter 6** states prohibited activity "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. Telecasting and broadcasting of such speeches shall be deemed illegal")[2]. On November 30th (Tuesday) 2021, times of Addu online news states that, the criminal court of Maldives has given 21 hours to Maldives police service to shut down all internet mediums used to promote religion other than Islam. The order was made under the Religious Unity Act (Act No. 6/94) which prohibited the practice by citizen of any religion other than Islam. However as of date, no sites have been blocked. It is uncertain whether there will be any changes in the year ahead.

- The times of Addu, Internet service providers ordered to shutdown Contents promoting religion other than Islam: (https://timesofaddu.com/2021/11/30/isps-ordered-to-shutdown-content-promoting-religions-other-than-islam-within-72hrs/)
- Center for law and Democracy: (https://www.law-democracy.org/live/wp-content/uploads/2021/10/Maldives-Report.Final_.pdf)
- Six websites disseminating anti-Islamic views blocked: (https://en.sun.mv/24921)
- Website have not been blocked: (https://voice.mv/50765/)

2.2.3 - Use of privacy-enhancing and circumvention technologies - As of date, there are no restrictions, moreover, the use of Virtual private network (VPN) and circumvention technologies have increased during the COVID-19 pandemic, as organizations have installed and used Wide

[1] Maldives Case Study, Situation Analysis on the effects of and responses to Covid-19 on the Education Sector in Asia, UNESCO and UNICEF, October 2021 (https://www.unicef.org/rosa/documents/maldives-case-study)

[2] New Religious unity regulation: English (https://minivannewsarchive.com/society/new-religious-unity-regulations-english-6877)

Area Virtual Networks for extending workspaces to homes. There was an incident in December 2021, people complained they couldn't access clubhouse (the social Audio App) without using VPN, however CAM stated that they did not block the App. Also, persons routinely use circumvention technologies to access region-locked content on web services such as Netflix, YouTube, etc. It is not forecasted that any restrictions will be made in the next couple of years.

- Clubhouse App was not blocked: (https://mihaaru.com/news/101954)

2.2.4 - Monitoring and surveillance of online behavior – In November 2020, minister of home affairs Mr. Imran Abdulla, mentioned that there are challenges dealing with cybercrimes, due to lack of comprehensive cybercrime legal framework and hurdles in gathering evidence impact the effectiveness of police work. There have been no news reports that indicate monitoring and surveillance of online behavior; however, it is a known fact that Wi-Fi packet-sniffing and such surveillance happens by tech-savvy deviants in the community, especially in the cities. Surveillance equipment (CCTV camera) that belongs to the state are quite plentiful within urban areas, located on the roads and it is unknown whether this equipment can access and intercept data on encrypted private Wi-Fi channels. There are no indications that the state will be taking steps in the years ahead.

- Lack of cybercrime legal framework: (https://www.gov.mv/dv/files/upr-maldives-intervention-on-reforming-law-enforcement-agencies-freedom-of-expression-and-association-transcript.pdf)

2.2.5 - Hate and dangerous speech - There are several reports of hate speech, dangerous speech, instigatory and threatening speech made on various platforms by known and unknown perpetrators, out of which very few have been acknowledged, addressed and/or prosecuted. In rare occasions, online expressions have resulted in further repercussions leading to physical violence[3]. It is very rare that such actions lead to murder. Crime statistics data in detail have been last published for 2020 statistics. As for data from 2020, there is no category of data on physical violent crimes that are connected to online activities. Anecdotal evidence suggests that between 2012 and 2017 there were at least three cases in which the victims had expressed views on media or online and later become victims of physical assault. One of them was a parliamentarian and an Islamic scholar, the two others were bloggers and journalists. Although data on and dangerous speech is not published, the police statistics do indicate that in 2020, there were a total of 19 cases investigated on threats done online, 6 cases investigated for threats done through sms.

In an attempt to address hate related crimes, in November 2021, the president signed a bill as an addition (2/2021) to penal code (9/2014). In how public spaces are defined in the law, it includes online media such as online forums. In defining public spaces, apart from the physical public spaces, it also includes platforms facilitated by radio, television, internet technologies. In clause 124 (a3) it is mentioned that if someone harms or encourages harm to someone based on ethnicity, country of birth, race, political views, religion, it is an offense. What is not defined or mentioned is what constitutes a harm. This increases the vulnerability of the victims. As per the Strategic Action Plan 2019 - 2023 of the Maldives, there are strategies in several sections that will address such issues, ensuring safety and well-being of persons in the Maldives. There are no indications that the state will be taking steps in the years ahead.

[3] Nikki Asia, hate crime bill widens Islamic division in the Maldives, Marwaan Macan- Markar, Asia regional correspondent, July 22, 2021

- https://gazette.gov.mv/gazette/6257
- Maldives passes hate crime bill to check extremism: ban public usage of terms "non-believer" or "Kafir" (https://www.southasiamonitor.org/maldives/maldives-passes-hate-crime-bill-check-extremism-bans-public-usage-terms-non-believer-and)
- Hate crime bill widens Islamic divisions in the Maldives: (https://asia.nikkei.com/Politics/Hate-crime-bill-widens-Islamic-divisions-in-the-Maldives)
- Crime statistics: (https://www.police.gov.mv/#casestat)
- Hate and assaults (https://thepress.mv/122066)

2.2.6 - Disinformation - Widespread political disinformation currently exists on social media platforms, mainly twitter.com. In February 2020, Health protection agency of Maldives tweets about the misinformation about covid-19, confirmed cases circulated to raise fear in the country. (https://twitter.com/hpa_mv/status/1233747516681678848). On 19th march 2020, The Maldives broadcasting commission conducted an investigation, following persistent and numerous complaints from the general public on the broadcasting by certain channels, which contained inaccurate and misleading information concerning the Covid-19 situation in the Maldives. Moreover, the police also warned against the public commenting untrue information on the comment sections on online news sites.

In December 2020, a statement issued by the Ministry of Foreign Affairs expressed concern over spreading hatred, misleading information and false allegation regarding bilateral ties with India and it further reads that all parties and political leadership to act responsibly and to refrain from spreading false information. While the Strategic Action Plan 2019 - 2023 has a strategic plan *(Page 339, Heading 4.8, Policy 1, Strategy 1.2)* that addresses this problem, it has yet to be enacted by the state. Policy 1, Strategy 1.1 further outlines the various government policies related to internet and internet services, and internet service providers, that will need to be updated and modernized.

- Statement by the government of Maldives to censure local news outlet channel 13: (https://www.gov.mv/en/news-and-communications/statement-by-the-government-of-the-republic-of-maldives-on-the-decision-by-the-maldives-broadcasting-commission)
- Individuals spreading false information: (https://psmnews.mv/en/67170)
- Maldives concerned over misinformation against India: (https://thedailyguardian.com/maldives-concerned-over-misinformation-against-india/)
- Strategic Action Plan (SAP) 2019-2023: (https://storage.googleapis.com/presidency.gov.mv/Documents/SAP2019-2023.pdf)

2.2.7 - Net neutrality breaches - To date, all three internet service providers in the Maldives (Dhiraagu, Ooredoo and ROL) have individualized services that serve content that is not on public domain (such as commercially produced entertainment content on DhiraaguTV), however they do not infringe upon access to public domain content. They provide internet bundles with free access to social media such as Facebook and Viber. It is uncertain whether there will be any changes in 2022 or 2023.

- Dhiraagu packages:
  https://www.dhiraagu.com.mv/personal/for-mobile/plans/prepaid

Resources / Other focus on Digital Rights

1- Maldives journalist Association (MJA), www.mja.org.mv, mjamaldives@gmail.com
2- Human Rights Commission of the Maldives (HRCM), www.hrcm.org.mv, +960 3336539, +960 3003130, informationofficer@hrcm.org.mv
3- Transparency Maldives, www.transparency.mv , +9603304017, office@transparencymaldives.org
4- Association for Democracy in the Maldives (ADM), https://democracymaldives.org, admin@democracymaldives.org
5- Society for Peace and Democracy, www.peacedemocracy.org, info@peacedemocracy.org +960 9182819
6- Department of law, Faculty of Sharia's and law, the Maldives national University, email: Fathimath.waheedha@edu.mv