



**USAID**  
FROM THE AMERICAN PEOPLE



**Internews**  
Local voices. Global change.



**ADVANCING RIGHTS**  
IN SOUTHERN AFRICA  
ARISA



# **A SURVIVAL TOOLKIT FOR JOURNALISTS:**

## **HOW TO PROTECT YOURSELF AGAINST DIGITAL SURVEILLANCE**

# ACKNOWLEDGEMENTS

The Survival Toolkit for Journalists: How to protect yourself against Digital Surveillance guide was developed in response to the growing threat of digital surveillance and cyber security legislation, used by governments and others to track and monitor journalists in their efforts to harass and muzzle journalists from carrying out their work. The guide provides journalists and media houses with a deeper understanding of the legal frameworks on cyber security laws in the SADC region, and offers critical knowledge and tools that can be implemented by journalists and media houses to protect their online spaces, digital footprint and data.

ARISA would like to thank and acknowledge Golden Maunganidze of the Regional Media Institute (MISA) of Southern Africa, Jean le Roux of DFR Lab and Tawanda Mugari of Digital Society of Africa, for developing the informative and rich content contained in the Toolkit, we know that it will be an important resource for journalists across the region.

Specific acknowledgment is also given to Dr. Allen Munoriyarwa, from the University of Johannesburg, who worked closely with the ARISA team to develop the program and content for the Digital Surveillance training program and who provided additional insights and expert knowledge into the Toolkit. ARISA would also like to thank Golden Maunganidze of the Regional Media Institute (MISA) of Southern Africa for writing the Foreword for the Toolkit.

- © *Advancing Rights Southern Africa (ARISA)*
- © *Media Institute of Southern Africa (MISA)*
- © *DFRLab*
- © *Digital Society Africa*



**MISA Regional** advocates for media freedom and freedom of expression in southern Africa.

**Atlantic Council's Digital Forensic Research Lab (DFRLab)** has operationalized the study of disinformation by exposing falsehoods and fake news, documenting human rights abuses, and building digital resilience worldwide.

**Digital Society of Africa (DSA)** works to strengthen the resilience and ability of frontline activists; human rights defenders and other at-risk groups in the region to independently recognize and respond to digital threats and attacks.



**USAID**  
FROM THE AMERICAN PEOPLE

This toolkit is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of ARISA and do not necessarily reflect the views of USAID or the United States Government.

# TABLE OF CONTENTS

<b>ACKNOWLEDGEMENTS</b>	<b>2</b>
<b>FOREWORD</b>	<b>4</b>
<b>1. INTRODUCTION</b>	<b>6</b>
<b>2. INTERNATIONAL FRAMEWORKS ON SURVEILLANCE AND PRIVACY ISSUES</b>	<b>7</b>
International Legal Instruments	7
Regional Legal Instruments	7
Key Features of Surveillance Laws in the SADC Region	9
<b>3. TACTICS OF SURVEILLANCE USED ON JOURNALISTS</b>	<b>10</b>
<b>4. UNPACKING THE DIGITAL SECURITY SURVIVAL TOOLKIT</b>	<b>11</b>
Operational Security	12
Personal Security	16
Support Structures for Journalists	17
Digital Hygiene Best Practices	20
Protecting Your Data	22
Advocacy Opportunities	23
Additional Resources and Training Opportunities	24
<b>5. CONCLUSION</b>	<b>25</b>

# FOREWORD

## IN DEFENCE OF DIGITAL SPACE IN SOUTHERN AFRICA IN THE AGE OF SURVEILLANCE

Online technologies have enabled the exercise of freedom of expression and access to information in a way never imagined before. People are freer to express themselves while access to information is literally at their fingertips. The truth of this proposition is self-evident. However, while these technologies have been a facilitator for freedom of expression, they also allow for digital surveillance of citizens and more particularly journalists and activists globally and continentally in general and in Southern Africa region specifically.

The irony is that online and digital technologies are enabling tools for freedom of expression, but they are also the biggest threat to that very same right. Such complex contradictions constitute a colossal challenge, that urgently requires a competitive response aimed at safeguarding the former against the latter. We are convinced that the defence of expression online in the face of surveillance, constitutes an engine upon which the right to express and citizens make informed decision making towards our collective good as a people of Southern Africa. Such a defence shield cannot be built through a fragmented approach, but rather through regional, continental, and global collaborative efforts. This is mainly because governments are increasingly acquiring new tools that help them surveil citizens, infringing on the right to privacy through collaborative efforts with other states.

The right to privacy is a prerequisite for journalists to do their work and ensure access to fact-based and reliable information. Privacy is a necessity if journalists are to communicate freely with sources, receive confidential information, investigate corruption, and guarantee their safety and that of their sources. For this reason, there is a need to ensure that the right to privacy is protected because without it we risk having societies that are characterised by self-censorship, thereby translating to decreased access to information and ultimately undermining democracy.

Anecdotal evidence in Southern Africa shows that governments in the region are increasingly resorting to digital tools for surveillance and this is a serious cause for concern. Freedom of expression and of the media are quite fragile in the region and the acquisition of such tools could be the death knell of these rights in the region. At least three Southern African countries; Botswana, Zambia, and Zimbabwe – have acquired sophisticated tools developed by an Israeli company, Circles, which they use to monitor the behaviour of their citizens online. Furthermore, what is worrying is that most countries in Southern Africa are coming up with cyber security laws, which in principle are needed, but these are used as a guise for surveillance.

Just recently, Zambia fast tracked a cyber security law, Zimbabwe enacted one and other countries such as Botswana, Namibia, Lesotho, and Mauritius are in the process of developing theirs. In 2021, the South African Constitutional Court ruled that the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) was unconstitutional. The ruling came after a journalist, Sam Sole, who had been the subject of state surveillance, and the Amabhungane Centre for Investigative Journalism applied to challenge the Act's constitutionality. This, therefore, shows that state surveillance of journalists and activists is quite widespread and, as alluded before, this could pose one of the biggest threats to journalism and freedom of expression in a region where democracy is quite nascent.

In such circumstances, the need for upskilling digital security for journalists cannot be overemphasised. Therefore, the development of this toolkit is quite timely, as it provides best practices on digital security and digital hygiene for media houses and journalists. It includes operational security, developing a digital security policy, and the use of virtual private networks (VPNs). The toolkit also provides explainers of key surveillance software and terminologies. Quite importantly, it also provides resource links to open-source software and digital security software, which journalists can explore and use to protect their privacy online.

This toolkit will also equip journalists with knowledge on the software, actors and their roles and responsibilities in protecting themselves. It will also provide a basic digital hygiene tool kit aimed at protecting social media platforms and their digital devices. It is our hope that journalists will find this toolkit useful and will use it to protect themselves and their sources of confidential information.

Although primarily developed for journalists, the toolkit can also be adopted by activists and other citizens who seek to protect themselves and their online communications. Since technology is a fast-paced terrain, this is the first step towards a marathon of continuously reviewing the gaps and proactively attending to the future needs which will be part of a mix of interventions including training, networking, and knowledge exchange platforms.

*Golden Maunganidze*

**MISA Regional Chairperson**



# 1. INTRODUCTION

Surveillance of journalists has become a very topical and controversial issue that now requires attention at a number of levels – the level of the state, CSOs, and journalism organisations themselves. The systematic and arbitrary harvesting of journalists' information, tracking and targeting of journalists is on the increase especially in the SADC region where some regimes seek to retain control of the media and stifle divergent views and suffocate opponents. In countries such as Zambia, Zimbabwe, Namibia and Malawi, there is deep-rooted fear that enacted cyber laws are already being used for surveillance purposes. For instance, South Africa uses the RICA Act to regulate the interception of communication and Zimbabwe has the Interception of Communications Act while Zambia deploys the Electronic Communications and Transactions Act of 2009. Thus, anecdotal evidence in Southern Africa shows that governments in the region are increasingly resorting to digital tools for surveillance and this is a serious cause for concern.

At least three Southern African countries; Botswana, Zambia, and Zimbabwe have acquired sophisticated tools developed by an Israeli company, Circles, which they use to monitor the behavior of their citizens online. This calls for journalists, their organisations and other media- support institutions to act in ways that protect journalists from surveillance, be it by state or non-state agency. There is need, therefore, to come up with a toolkit of strategies that journalists in Southern Africa can make use of in quotidian news gathering and reporting practices. State security agencies have been the most serious threats to journalists. This is because they have the technical know-how, huge budgets to practice surveillance, and trained people. More importantly, in a region where state security apparatuses are view as partisan, they also have a political motive. At an international level, the UN has come with a standard instrument that seeks to safeguard privacy and protect individuals from surveillance. Though not necessary addressing journalists per se, this framework is important to tease out here as it contextualises some of the points made in the toolkit.

## 2. INTERNATIONAL FRAMEWORKS ON SURVEILLANCE AND PRIVACY ISSUES

Surveillance is strongly linked to practices of privacy. An increase in surveillance practices, deleteriously impact the enjoyment of the right to privacy. As espoused in many regional and international statutes, privacy is a fundamental human right. The 1948 Universal Declaration of Human Rights recognises the right to privacy. The International Covenant on Civil and Political Rights (UN 1966) equally recognises the right to privacy of communication as a universally guaranteed right. Article 12 of the Universal Declaration of Human Rights states that:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks’

(UN, 1948)

Article 17 of The International Covenant on Civil and Political Rights reinforces the right to the protection of privacy without discrimination. These international legal instruments, however, recognises violations that are based on law. Yet, in the same vein, they recognise that the violation should have to intention to achieve a legitimate aim, and as such, it should be proportionate to the aim being pursued (Privacy International 2014). Majority of legal instruments also recognises the dangers of mass and indiscriminate surveillance. The preference is for targeted surveillance that pursues legitimate aims. In addition to legitimacy, surveillance ought to be proportionate, and making provision for other safeguards like user notification, judicial authorisation and other transparency and oversight mechanism supposed to be inflected within the practice.



### INTERNATIONAL LEGAL INSTRUMENTS

The UN Human Rights Council promulgated the Promotion, Protection and Enjoyment of Human Rights on the Internet in 2016. In 2018, the UN passed the Right to Privacy in the Digital Age. Both instruments recognises the right to privacy and the need to limit surveillance. They, therefore, provide guides on which local legislation can draw on in order to provide rules and regulations that protect privacy as a fundamental human right. Moreover, both international instruments provide a standard on which local surveillance regulations can be assessed in term of the extend to which they align with global standards for the protection of privacy.



### REGIONAL LEGAL INSTRUMENTS

At a regional level of SADC, The Declaration of Principles on Freedom of Expression and Access to Information promulgated by the African Union (AU) remains the guide on which surveillance and privacy issues are clearly articulated. The instrument is very clear in terms of the circumstances under which surveillance can be permissible. It states thus,



States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.

**(Principle 41, The Declaration)**

This declaration makes it explicitly clear that indiscriminate surveillance, untargeted surveillance, collection analysis and sharing of a person's communication is illegal. In addition to this, states are encouraged to ensure that domestic legislation on surveillance comprehensively safeguard the right to privacy. Amongst the internationally accepted standard safeguards are limitation on targeted surveillance imposed by a judicial authority, specific time limitations on surveillance, well-defined scope of surveillance and user notification. An important safeguard to recognise is the right to privacy. Both international and regional declarations impose a responsibility to other rights associated with privacy, for instance, the right to anonymity. Even the African Union declaration recognises these rights recognises that there is need to put in place some standard safeguards that fence off individual privacy from the prying eyes of surveillance forces and institutions. To make the safeguards functional and effective, they should be built in the constitutional arrangement of every country. For example, the requirement for judicial authorisation, just and appropriate, time-framed surveillance should be creatures of the legislation. This is meant to promote both accountability and transparency in the architecture of the surveillance system. Even though the AU declaration is a positive and forward-looking document, many countries have not yet ratified the document. Others have drifted into draconian legislative practices that curtail the very freedoms the declarations are meant to protect. Perhaps we must briefly flesh out the principles that govern transparent practices of digital surveillance. There are two very important such principles the necessary and proportionate principles.

## **THE NECESSARY AND PROPORTIONATE PRINCIPLES**

In addition to the intra-national and regional legal instruments have explored above, there is also the International Principles on the Application of Human Rights to Communications Surveillance (generally referred to as 'The Principles'). In 2013, hundreds of CSOs, agreed to adopt these principles as the threat of surveillance escalated and the respect for human rights lagged behind in some countries. Leading these efforts were organisations were Privacy International (PI), the Open Rights Group, Electronic Frontier Foundation (EFF) and Association of Progressive Communications (APC). The principles promulgated about 14 key practices that would lead to the observation of human rights. At the same time, they would lead to respect for other individual rights associated with human rights. They emphasised the centrality of judicial authorisation in surveillance. However, the emphasis was also on a competent judiciary, and, thus, not just a judiciary. Furthermore, important aspects of surveillance featured heavily in the principles. For instance, an emphasis on legitimate aims of the practice, legality, proportionality and the importance of user notification. There has been a broad acceptance that these principles represent what can ultimately morph up to be a global standard for surveillance practices. Suffice to mention that they have not been without criticism. Chief amongst these criticisms being that the principles represent the ideological, political and economic interests of the funders. Regardless of these criticisms, these principles represent a very positive, internationally accepted starting point on which surveillance practices at local levels can be anchored.





# KEY FEATURES OF SURVEILLANCE LAWS IN THE SADC REGION

Surveillance legislation in the region lags behind in terms of adherence to international standards as explained above. Countries in the region have promulgated legislations that do not, in many instances, meet these demands for transparency and accountability. Thus, the International Principles on the Application of Human Rights to Communications Surveillance, the UN Draft Instrument on Government-led Surveillance and Privacy and the African Commission (2019) Declaration of Principles of Freedom of Expression and Access to Information in Africa frameworks are still to be fully realised in many countries of the region.

**A general trend is the absence of the core ingredients of transparent and accountable surveillance. Interception of communication is still not legal in most instances. Retention of metadata after surveillance is still whimsical and not properly regulated in some countries. Most of the countries provide no mechanism for use notification.**

**TABLE 1: SUMMARY OF THE FEATURES**

Country	Is there a law?	Is there judicial oversight on the police?	Is there judicial oversight on intelligence officers?	Is it restricted to serious offences?	Is there user notification?	Are metadata and content given equal protection?	Does law require metadata to be retained?	SIM registration?
South Africa	✓	✓	✓	✓	X	X	36 months	✓
DRC	✓	✓	X	X	X	X	X	✓
Tanzania	✓	X	X	X	X	X	X	✓
Malawi	X	X	X	X	X	X	X	✓
Botswana	✓	✓	✓	X	X	X	X	✓
Eswatini	X	X	X	X	X	X	X	✓
Lesotho	✓	✓	✓	X	X	X	36 months	X
Namibia	✓	✓	✓	✓	✓	✓		X
Mozambique	X	X	X	X	X	X	X	✓
Angola	✓	✓	✓	✓	X	X		✓
Zambia	✓	✓	✓	X	X	✓	3 months	✓
Zimbabwe	✓	X	X	X	X	X	6 months	✓

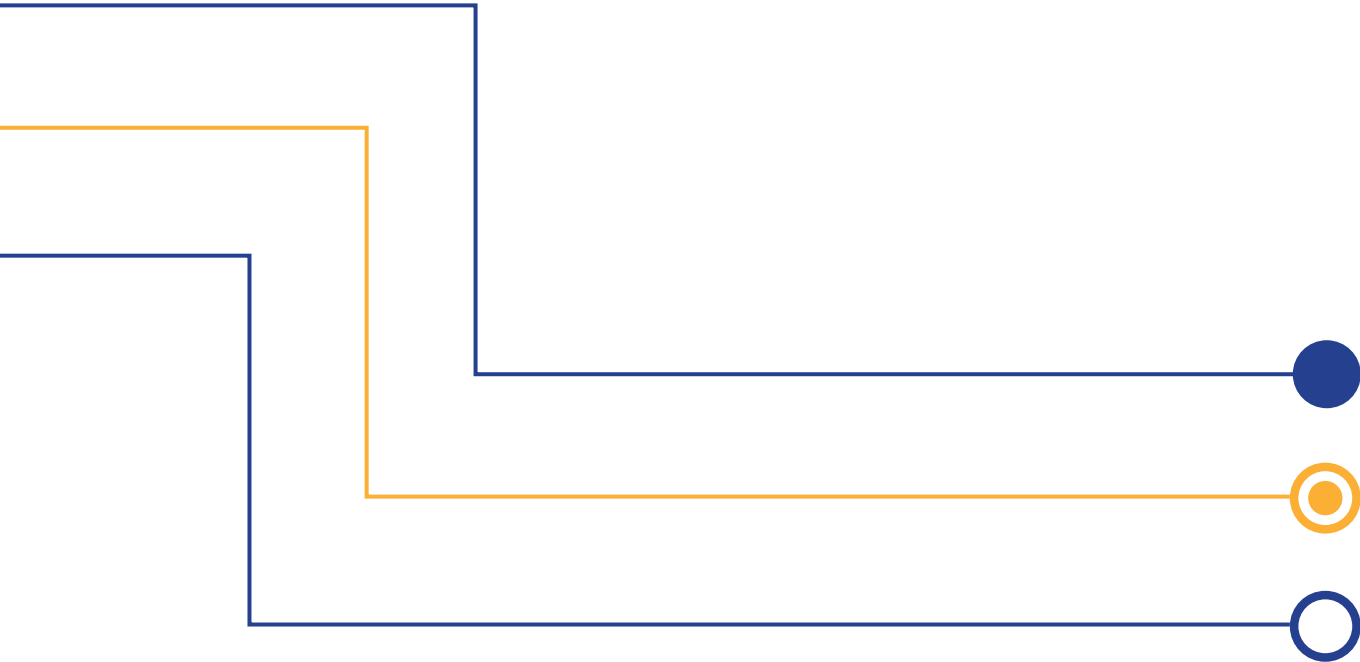
Source: Munoriyarwa and Mare, forthcoming

# 3. TACTICS OF SURVEILLANCE USED ON JOURNALISTS

In the table below, we outline the digital tactics that journalists can be subjected to. Journalists in the SADC region must be aware of these tactics mainly used by governments or other state institutions against journalists.

**TABLE 2:** SURVEILLANCE TACTICS

SURVEILLANCE TACTIC	DESCRIPTION OF TACTIC
Electronic communication surveillance	Surveillance of email, instant messenger, text and voice (both landline and mobile). tapping, bugging, NSO surveillance tool.
Public space surveillance	Using existing public space, like CCTV infrastructure to monitor where journalists go, who they meet, which places they visit. Also included here is videotaping.
Geo-location surveillance	The use of location technologies such as GPS or IP addresses to identify and track the whereabouts of connected electronic devices. Because these devices are often carried on an individual's person, geolocation is often used to track the movements and location of people.





## 4. UNPACKING THE DIGITAL SECURITY SURVIVAL TOOLKIT

The fast pace of change in digital technologies means that those intent on surveilling journalists now have many options in their arsenal of surveillance. Surveillance has become more stealth and effective. The toolkit offers journalists and media houses practical steps and knowledge that can be easily implemented to fight back against creeping surveillance. In this section on Operational Security, the toolkit outlines what journalists can do upon realisation that they are subject to surveillance and is especially helpful for those covering sensitive assignments.

# OPERATIONAL SECURITY

Journalism, and particularly investigative journalism, often takes place in contested information environments, and the very act of exposing the truth can upset powerful or dangerous individuals and organizations. While the risks of investigating stories in the public interest is not new, social media and digital platforms have emphasised the opportunities - and risks - associated with conducting investigations. To this end, it is important for journalists and open-source researchers to conduct their work online in a manner that keeps themselves and their sources safe.

## A. CREATING AND USING INVESTIGATION ACCOUNTS

Always conduct your investigation using a separate, purposefully created account that cannot be linked back to you. A suite of investigations accounts is trivial to set up, and the benefits are numerous.

- **Set up a dummy email.** Create a new email address using any of the free email providers (Gmail, Yahoo and Microsoft are all acceptable) that cannot be linked back to you. **ProtonMail** (<https://protonmail.com/>) is a more secure option but will sometimes be flagged as “suspicious” by social media platforms and require you to provide additional information. One can also check if their email account has been exposed through a platform data breach on <https://haveibeenpwned.com/>

- **Set up your investigations accounts.** Create your investigation accounts on the various social media platforms using this new email address. Use generic usernames or profile pics that cannot be traced back to you. Make sure you also have setup multi-factor authentication and have reviewed the security settings on all accounts. HavelBeenPawnd is the only reliable tool to use for this. In other cases you'll usually realise your account has been compromised based off of the fact that you can no longer access the account.

- **Don't allow the platforms to find your contacts.** In some cases, social media platforms might prompt you to provide it with access to your contacts. Never allow this; not only does it provide a link between your real identity and your investigations account, but it can also suggest your contacts to your investigation target as possible friends.

- **Engage as little as possible.** Follow as few other accounts as possible (if any at all) and never interact with any of the content you're investigating. This includes liking, sharing or commenting on posts.

- **Be mindful.** While using your investigation account, be mindful of your actions. Ensure you're using the correct account before sending a DM, and make sure you don't accidentally reveal your investigation accounts when taking screenshots for your article.

Not only does using your personal accounts potentially expose you (and by extension your friends and family) to the subject of your investigation, but it could also alert them to the fact that they are being investigated in the first place.

## B. USE VPN'S AND BROWSERS

It is recommended to use a virtual private network, or VPN, while conducting your investigations. A VPN is used to obfuscate your computer's online "identity" while accessing websites and resources on the web, in essence creating a layer between your computer and the website you are accessing. Although some east-European countries have banned the use of VPN's, countries in the SADC bloc have no legal prohibitions against using a VPN to access the internet.

In simplified terms, when you access an online resource your device sends a request to the website through your internet service provider. This request contains certain information about your connection, including the return address. The response is then sent back to your device. When investigating a malicious website, or conducting an investigation, it is prudent to use a VPN to limit the amount of information linking back to your device or your organisation. However, it is also important to note that a VPN can only be used where there are blockages of certain online platforms. It cannot assist if there is a total Internet blackout.

**Adding anonymity.** A VPN adds another layer to this exchange between your device and the online resource. Your device's request is sent to the VPN provider first, which in turn sends the request to the online resource you requested. The response is then sent back to your VPN provider, which forwards the information to your browser. If the website you've accessed is monitoring the devices accessing it, they will only be privy to the details of the VPN provider, and not your device. The trade-off is between speed and privacy, with VPN's being slightly slower as a result of the additional layer of communication.

**Encrypted communications.** Additionally, a VPN encrypts the traffic between your device and their servers. Any attempts at intercepting the communication would be futile as the information can only be decrypted by either the VPN provider or your device.

**Circumventing geoblocks.** VPNs are also useful for circumventing geo-blocked online resources. Some websites are only accessible to users within their country, and some VPN's can be geolocated to a specific country in order to circumvent such blocks.

An important consideration when choosing a VPN provider is the level of recordkeeping maintained by the VPN provider. Some free VPN providers will maintain access logs, meaning a determined challenger could pursue the legal process required to obtain these access logs. Ideally, you want to ensure that your VPN provider does not maintain any access logs on your activity.

It is always better to make use of a paid VPN which is contractually obligated to destroy your access logs. NordVPN, TunnelBear and ExpressVPN range between \$3 and \$10 per month, but the expense is well worth the utility and the peace of mind.

However if you do need a free, reliable free alternative is ProtonVPN, from the same developers as ProtonMail. While you might see reduced speeds and less VPN servers than the paid options, it is a secure and cost-effective alternative. Some examples of VPNs are **Psiphon** (<https://psiphon.ca/en/download.html>), **TunnelBear** (<https://www.tunnelbear.com/>), and **NordVPN** (<https://nordvpn.com/>) just to mention a few.

## C. PASSWORD MANAGERS AND TWO FACTOR AUTHENTICATION (2FA)

Even the most secure encryption is rendered null if your passwords are weak or compromised. A determined hacker can gain access to your accounts using “brute force” techniques that sequentially tries a database of common passwords, or by using old passwords found on one of several publicly available leaks. Create stronger passwords. This can be done by:

- **Combining upper, lower and alphanumeric symbols.** The more complex a password is, the more effort it takes to expend, and even more so if it's not a dictionary word. For example, the password “newspaper” can be cracked within 0.2 seconds, but “rewspapen” would take around 2 hours to crack. By comparison, “R3wsp@pen!” would need two full months of brute forcing to crack the password. You can use an online password strength checker such as Nordpass (<https://nordpass.com/secure-password/>) to check whether your password is secure enough.

- **Doubling up.** Two factor authentication (2FA) is a secondary layer of protection that can be enabled on most email, social media and even banking platforms. It requires a secondary confirmation when logging into your account from a new device, and can range from a prompt on a 2FA app on your smartphone to an automated voice call or SMS containing the authentication code. **Microsoft's Authenticator** ([https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en\\_ZA&gl=US/0](https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_ZA&gl=US/0)) app & Google Authenticator app are free to use and can work using biometric verification.

- **Use trusted tools to create a password manager.** A password manager can simplify the creation and storage of strong, complex passwords without needing to remember all of them. The drawback: you need a strong, memorable passphrase to secure it. Apps such as KeePassX and LastPass allow you to generate and store passwords centrally and to automatically enter the correct password when visiting a website.

- **... and keyphrase.** The obvious risk is that if your password manager is compromised, all your passwords are compromised too. A strong passphrase is essential: use a series of five or more words to construct a phrase you will remember. HavelbeenPawened can be used to find out if a password has been compromised although ultimately this is the ultimate responsibility of the user to ensure that the password is protected.

- **Take it offline.** There is nothing wrong with writing your passwords down, as long as you take extra steps to keep it secure. A strong password hidden in the margin of an old journal is much better than a weak password you can remember easily.

## D. SANDBOX ENVIRONMENTS AND VIRTUAL MACHINES

When receiving electronic files or digital evidence of an unknown origin, it is important to take the necessary precautions to verify the safety of the files. Anti-virus and anti-malware scans should identify most threats, but for the utmost safety a sandbox environment can be used first.

- **Virtual machines.** A virtual machine or VM is a virtualised environment created on your existing computer or laptop using specialised software. Think of this as a PC within your PC, one that you can reset as simply as pushing a button. If you maintain a fresh installation of Windows or Linux (even trial versions will work) you can access the files in an environment that keeps the rest of your work safe. **VMWare** (<https://www.vmware.com/>) and **VirtualBox** (<https://www.virtualbox.org/>) are popular options for setting these up.



## E. MOBILE PHONES AND SECURITY

Journalists in SADC use mobile phones to conduct their work. The popularity of mobile phone communication has resulted in most journalists being vulnerable with compromised security when using phones. Mobile phone surveillance has been a topic of conversation since news broke of Pegasus spyware and its use against journalists, activists and heads of State. As mobile phones have become smarter, more involved in our daily lives and more connected, the avenues for exploitation have also increased significantly.

**Mobile phone spyware is effective because it circumvents any other forms of protection provided by phone apps. Encrypted messages are intercepted after your device decrypts them, meaning even normally encrypted messaging apps and emails are also compromised. It can gain access to your contact list and phone call logs, gallery files and your phone's geolocation coordinates. It can also use the phone's camera and microphone to listen and watch in.**

As a slight consolation, such sophisticated spyware is extremely rare and expensive to deploy. The vast majority of journalists won't encounter such sophisticated attacks.

### HOW TO KEEP YOUR MOBILE ACTIVITY AND DATA SAFE

- **Keep your phone up to date.** Mobile phone developers frequently identify and patch vulnerabilities in their smartphone operating systems, closing the doors usually left open for attack. Keeping your phone up to date means it has the latest security possible, and known vulnerabilities have been addressed.
- **Don't disable security features.** Smartphones have built-in security features that can limit the impact of malware. Disabling these features are not recommended.
- **Don't click unknown links.** Pegasus was unique in that it could compromise a phone with no user input. The vast majority of malware will however require some form of user input, either through clicking a link or installing a suspicious app. Never click on unknown links, and only install apps from a source you trust.
- **Guard physical access.** Another way of compromising a mobile device is through installing the malware manually. This requires physical access to the device. Make sure you don't leave your phone in the possession of strangers, and ensure you have a passcode or biometric lock enabled on your mobile device.
- **Scrutinize the apps you use.** Every app you install on your device requests certain permissions. For example, your messaging app might request access to your camera or gallery in order to send pictures to your contacts, or to your microphone to record voice notes. Some seemingly innocuous apps will abuse this and sneak in permissions that are excessive and intrusive. There is no reason for a flashlight app to require access to your contact list for example, so before agreeing to the app permission, scrutinise these for the permissions they request.

But what happens when internet access is lost? Some government have throttled or even blocked access to the internet during periods of unrest, and during natural disasters internet connectivity might be non-existent.

Offline messaging apps, such as Bridgefy and Briar allows users to communicate even when the internet is down. These apps create a digital chain between various devices using their Bluetooth and Wifi connections, in essence creating a small network where each person using the app can be used to "hop" the message to the recipient. The drawback is of course range: the sender and receiver need to be linked by a network of these devices, with each device having a range of around 100m. The more people that use it, the more effective it becomes.

# PERSONAL SECURITY

Keeping your personal information safe and out of the hands of hackers is just as important as keeping your devices safe.

## A. SHARING OF PERSONAL CONTACT DETAILS

A large part of journalism is building up networks of contacts, and this includes sharing contact details. Experienced journalists will be doing these things anyway, but it is worth repeating regardless.

**Separate personal and work-related contacts.** Don't use your personal phone number or email address to contact sources or communicate related to your work. Maintaining a barrier between your work and personal communication means you're not inadvertently sharing communication methods that can be used to get additional information on you.

**Keep separate devices.** Ideally, you'd want a separation between your work and personal devices as well. Having a work-only phone that you can use to record interviews or communicate with sources means attempts to compromise your sources won't also compromise your personal contacts too.

## B. LOCKING DOWN PERSONAL ACCOUNTS

Every now and then you might be in a position where your reporting attracts (or might attract) the wrong kind of attention. In cases like these, it is often useful to pre-emptively lock down your social media accounts until the worst kind of attention subsides.

The unfortunate reality is that, short of dropping off the grid and removing yourself from society entirely, there is no way to prevent you from being doxxed. The aim is to minimise the impact when it does happen, and to leave as little information that can be used against you as possible.

**Manage your privacy settings.** Social media platforms have various options to limit the amount of information you share online. It is important to be proactive about your privacy - once privacy has been lost, it is near impossible to claw it back. For example, limiting your posts to "friends only" on Facebook for personal posts will prevent others from seeing what is happening in your personal life. Limiting who follows you, who responds to your posts or who can see your profile images can all be done on the platforms pre-emptively.

**Curate your audience.** In addition to managing your privacy settings, you can and should curate your audience. While this is easier on platforms with bidirectional relationships (think Facebook friends, as opposed to followers on Instagram) it is incumbent on you as a user to curate your audience. Posting personal information to a closed group of friends and family is preferable than posting it in public where you have no control over who sees it.

**Locking it down.** If you expect severe threats or backlash, consider shutting down or deactivating your personal social media accounts for a while. Anyone trying to obtain personal information on you might become frustrated at the lack of personal information out there and abandon the attempt. Deactivation on most social media platforms is quick and reversible.

● Doxx yourself. Doxxing yourself frequently gives you an indication of how much of your personal information is out there. Treat yourself like an investigation and perform searches using your phone numbers, email addresses and physical addresses, reverse image search your profile images and put yourself in the shoes of a would-be doxxer. Knowing what is out there, and how easy it is to find, will let you know what you need to remedy before being doxxed by someone undesirable. In order to mitigate the impact of doxing the main step is to make sure that you minimize the personal information you share on online platforms.

## SUPPORT STRUCTURES FOR JOURNALISTS

Traditionally, journalism as a profession, has always had institutional support structures that support the journalism community. These support structures have always played a role in supporting the fourth estate role of journalism, and its importance, as a profession in supporting democracy and public opinion formation. These include, international organisations like the International Federation of Journalists, International Consortium of Investigative Journalists (ICIJ), Global Investigative Journalism Network, Freedom House, International Committee for the Protection of Journalists(ICJ) and regional media organisations such as Media Institute of Southern Africa.

### WHAT DO IF YOU ARE UNDER SURVEILLANCE?

A journalist who is subjected to surveillance, or suspect being subjected to such, should notify these international support structures for journalists. They are very instrumental at documenting such cases, making them known through existing networks, and exposing blatant abuse of surveillance especially by state and quasi-state actors. A surveilled journalist, should also inform local organizations within their countries who work in conjunction with these global organizations. In Southern Africa, there is a trend that every country has an editors' forum, or such organizations for local journalists who can raise the issue with the authorities. Raising the issue and making it public often scares away culprits from taking more tragic action like assassinating a journalist once their cover is blown. Also, most of the global journalism organizations where are very influential such that they can exert influence and policy shifts on states, or in the least, a lull in surveillance activities.

It is also important for journalists to weigh the option of judicial intervention. Usually the courts shy away from adjudicating on speculative cases, but once a journalist establishes the existence of surveillance, a judicial review of such action is often route that can yield the desirable results of fending off the state from journalism work.

### THE ROLE OF NEWSROOMS

When a journalist is or believes they are under surveillance they should as a first port of call inform newsroom management, who have a responsibility to protect their journalists.

Taking actions such as changing electronic gadgets, changing email addresses, deleting old emails to avoid fishing of old data, changing passwords etc. can mitigate some of the surveillance tactics. Newsroom management can assist further by helping in the purchase of new and more secure devices, raising the issue with the alleged perpetrators of surveillance.

At institutional level, newsroom management can engage the alleged perpetrators and register their awareness of the matter.

## PROTECTION OF SOURCES

### What kind of voice recorders must journalists use?

Journalists can be using their mobile phones for voice recording and in addition use the Tella App (<https://tella-app.org/>) which then encrypts and protects all documentation and audio recordings.

### Are WhatsApp voice messages secure?

These are secure as they are being transmitted over an end-to-end encrypted connection. The problem comes when the receiver of the message has poor security practices with their device which can then expose these messages to the wrong hands.

### What about Signal, Telegram, Zoom, Teams etc?

Please refer to Protecting Your Data below for these answers; Signal Messenger can also be used to

take pics and blur the faces of sources too; or one can also use ObscuraCam (<https://guardianproject.info/apps/obscuracam/>) to anonymize their pictures.

### What is PGP (Pretty Good Privacy) encryption and how can that protect journalists?

When journalists are subjected to surveillance, their sources are also at risk. A cardinal practice of journalism is the protection of sources. Journalists should never at any govern time, jeopardise the safety of their sources. Here are a few tips for journalists when they are subjected to surveillance, or when they suspect that they are being surveilled.

## IF YOU SUSPECT YOU ARE UNDER SURVEILLANCE – YOU SHOULD:

(a). Immediately inform your sources about your suspicion so that they take protective action as well. If your sources are whistle-blowers, you may endanger their lives once they are discovered. It is important to shield them from this danger by letting them know. Vindictive regimes can 'contact- tracing' your sources and eliminate them.



(b). Immediately delete any metadata about your sources that you might have saved on your gadgets. Here are the steps you can take to delete email address of a 'sensitive' news source when your privacy is compromised by surveillance:

1. Click the People option in the navigation bar in the bottom-left section of the screen.
2. Find and select the contact you want to delete.
3. Click the Delete option in the Ribbon, or right-click the user and select Delete from the drop-down menu.

Investigative journalists should take care for a number of reasons. Doing investigative journalism means dealing with a number of sources. There are 'embedded sources'. These are new sources who are within the system, providing leaks and other documents. They are long-term sources that will be used for a number of stories.

## TOP TIPS TO PROTECT YOUR SOURCES

1. Do not save their numbers, their emails and any other metadata of your sources on your devices.
2. When receiving documents from your sources avoid scanning, sending jpeg pictures or any electronic transfer of the documents. They may be captured in the process of transmission. Find safe spaces to physically receive the documents. An abandoned mill, a hidden rail line, a dusty outskirts outside town. When you receive such documents, do not be overwhelmed by the urge to do back -up copies in town. This could lead to a paper trail which can be traced back to you or your source.
3. To minimize an electronic paper trail that can be used by surveillers against you, avoid using public internet service providers (ISPs). Remember in some countries, security regulations can be used by authorities to ask ISPs to turn over your browsing history.
4. Rather use the incognito browsing mode on many browsers. Incognito mode helps in protecting your browsing history. Your browsing history is trail that can be used by surveillers against you. By checking your browsing history, they know which stories you are chasing and who you might possibly want to talk to. Here are the guidelines you can follow to browse in incognito mode:

- On your Android phone or tablet, open the Chrome app. 
- At the top right, tap Switch tabs. On the right, you'll see your open Incognito tabs.
- At the top right of your Incognito tabs, tap Close. 

5. Governments or other powerful people can adopt desperate measure like illegal search and seizure on roadblocks. Do not carry sensitive documents in your car. Do not keep them at your house as well, nor at work.



### **Safe houses:**

When surveillance becomes so banal and violent, it is important to move the affected journalist(s) into safe houses. This is useful because surveillance can be weaponized by agency to traumatize even the journalists' family. In the worst case scenario, safe houses safeguards the journalist, and keep their families away from exposure to the occupational hazards of their family members.

# DIGITAL HYGIENE BEST PRACTICES

Digital hygiene is similar to personal hygiene, it refers to your digital habits rather than your personal grooming habits. Digital hygiene is our crucial first line of defence against new and evolving digital threats, such as malicious emails, social engineering, phishing, cyber harassment, hacking accounts and devices & the theft of private data. In most instances you are the main culprit. Most hacks occur because passwords or critical information has been shared by you. By improving your digital hygiene, you'll be better protected against cyber threats and possible digital surveillance.

**Know your device:** there is value in knowing your device be it a laptop, mobile phone, or camera. Things to take note of are the make, model, software installed and hardware specifications; knowing this enables you to better understand what you want and need to protect.

**Virus Protection:** does your device have an antivirus software? An antivirus software helps protect your computer from virus attacks which can corrupt your documents or harm your computer. A comprehensive comparison of different antivirus software can be found at [www.av-test.org](http://www.av-test.org).

**Enable Firewall:** a firewall monitors and checks all incoming and outgoing traffic on your device. Make sure that it is always on/enabled as it also assists in flagging suspicious connection requests and/or traffic.

**Software Updates:** your devices should be always up-to-date in terms of their software; updates help patch up known vulnerabilities found by the software provider and also enhance the performance of the software.

**User Profiles:** if you are sharing a device make sure that each user has a different user profile they use to log in. Having separate profiles which are all password protected enables the separation of user files and settings.

**Lock Screen:** make sure that your device is locked with a strong password and you do not share this password with anyone.

## HOW TO AVOID PHISHING ATTACKS?

Passwords, multifactor authentication, and encryption will successfully increase the security of email communications. This protection drives adversaries to attempt to use other methods to bypass the security in place. One method used by these attackers is called phishing. In phishing attacks, the attacker uses communication channels (email, IM, SMS) to get you to unwittingly reveal your credentials (username, passwords, birth date, IDs etc) so they can gain access to your online accounts. Malicious links are usually embedded in the messages to get you to click them, redirecting you to websites where you type in your credentials.



# WHAT CAN YOU DO ABOUT PHISHING?

## Look out for:

1. **Typos and bad grammar, JDLR:** spelling mistakes and logos that just do not look right;
2. **URLs (web addresses) that are not connected to the service:** an email from Netflix should have a redirect link to the Netflix service. When in doubt, just navigate to the website yourself, rather than using the link in an email;
3. **Unsolicited attachments:** sometimes phishing emails come with an attachment to get you to download malware. Open all unsolicited attachments in a cloud drive such as Google drive to avoid downloading it to your device;
4. **Social pressure:** Attackers do not want you to think about it too much, so they will send urgent-sounding emails to get you to click immediately.

## ADDITIONAL ONLINE SECURITY MEASURES

While using encrypted platforms to communicate and browse the internet secures these activities, there is still some vulnerability as the Internet Service Providers (ISP) as well as the websites that you visit can still view and store your personal data. The companies that own the websites you visit can store metadata (data about data) about you. To enhance security from these companies and ISPs, one can use the following methods:

- **Using privacy respecting browsers:** your browser is your portal to the internet. A secure browser that protects privacy is a critical tool for staying safe online. Many browsers today are being used as data collection tools for advertising companies using privacy-abusing business models. Selecting the best secure browser all comes down to identifying the best fit for your unique needs. Since this is a personal decision with subjective criteria, a list is provided below of currently well rated private and secure browsers, along with links to further investigate features:

1. **Brave**  
<https://brave.com/privacy-features/>
2. **Mozilla FireFox**  
<https://restoreprivacy.com/firefox-privacy/>
3. **Tor Browser**  
<https://www.torproject.org/projects/torbrowser.html.en>
4. **Ungoogled Chromium**  
<https://github.com/Eloston/ungoogled-chromium>

- **Add-ons to reduce ad content tracking:** These are small applications that can be installed on your web browser. They help to prevent malware, block, and erase your activity and trackers that may be installed on browsers when one visits a website. Trackers and cookies use personal information to tailor advertisements based on your online activity.

### Recommended add-ons:

- **PrivacyBadger** (<https://privacybadger.org/>)
- **DisconnectMe** (<https://www.disconnect.me/>)
- **uBlockOrigin** (<https://ublockorigin.com/>)

# PROTECTING YOUR DATA

Data protection can be implemented at different states of data: Data-in-transit & Data-at-rest. To protect these data, a method called encryption is used. Encryption is a technique of scrambling normal, readable text to unreadable text.

**Data in transit** is any data or information moving from point A to B, that is, email communications, internet use, instant messages, and online video conferencing. Whilst data is in motion, it is vulnerable to attacks and tampering if unprotected. Think of this like sending a postcard in the mail. Anyone can read the messages while in transit.

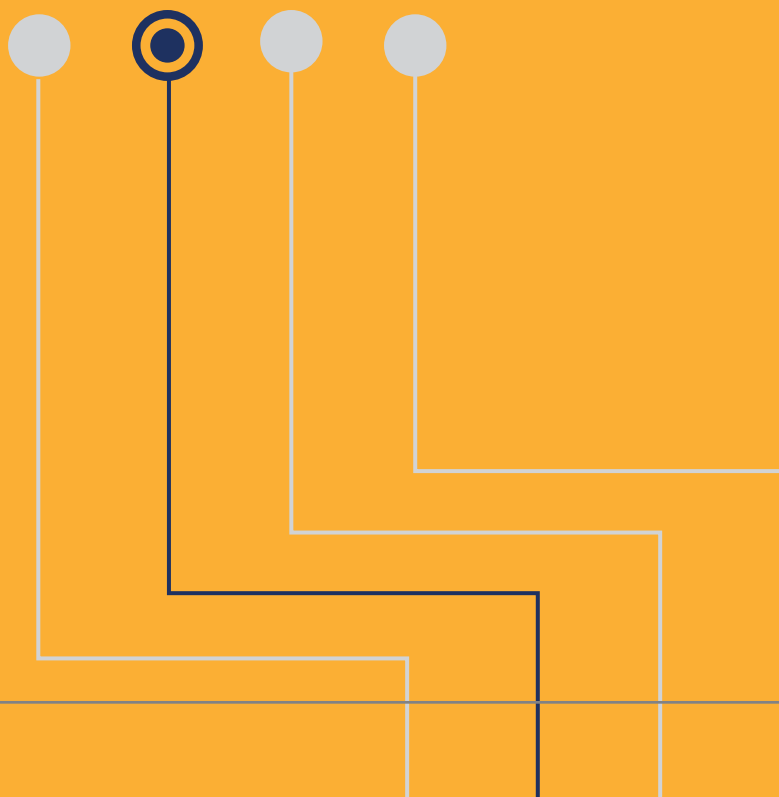
## PROTECTING YOUR DATA IN TRANSIT

**Email encryption:** Use more secure email platforms such as **ProtonMail** (<https://protonmail.com/>), **Tutanota** (<https://tutanota.com/>) and **Thunderbird** (<https://www.thunderbird.net/en-US/>) email clients which enforce encryption.

**Website encryption:** Always try to visit websites that have HTTPS protocol in use. These can be identified by a green locked padlock in the address bar. To make sure that all the websites you visit are HTTPS enabled, one can install an addon in your chosen browser (Google Chrome, Firefox, Edge) called HTTPS Everywhere (<https://www.eff.org/https-everywhere>)

**Instant Messaging:** Use more secure platforms such as Signal Messenger or Wire Private Messenger that have verifiable end-to-end encryption to secure communications and more enhanced features like user-defined disappearing messages, screenshot disabling, customised username etc.

**Video conferencing:** Use platforms such as **JitsiMeet** (<https://meet.jit.si/>), **BigBlueButton** (<https://bigbluebutton.org/>) that have encryption built in and are more privacy respecting.



# ADVOCACY OPPORTUNITIES

There are number of advocacy opportunities that are still available to journalists in the region to fend off surveillance. These include the following:

**Working with SCOs to set an agenda.** CSOs are active in many countries. There are opportunities for productive collaboration between the media and CSOs in the fight against illegal, and non-transparent surveillance. The media, for instance, can use their power to set a public agenda on surveillance and put the matter on the limelight, while COSs use their infrastructures and power accumulated over time, to advocate for reform. CSOs can influence surveillance policy -making. Furthermore, they build new links with these global organisations. New links facilitate a broad dialogue and exchange of ideas on how to actively resist unfettered and murky surveillance practices.

**Exposing surveillance through the power of journalism;** the pen remains the most potent weapon journalists have. By devoting time to write about it and keeping digital surveillance in the limelight, journalists can go a long way in fighting back against surveillance. Institutions that surveil on people thrive on secrecy much of the time. When they are exposed, they tend to lose the capital of their secrecy. Exposure is a very important weapon, hence in the arsenal of journalists. Lastly, journalists and CSOs have an opportunity to advocate the ratification of existing instruments at global and regional levels in which their countries are member states.

**A Just Model Surveillance Law for the SADC region?** Active collaboration could lead to journalists and CSO organizations working together to advocate for a more just and unified model of surveillance for the benefit of all. Such a model law would have the following objectives:

1. Advocate for the creation of an enabling environment for journalism.
2. Protection of journalists' rights to privacy
3. Foster a culture of legal and transparent surveillance in the region
4. Ensure surveillance does not target journalists on the basis of their community of practice.
5. Ensure that surveillance regulation in the region adhere to global standards as we outlined above, and that it reflects the common practice of targeted, time-framed and justifiable surveillance.
6. A model law that gives CSOs and journalists the power and opportunity to litigate.

# ADDITIONAL RESOURCES AND TRAINING OPPORTUNITIES

## RESOURCES

- Frontline Defenders | Security-in-a-box | Tools and Tactics for Digital Security  
<https://securityinabox.org/en/>
- Freedom of the Press Foundation | Guides and Training  
<https://freedom.press/training/>  
<https://freedom.press/anti-phishing-and-email-hygiene>
- Surveillance Self-Defense | A project of the Electronic Frontier Foundation  
<https://ssd EFF.org/>  
<https://www EFF.org/deeplinks/2020/06/digital-security-advice-journalists-covering-protests-against-police-killings>
- Helpdesk.rsrf.org | A project of Reporters Without Borders  
<https://helpdesk.rsrf.org/digital-security-guide/>
- Committee to Protect Journalists (CPJ) | Digital Safety Kit for Journalists  
<https://cpj.org/2019/07/digital-safety-kit-journalists/>
- International Journalists' Network | Digital Security do's and don'ts for journalists  
<https://ijnnet.org/en/story/digital-security-dos-and-donts-journalists>
- Browser security - Data detox digest (browser edition)  
[https://cdn.ttc.io/s/datadetoxkit.org/essentials/ddk-digest\\_browser\\_EN.pdf](https://cdn.ttc.io/s/datadetoxkit.org/essentials/ddk-digest_browser_EN.pdf)

## TRAINING OPPORTUNITIES

- Digital Society of Africa | [www.digitalsociety.africa](http://www.digitalsociety.africa) | [info@digitalsociety.africa](mailto:info@digitalsociety.africa)
- Defend Defenders | [www.defenddefenders.org](http://www.defenddefenders.org) | [protection@defenddefenders.org](mailto:protection@defenddefenders.org)
- Frontline Defenders | [www.frontlinedefenders.org](http://www.frontlinedefenders.org) | [info@frontlinedefenders.org](mailto:info@frontlinedefenders.org)
- Southern Defenders | [www.southernafricadefenders.africa](http://www.southernafricadefenders.africa) | [info@southernafricadefenders.africa](mailto:info@southernafricadefenders.africa)

# CONCLUSION

Although efforts in the region are being directed to training on digital security and journalism surveillance, currently the region does not have capacity and resources to support journalists in these areas and must rely on international institutions to provide support and training. This toolkit is a step towards identifying and filling these gaps. Looking ahead there is a need for a coordinated approach to develop a clear intervention strategy among media institutions and civil society. One such example could be the lack of legal recourses available to journalists when facing surveillance. Currently assistance is provided on a case-by-case basis depending on availability of resources.

## CONNECT WITH US:



ARISAProgram



@ARISA\_SADC



Internews in South Africa



@InternewsSA





ARISA is a five-year USAID funded human rights program being undertaken by a consortium of four partners - Freedom House, ABA Rule of Law Initiative, Pact and Internews. ARISA works in select Southern Africa Development Community (SADC) countries to improve the recognition, awareness, and enforcement of human rights in the region, including protecting the region's most vulnerable and marginalized groups.

## CONSORTIUM PARTNERS:

