



REUTERS/ Siphwe Sibeko

UNDERSTANDING THE LAWS ON JOURNALISTIC SOURCES IN SOUTH AFRICA

INTRODUCTION

This Guide provides journalists with a practical understanding of the legal framework on news sources in South Africa. This awareness will empower journalists to understand their legal rights and obligations and continue to report on issues of vital public interest. The Guide assesses the recognition of news sources in law, the protection of news sources as well as search and seizure relating to journalists' gadgets and information.

1. WHO IS DEFINED AS A JOURNALISTIC SOURCE?

There is no legislation that specifically regulates journalistic sources. Courts have considered the issue of journalistic privilege and maintaining confidentiality of sources but have never provided a clear definition of a “journalistic source”. However, it can be inferred that journalistic sources are individuals who have knowledge pertinent to a story. Sources also include documents that contain relevant information for journalistic work.

2. WHICH LAW PROTECTS JOURNALISTIC SOURCES?

The [Criminal Procedure Act](#) governs the police’s powers of search and seizure. The [Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002](#) (RICA) covers the interception of journalists’ communications by the police. In 2021, the [Constitutional Court](#) declared RICA unconstitutional for failure to provide adequate safeguards to protect the right to privacy regarding access to courts, freedom of expression and media, and legal privileges. In particular, RICA did not address proper process for the surveillance of journalists - there was no requirement to notify a person that they had been a subject of surveillance. The Constitutional Court suspended the order of invalidity for a period of three years to allow Parliament time to cure the various constitutional defects identified. This means that the law is still in effect until the suspended period lapses.

However, the declaration of unconstitutionality for the lack of post-surveillance notification was not suspended. As such, post-surveillance notification must be issued by the law enforcement officer to the subject, when the subject is a lawyer or a journalist. The person applying for the surveillance warrant must also disclose to the designated judge if the subject is a lawyer or a journalist.

When it comes to data protection and the collection and use of personal information about an individual, the [Protection of Personal Information Act 4 of 2013](#) (POPIA) applies. However, POPIA does not apply to the processing of personal information solely for the purpose of journalistic expression to safeguard public interest,

while balancing the right to privacy and the right to freedom of expression. POPIA further notes that, where a journalist processes personal information for journalistic purposes and is subject to a code of ethics that provides adequate safeguards for the protection of personal information, such code will apply to the processing concerned instead of POPIA. For example, the [Press Code of Ethics and Conduct for South African Print and Online Media](#) (the Press Code) deals with processing of personal information.

In addition, the [Promotion of Access to Information Act 2 of 2000](#) promotes the right of access to information held by the State and any information held by another person that is required for the exercise or protection of any rights. A journalist may be required to disclose a record of confidential information if that record is required for the protection or exercise of another person's rights. The journalist would have to provide the record if the person requesting it complies with the procedural steps set out in the Act, and if the disclosure does not constitute the exclusions (for example, where the disclosure would involve the unreasonable disclosure of personal information about a third party). Sources also include documents that contain relevant information for journalistic work.

3. DOES THE LAW PROTECT ME FROM REVEALING MY SOURCES? WHEN MIGHT I BE REQUIRED TO REVEAL A SOURCE?

Journalists can, in certain instances, be required to disclose their sources of information, particularly if ordered to do so by a Court. The [Criminal Procedure Act](#) provides that a Judge or Magistrate may, upon the request of South Africa's National Prosecuting Authority (NPA), order any person who may have information about an alleged offence to appear before a Court to provide information. Should such person refuse or fail to provide the information required, they may be sentenced to a period of imprisonment of up to two years or, in the case of information related to "serious" matters, up to five years.

This mechanism, under the [Criminal Procedure Act](#), has in the past been used to require journalists and media organisations to reveal the identities of confidential sources. However, a person who refuses to give information under subpoena (an order to appear in court) may not be jailed unless the Court is of the opinion that the information sought is necessary for the administration of justice or the maintenance of law and order. Any person subpoenaed, including a journalist, may escape imprisonment for refusal to disclose a confidential source by raising a "just excuse".

In civil proceedings, where a person is subpoenaed to give evidence in a civil trial and refuses to answer questions put to him or her, the Court may commit the person to prison (the [Superior Courts Act, section 35 \(3\)](#)). However, imprisonment can be avoided if a journalist or subpoenaed witness raises a "reasonable excuse".

A "just excuse" or "reasonable excuse" would depend on the circumstances of the case. In [S v Cornelissen](#) the court held that a journalist's refusal to disclose their source due to confidentiality will not necessarily constitute a just excuse. Courts have acknowledged a "just excuse" for a journalist not testifying where the police have not explored other possible witnesses who could provide the same evidence as the journalist.

The context in which a journalist's source provides information is a central consideration to whether disclosure should be permitted or prohibited. If the source acted out of civic duty in exposing corruption, this may warrant the protection of the source's identity. On the other hand, confidentiality may be more easily overridden where the source provided information in relation to a crime for which disclosure would be required for effective investigation and prosecution.

4. WHAT RIGHTS DOES A SOURCE HAVE?

A journalist's source does not enjoy any special protection under South African law and can rely only upon the same protections offered to ordinary citizens under the Constitution and other laws.

Many journalists are members of organisations that are bound by some form of journalism ethics code. The [Press Code](#) is such an example. The Press Code applies to the content published by all its members and has sections dedicated to:

- a. the gathering and reporting of news;
- b. independence and conflicts of interest;
- c. privacy, dignity and reputation;
- d. protection of personal information; and
- e. confidential and anonymous sources.

The Code specifically states that the media shall protect confidential sources of information and not publish information that constitutes a breach of confidence.

A journalist's source also enjoys protection of their right to privacy. The right to privacy in South Africa is protected by the common law as well as section 14 of the [Constitution](#). The right to privacy is not, however, absolute and may be limited where it is reasonable and justifiable to do so by the Constitution. This may include where a person is compelled to provide evidence in a Court of law.

5. WHAT SHOULD I BE WARY OF WHEN DEALING WITH A JOURNALISTIC SOURCE?

There are no specific laws in South Africa that govern the relationship between a journalist and their sources. Journalists, however, generally abide by some form of code of ethics or code of conduct, such as the Press Code, which states that the media shall:

- a. identify themselves as media, unless public interest or their safety dictates otherwise;
- b. protect confidential sources of information; and
- c. not publish information that constitutes a breach of confidence, unless the public interest dictates otherwise.

The Code applies to content published by its members. These include the South African National Editors' Forum, the Forum of Community Journalists, the Association of Independent Publishers, and the Interactive Advertising Bureau.

6. CAN I FACE LEGAL ACTION IN MY INTERACTIONS WITH A SOURCE, AND IN WHAT CIRCUMSTANCES?

While the [Press Code](#) is a form of self-regulation, it is enforced by the [Press Council](#), the Press Ombudsman and the South African Press Appeals Panel. However, there are no penalties expressly stated in the Press Code relating to the breach of its provisions.

It is conceivable that a source may have a claim for damages against a journalist or media outlet who disclosed that source's identity contrary to an agreement of confidentiality and the source suffered financial loss as a result.

7. IN WHAT INSTANCES MAY I RECORD A SOURCE?

There is a general prohibition on recording conversations under [RICA](#). [RICA](#) also prohibits accessing the content of a communication through "bugging" offices, listening in on telephone conversations, and accessing emails, data or text.

There are, however, exceptions to this general prohibition, and recording conversations will be lawful where:

- a. the person recording is party to the conversation; or
- b. prior written consent has been received by one of the parties to the communication.

Journalists may therefore lawfully record conversations (even without the consent of other parties) if they are a party to the conversation (for example, if they are interviewing someone).



REUTERS/ Siphwe Sibeko

8. CAN THE POLICE CONFISCATE MY DOCUMENTS/ GADGETS FOR INVESTIGATION? IN WHAT INSTANCES CAN THEY DO SO?

The golden rule when it comes to search and seizures by the police is that a valid search warrant must be obtained before a search and seizure is carried out. A search warrant must be obtained by way of an order of Court. A warrant authorises the police to enter premises, conduct a search, and seize any items relevant to the specific investigation.

The items that can be seized during a search and seizure are listed in the [Criminal Procedure Act](#). They include articles concerned with, or reasonably believed to be intended to be used in, the commission of an offence. They also include articles that may be evidence of the commission or suspected commission of an offence.

The legislation uses the term “article” which is defined as physical things or documents, and therefore does not include the seizure of electronic information systems, electronic documents and data messages. This would only be permitted in cases where there is a cyber inspector appointed for the investigation who has been duly authorised to do so.

The only item that can be exempt from a search and seizure is a document or communication that is privileged. The current position in South African law is that there is no legislation providing privilege over communication between journalists and their sources. In other words, there is no special blanket of legal protection afforded to journalists in this respect beyond that which is afforded to the ordinary South African citizen or resident.



SHUTTERSTOCK/ Jeff Daniels

9. CAN THE POLICE CONFISCATE MY DOCUMENTS ONLINE? CAN THE POLICE TAP MY COMMUNICATIONS WITH SOURCES, INCLUDING VIA SECURE/ENCRYPTED PLATFORMS?

The authority of the police to confiscate documents online is limited to what has been stipulated in the search warrant. As discussed in 8 above, the power to confiscate electronic documents is not within the scope of an ordinary search and seizure under the Criminal Procedure Act and would require the assistance of a cyber inspector.

The role and powers of the cyber inspector are set out in the [Electronic Communications and Transactions Act \(ECTA\)](#). According to ECTA, a cyber inspector must obtain a warrant from a judicial officer that will detail the scope of their powers in terms of what they can search and seize. This warrant must be issued by a Magistrate or Judge. The warrant expires after one month from the date it was issued. Before inspection, the cyber inspector must produce the warrant and their certificate of appointment to show that they are authorised to conduct or participate in the search and seizure operation.

In addition, the police may seek an order under RICA to have a mobile operator provide records from intercepting someone's telephone line. This is dealt with at page 8.

With regard to encrypted messages, RICA allows the police to apply for a "decryption direction" in order to compel an individual or an encryption service provider to provide the decryption key necessary to review encrypted messages.

10. IN WHAT INSTANCES CAN LAW ENFORCEMENT INTERCEPT MY COMMUNICATION ONLINE?

Monitoring of a journalist's communication online is governed by [RICA](#). Law enforcement agencies must apply to what is commonly known as a "RICA Judge" (who is a retired judge designated to reviews concerning [RICA](#)) for permission to intercept the online communication of an individual suspected of criminal or terrorist activities. According to [RICA](#), lawful interception is only allowed in cases where there is a reasonable ground to believe that a serious criminal offence such as high treason will be committed or where the information concerns an actual threat to public health, safety or national security.

In the event that the RICA Judge is convinced of the need to intercept the communication, they will issue an order termed as an "interception direction", which will compel the relevant mobile operator to comply and assist the law enforcement agency with gathering the intelligence sought.

RICA was declared unconstitutional by the [Constitutional Court](#). However, the Court's order of invalidity has been suspended for a period of 3 years so that Parliament can make the relevant amendments.

[RICA](#) was declared unconstitutional due to a number of defects including that the application to the RICA Judge is done on an *ex parte* basis, which means that the person they are intending to place under surveillance will not be a party to the process and, accordingly, will have no opportunity to object to the order being granted. RICA also does not provide any process for this intended person to be notified of the interception, even after the surveillance has been concluded.



As a result of this case, the [Constitutional Court](#) granted interim relief so that people must be notified if they had been under surveillance. The court extended protection to information shared with journalists in confidence. In terms of this interim relief, the State must disclose to the designated RICA Judge the fact that the intended subject of interception is a journalist in the application for interception.

11. WHAT PROCEDURE MUST THE POLICE FOLLOW TO INTERCEPT MY COMMUNICATION OR CONFISCATE MY DOCUMENTS?

Journalistic documents are not privileged by virtue of being documents obtained or held by a journalist. This means they would have to be produced in the event of a subpoena or where a search warrant orders their production. The scope of the police's power to search and seize will be set out in a valid search warrant, which details the parameters of the search and what can be seized. Police are required to act on the warrant during the day unless they have obtained a special authorisation to execute it during the night.

Notably, the powers of search and seizure provided in the [Criminal Procedure Act](#) are not applicable to electronic documents so these would be exempt from search and seizure, unless the warrant requests the presence of a cyber inspector.

Electronic documents are not exempt from being produced by way of a subpoena. The [Criminal Procedure Act](#) makes provision for the Court, the police, the prosecutor or an accused to compel the attendance of any person to give evidence or to produce any book, paper or document in criminal proceedings.

12. WHAT PROCEDURE MUST THE POLICE FOLLOW TO INTERCEPT MY COMMUNICATION OR CONFISCATE MY DOCUMENTS?

The police must obtain a search warrant before conducting a search and seizure operation to confiscate documents. This warrant is obtained from a Magistrate, Judge or Justice of the Peace (sections 21 and 25 of the [Criminal Procedure Act](#)).

In order to intercept a journalist's communications, the relevant law enforcement agency will have to bring an application to a RICA Judge under [RICA](#) and show why an order permitting interception should be granted in its favour. The law enforcement agency making the application is now required to disclose that the subject of the interception request is a journalist. It is only when that order is granted by the RICA Judge that a law enforcement agency can lawfully monitor a person's communication lines and receive a report from the interception.

A photograph showing silhouettes of people at an event against a blue sky. In the foreground, a person's hand is holding a microphone. In the background, another person is holding a camera. The scene is captured from a low angle, looking up at the participants.

REUTERS/ Ueslei Marcelino

ABOUT US

The Thomson Reuters Foundation is the corporate foundation of Thomson Reuters, the global news and information services company. The Foundation works to advance media freedom, raise awareness of human rights issues, and foster more inclusive economies. Through news, media development, free legal assistance, and convening initiatives, the Foundation combines its unique services to drive systemic change. Its mission is to inspire collective leadership, empowering people to shape free, fair, and informed societies. TrustLaw is the Thomson Reuters Foundation's global pro bono legal programme, connecting high-impact NGOs and social enterprises working to create social and environmental change with the best law firms and corporate legal teams to provide them with free legal assistance in order to produce ground-breaking legal research and offer innovative training courses worldwide.

ACKNOWLEDGEMENTS & DISCLAIMER

The Thomson Reuters Foundation would like to acknowledge and extend their gratitude to the legal team at Bowmans South Africa, who contributed their time and expertise on a pro bono basis to make this Guide possible. This Guide is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances. We intend the Guide's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. Bowmans South Africa and the Thomson Reuters Foundation accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this Guide or any inaccuracies herein.