

# RESPONSIBLE REPORTING ON



# WHISTLEBLOWING

A GUIDE FOR SOUTH AFRICAN JOURNALISTS, EDITORS AND  
NEWSROOMS PRODUCED BY THE WITS CENTRE FOR JOURNALISM

## Responsible Reporting on Whistleblowing

TEXT: Nechama Brodie and Mandy Wiener

DESIGN: Adèle Sherlock

With thanks to Charl du Plessis for legal input and guidance

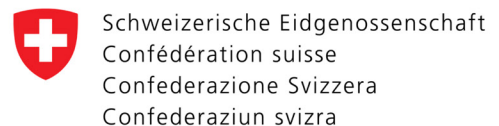
© Wits Centre for Journalism, 2024

Produced by the Wits Centre for Journalism in partnership with the GIZ Transparency, Integrity and Accountability Programme (TIP) in South Africa and supported by the South African National Editors' Forum (Sanef).

Published under CC BY-NC 4.0 <https://creativecommons.org/licenses/by-nc/4.0/>

This text is free to use and distribute, and may be freely adapted, provided it is not for commercial purposes. Credit must be given to the original author/s.

The authors would like to thank the following individuals for their assistance in preparing this guidebook: Dr Liezl Groenewald; Stefaans Brummer; Dr Ugljesa Radulovic; Cynthia Stimpel; Gareth Newham; Cherese Thakur; Joanna Atkinson; Thobile Madonsela; Reggy Moalusi; Hopewell Radebe; Dzudzie Netshisaulu.



**State Secretariat for Economic Affairs SECO**



# CONTENTS

## RESPONSIBLE REPORTING ON WHISTLEBLOWING

<b>ABOUT THIS HANDBOOK</b>	2
<hr/>	
<b>Section One: Defining ‘whistleblowing’</b>	
What is a whistleblower?	3
What does whistleblowing mean in law?	7
<hr/>	
<b>Case Study: The Gupta Leaks</b>	19
<hr/>	
<b>Section Two: Recognising whistleblowing</b>	
The whistleblower spectrum	20
Barriers to blowing the whistle	25
<hr/>	
<b>Section Three: Responsible reporting</b>	
Best practices for reporting on whistleblowers	30
Safety and security	35
<hr/>	
What happens next?	43
<hr/>	
<b>Appendixes:</b>	
Resources	45
References	46
<hr/>	

# ABOUT THIS HANDBOOK

This book is designed for journalists, editors, and anyone working in a newsroom. It provides an introduction and guide to responsible and ethical practices for reporting on stories that involve information or disclosures that might be described as ‘whistleblowing’ (see the next section for some definitions of this term). While most whistleblowing guides focus on supporting and protecting potentially vulnerable informants, this handbook considers the role of journalism in not only protecting its sources, but also safeguarding ethical, accountable and transparent media practices, including verifying the credibility and integrity of information provided by such disclosures, and doing so in a responsible manner.

Although this guide is developed specifically for South African media, many of the processes we recommend can be followed by journalists anywhere in the world, and we believe it will help reporters and editors to systematically research and fact-check information provided by confidential sources – without unnecessarily endangering the participants, and without compromising on journalistic principles.

This book is also intended as a training guide that can be used by editors and other newsroom managers, to teach or share ideas around key concepts, and recommend best practices when it comes to reporting on whistleblowing. At the back of this book, we have provided a series of exercises that can be used for this purpose.

The content in this book was created through consultations with a number of experts, from whistleblowers and journalists to support agencies, research institutions and legal specialists, to produce a framework for journalistic best practices. However, it is important to emphasise that the advice and information in this book does not constitute legal advice. Throughout this guidebook we have provided information about additional resources including civil society organisations devoted to combatting corruption, and assisting people with disclosures that are made in the public interest. Journalists, editors and sources (including whistleblowers) should always consult with specialist organisations and seek legal advice and support where this is necessary.

# whistleblower or whistle-blower (noun)

a person who reveals something covert  
or who informs against another

## WHAT IS A WHISTLEBLOWER?

When we call someone a whistleblower, we usually mean they are an **informant**, or an **informer** – someone who has information that is in the public interest, usually about a wrongdoing (an older meaning would be someone literally playing a whistle, like in a marching band). The origin of the contemporary use of the word comes from the late 1800s, when policemen would blow a whistle to draw attention to a crime, and referees at sports matches would blow a whistle to enforce the rules of the game in play. Blowing the whistle quickly became used as a metaphor for calling attention to something, usually unlawful or irregular activity that had been hidden or kept secret.

Today, many countries have introduced laws that protect employees who ‘blow the whistle’ on their employers, revealing corrupt or criminal or improper practices in the workplace, but (at least from a news reporting and even a community perspective) this is only one type of whistleblowing. It’s important for reporters to keep these differences and variations in mind from the start. In some contexts, calling a source a ‘whistleblower’ might imply a legal definition, or a legal finding; but this is not always the case, particularly when a source approaches a journalist with information before any legal charges or processes have begun.



This handbook will help reporters and editors to research and fact-check information provided by confidential sources – without unnecessarily endangering the participants, or compromising on journalistic principles.

Media workers should always remember that what a journalist or editor thinks of as a 'whistleblower', and what the law considers whistleblowing might be two very different things; and disclosing a 'whistleblowing' story in the press might have legal as well as other consequences for the source or informant! On the next page, we provide a starting point to help you (and your source) think about the best ways to report this kind of information using the media.

## WHAT'S IN A NAME?

The term 'whistleblower' has a number of (non-legal) synonyms, which often depend on how you view the role or character of the person 'blowing the whistle' or the information they are providing. Many of these words are not very complimentary – like **snitch, tattle-tale, rat, tell-tale, impimpi**. Reporters should always consciously think about the words that are used in news reports (and not only in the body copy but also in news headlines and blurbs). Try to think of neutral words (like simply calling a person a 'source'), or phrases that describe the context or relevance of the person ('an employee at this institution') without labelling the person as good or bad. Of course, you may not be able to describe the source easily, even in vague terms, if you need to protect or obscure their identity – but in these cases, you can try to refer to the facts (e.g., 'Allegations of R100-million losses at XYZ department') without referring to the person in detail.



Think about the words you want to use to describe your source, and only use 'whistleblower' in the right circumstances, and at the right time. Choose neutral language and avoid using terms that imply the source is a 'good' or 'bad' person. Keep reporting focused on the facts of the case, and not the attributes or character of the source.

## WHISTLEBLOWER OR SOURCE?

***A whistleblower can be thought of as an honest citizen who exposes hard facts or 'eyewitness' evidence of serious wrongdoing, even though it places them at risk of severely detrimental consequences.***



For the purposes of this handbook, when we use the term 'whistleblower' we mean any person or persons disclosing information (which other people might be trying to hide) that potentially exposes wrongdoing, and is in the public interest. Although this broad definition does not directly align with those included under the Protected Disclosure Act (see next page) and other related laws, when it comes to reporting on wrongdoing, corruption, and crime, it is important to acknowledge the role many other citizens play in exposing these actions. The idea of an 'honest' citizen also means, in this context, that they are exposing important information that (to the best of their knowledge) is true – it doesn't mean the whistleblower has to be virtuous in every single aspect of their life.

Some things to consider when meeting a source who claims to have this kind of information (choose all that apply):

- A** Is your source providing information about a current or former employer (including contract workers)?
- B** Is your source providing information about criminal or harmful activities in their community or the place where they live or work?
- C** Has your source tried to report this information or stop the wrongdoing in any other way (for example, reporting it to the police or to the employer)?

If you answered 'A' (and any of the other selections), your source might be covered by the Protected Disclosures Act (see next pages) – this is important as the Act includes very specific legal frameworks and processes for making disclosures, and the media should generally not be the first point of call.



For cases where you have selected 'A', journalists should also be able to select 'C' (it has previously been reported to another agency) before proceeding with a source or story. In terms of the Act, informants making protected disclosures are only allowed to go to the media (without having reported it elsewhere) in very specific circumstances. We explain what this means in more detail in the next few pages.

If you selected 'B', pay close attention to Sections 2 and 3 in this book, which describe some of the risks and harms whistleblowers may be exposed to, and best practices for reporters and newsrooms including keeping both sources and reporters safe.



“ The idea of an ‘honest’ citizen also means, in this context, that they are exposing important information that (to the best of their knowledge) is true – it doesn’t mean the whistleblower has to be virtuous in every single aspect of their life.

# WHAT DOES WHISTLEBLOWING MEAN IN LAW?

More than 170 countries and self-governing territories around the world have adopted legal protections or laws relating to whistleblowers – but the definition of who or what is a whistleblower and how the law/s extend to them can vary greatly.

Most formal laws that specifically name and protect 'whistleblowers' (or protected disclosures) refer to employees who report a wrongdoing by their *employers*, and who need to be protected from retaliation as a result of reporting the wrongdoing. In America for example, the Whistleblower Protection Act (WPA) protects federal (government) employees who disclose information about federal violations of laws, gross mismanagement, wasteful expenditure, abuses of power, and dangers to public health or safety. The Ethics Institute (see our Resources and References sections at the end of this book) describes whistleblowing as 'the disclosure by a person, usually an employee in a government agency or private enterprise, to the public or those in authority, of mismanagement, corruption, illegality, or some wrongdoing'.

Of course, many people who report wrongdoing are not employees, and are not reporting their employers. This makes the term 'whistleblower' difficult to narrow down, as it might mean different things in different regions, countries and contexts, and the 'common' or public meaning might not be exactly the same as the legal meaning. Journalists should keep this in mind when using terms that might have multiple different interpretations. In a White Paper on South African whistleblowers published by the Gordon Institute of Business in 2021 (see References), most respondents defined whistleblowing as simply 'reporting irregularities' by bringing them to the attention of someone in a position of authority.

Legally, there is no broad, universally applicable protection for whistleblowers in South Africa – and the so-called whistleblowing Act (the Public Disclosures

Act or PDA) doesn't even use the term whistleblower, it talks about 'employees or workers' or people that 'assist' employers in carrying on their business (like contractors). That is because it is largely focused on protecting whistleblowers from their own employers (including, of course, cases where that employer is the state).

Journalistic sources aren't necessarily going to be covered by the protection of the PDA just because they're leaking information to a journalist and that's an important thing for journalists to know. We may regard many sources as whistleblowers, as a matter of journalistic best practice, but there are relatively strict legal requirements that have to be met for a source to qualify for protection under the Act when they are speaking to a journalist.

In South Africa, the **Protected Disclosures Act 26 of 2000** (PDA), and the later **Protected Disclosures Amendment Act 5 of 2017** (2017 PDA Amendment), were developed to 'help to deter and detect wrongdoing in the workplace, acting as an early warning mechanism to prevent impropriety and corruption within the public sector,' (Public Service Commission). The original PDA included employees in both the public and private sector (but excluded people such as independent contractors, volunteers and so on), while the 2017 PDA Amendment, among other features, extended the Act to cover former employees, contract/temporary workers, and employees who were deployed to other organisations by their employers. The Amendment also made it possible for these types of employees to break confidentiality, non-disclosure and similar agreements (with their employers) if these obstructed their ability to make protected disclosures. Importantly, the 2017 PDA Amendment also introduced requirements for employers to create formal processes and platforms for the reporting of criminal or irregular conduct in the workplace, and to enforce protective measures supporting people who reported misconduct.



# WHAT IS CONSIDERED A PROTECTED DISCLOSURE?

The Plateforme de Protection des Lanceurs d'Alerte en Afrique or Platform to Protect Whistleblowers in Africa (PPLAAF) says that 'information (including opinions) on the "misconduct" of an employer or colleague is eligible for protection under the PDA. Disclosable misconduct includes criminal offences, failure to comply with legal obligations, miscarriage of justice, endangerment of health and safety, damage to the environment and unfair discrimination.' Disclosures can be made 'in good faith', which is based on a common legal principle that assumes all parties are dealing with each other honestly and not knowingly making false declarations.

In addition to the PDA and PDA Amendment, the Companies Act 71 of 2008 and the Companies Amendment Act of 2011 also make provision for reporting actions or events that might pose a risk or a liability for the company.



What journalists think of as a 'whistleblower' and what the law considers whistleblowing might be two very different things.



In general, a protected disclosure applies to a worker or employee who has information about the behaviour or conduct of an employer or another employee, that shows one or more of the following:

- a: That a criminal offence has been committed, is being committed or is likely to be committed;
- b: That a person has failed, is failing or is likely to fail to comply with any legal obligation to which that person is subject;
- c: That a miscarriage of justice has occurred, is occurring or is likely to occur;
- d: That the health or safety of an individual has been, is being or is likely to be endangered;
- e: That the environment has been, is being or is likely to be damaged;
- f: Unfair discrimination as contemplated in Chapter II of the Employment Equity Act 1998, or the Promotion of Equality and Prevention of Unfair Discrimination Act 2000; or
- g: That any matter referred to in paragraphs (a) to (f) has been, is being or is likely to be deliberately concealed.

(PPLAAF)

The Protected Disclosure Act describes *protected* disclosures because, as PPLAAF explains, they are designed to protect whistleblowers 'from reprisal in the form of "occupational detriment"' which might include losing their job, or being subjected to disciplinary action. The Companies Act also protects employees from civil or criminal or administrative liability that results from a protected disclosure.

To do this, **the Acts provide for compensation for whistleblowers who are mistreated** – which can be up to 24 months' salary for unfair dismissals or unfair labour practices, and additional compensation that can be sought for 'damages suffered'. Because of this, the High Court, the Labour Court and the Commission for Conciliation, Mediation and Arbitration (CCMA) are most commonly used to deal with cases of undue retaliation in the workplace. [Of course, there are no such mechanisms or compensations for people who are not employees!]

For a disclosure to be protected under these regulations, **the information has to be disclosed to or through certain designated parties or authorities.** Ideally, the alleged wrongdoing should be reported to the employer, through a designated reporting platform (if the whistleblower works for the state, then they can report to a Member of Cabinet or of a provincial Executive Council); of course, this can be complicated when it involves disclosing wrongdoing in the workplace, and so several other entities are also designated. These include: the Public Protector, the SA Human Rights Commission, the Commission for Gender Equality, the Cultural, Religious and Linguistic (CRL) Commission, the Public Service Commission, and the Auditor General. A whistleblower can also discuss the information with a legal advisor if they are seeking legal advice.

## MORE ON THE LAW



### **Protected Disclosures Act 26 of 2000**

<https://www.gov.za/documents/acts/protected-disclosures-act-26-2000-07-aug-2000>

### **Protected Disclosures Amendment Act 5 of 2017**

<https://www.gov.za/documents/protected-disclosures-amendment-act-5-2017-english-afrikaans-2-aug-2017-0000>

### **Companies Act 71 of 2008**

<https://www.gov.za/documents/companies-act>

### **Companies Amendment Act 3 of 2011**

<https://www.gov.za/documents/companies-amendment-act-4>

### **Protection from Harassment Act 17 of 2011**

<https://www.gov.za/documents/companies-amendment-act-4>

**You can find copies of Acts and Amendments at [www.gov.za/documents/acts](http://www.gov.za/documents/acts)**



# THE PDA VS JOURNALISM INTERESTS

If we use one of the definitions we provided earlier, we might describe whistleblowing in this context as: 'an honest citizen who exposes hard facts or "eyewitness" evidence of serious wrongdoing, *even though it places them at risk of severely detrimental consequences in their job*' and who has hopefully already tried to remedy or report the wrongdoing but these attempts have been ignored or ineffectual.

In some cases, journalistic interests will to a certain degree overlap with what a whistleblower will need to qualify for protection in terms of the Act. Informally, this is how we might break down some of these descriptions in this case:

**An honest citizen.** In terms of the PDA, a court is going to be looking for a person who acts in good faith, out of a genuine desire to do the 'right thing' for the betterment of society, and who doesn't act for their own personal benefit. In the first volume of the official report on the Commission of Enquiry into State Capture (often referred to as the Zondo Commission), former Chief Justice Raymond Zondo wrote that a whistleblower is a person '*actuated by a sense of duty of the highest order*'.

This does not mean a whistleblower has to be a perfect citizen. Our courts have held that it is somewhat rare for a whistleblower not to be disgruntled in some way and this shouldn't necessarily disqualify them (from being protected). However, an ulterior motive or desire for personal gain makes things more complicated and should be a red flag for journalists in particular.



A court is going to be looking for a person who acts in good faith, out of a genuine desire to do the 'right thing' for the betterment of society, and who doesn't act for their own personal benefit

**Hard facts or 'eyewitness information'.** The PDA is actually not specific on what form information should take but we have included this here because a whistleblower speaking to the media must reasonably believe that the information they're disclosing is substantially true.



From a journalistic perspective, there is somewhat of an overlap here because we should typically also expect this from a source. Most often, for the media, 'reasonable belief' should translate as: hard evidence that backs up a claim. Lawyers and journalists may differ on what constitutes credible evidence – but ideally you should either have direct, relevant documentary evidence or, in certain cases, compelling oral testimony from a credible eyewitness. We discuss these requirements later in this handbook.

**Serious crime or wrongdoing.** The activity that the whistle is being blown about should be exceptionally serious, and a matter of clear and overwhelming public interest. This is relevant both in terms of the PDA requirements and most journalistic needs – but for slightly different reasons.

Journalists and editors should have a well-developed sense of what the law considers to be 'public interest'. You cannot 'blow the whistle' on a celebrity's love life or a private spat. But things also don't need to be of national prominence or involve a major constitutional crisis to qualify as being in the public interest. A batch of emails showing that a councillor of a small town has been asking for and receiving bribes over a long period of time would also be considered serious wrongdoing that is a matter of clear and overwhelming public interest.

Often people try to market themselves as a whistleblower but the information they provide is unremarkable and/or highly selective, and/or requires major speculative conclusions or assumptions. This is usually an indicator of questionable motives (see the next section). Journalists need to be very aware of this, particularly in South Africa, where there are often bitter and acrimonious factional disputes at play.



The things that disclosures should be about, according to the Act, **are contravention of laws or legal duties (including crimes), miscarriages of justice (egregious cases where the justice system has been abused or malfunctioned, roughly), where the health or safety of people is being endangered, where the environment is being harmed, or where unfair discrimination is taking place.** Those, roughly, are also things that the media would regard as being of public interest.

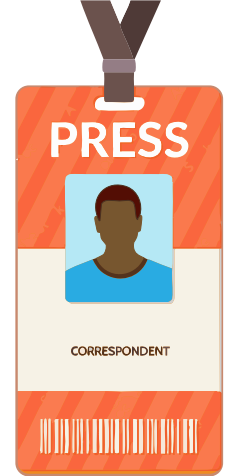
A final thing to take note of is the fact that the law puts a lot of stock on crimes or conduct that is in breach of laws or legal duties. That is a tough thing for journalists, who generally report on such things *before* a court ever reaches that conclusion. What is very important in those kinds of scenarios is that there is a reasonable belief that a crime has been committed or a law has been breached.

In these cases, journalists should consider two important things: what exact law/s or legal obligations have been breached (be specific); and, is there solid evidence that supports the conclusion that a law has been breached? Avoid vague, speculative conclusions or assumptions

**Severely detrimental consequences in their job.** This is more important to the whistleblower but, from a journalistic perspective, it's important to know that the PDA legislation is employment-orientated, although it has been criticised for this. Its entire purpose is to prevent occupational detriment to whistleblowers. Whistleblowers are usually going to be breaching express or implied terms of their employment contract by speaking to the media and face the risk of losing their jobs (or suffering some other occupational detriment) for what they're doing.

The reality is that many whistleblowers end up in a position where they can no longer be employed at the place they are blowing the whistle on. In order to get any sort of recognition, protection and compensation will usually involve a legal battle against an often better-resourced employer, and (in terms of labour law processes), compensation is generally not more than 24 months' remuneration.

**Previous (ineffective) reporting.** Where whistleblowers are speaking to the media, the ideal scenario is where they have first tried other, internal avenues by reporting it to their own employer or another authority designated by the PDA. This is not a hard requirement but, from the perspective of the whistleblower, it is far riskier to speak to the media as a first port of call because the requirements for protection are the most difficult to meet. Here, whistleblower and media interests will tend to diverge, which makes it tough ground to navigate.



## CAN A WHISTLEBLOWER MAKE A PROTECTED DISCLOSURE TO THE MEDIA?

Technically a whistleblower can always speak to the media, but for a whistleblower to qualify for protection under the PDA then the Act's strict requirements are going to have to be met. Section 9 of the PDA leans heavily towards whistleblowers reporting impropriety first to their employers or to specific designated authorities. It doesn't expressly *exclude* the media as a first port of call, but makes it much *harder* for a whistleblower (going to the media) to qualify for the Act's protections. In these circumstances, it will also be important that the whistleblower meets the previously mentioned requirements – that they are acting in good faith, reasonably believe the allegations to be true, and are not motivated by personal gain.

There are also a number of exceptional circumstances where a whistleblower could be considered (under the Act) to have a good reason to approach the media first, and still be considered a protected disclosure, but it's probably a good idea to get specific legal advice about this *before* printing a story (see our Resources section for organisations that can assist potential whistleblowers). These circumstances might include situations where the whistleblower would face potential harm or detriment from their employer, if there is a risk that disclosure to an employer or other body might lead to the concealment or destruction of evidence, if a disclosure was previously made (to the employer) and no action was taken within a reasonable period of time, and also if the alleged misconduct is of an extremely serious nature. Ideally, **more than one of these conditions should be applicable**. There should also be clear reasons why other designated channels or authorities (for example, the Public Protector) were not used or could not be used.

## WHAT JUSTIFIES TAKING INFORMATION TO THE PRESS?

There are strict, limited requirements for a source to get protection under the PDA. From a journalist or editor's perspective, **no promises about protection should be made without careful consideration and expert legal advice.**

A court might consider all of the following features when determining if a disclosure made to the media can be protected under the Act:

1. The identity of the person to whom the disclosure is made (the media plays an important role in exposing wrongdoing, so this is often a supporting factor);
2. The seriousness of the impropriety;
3. Whether the impropriety is ongoing or about to happen (if a matter is extremely urgent – like a power station is about to explode and the employer is hiding that – it is conceivable that a strong case could be made out);
4. Whether the disclosure by the whistleblower breaches a duty of confidentiality or a law (this is usually a negative factor);
5. What actions the employer or section authorities took when the wrongdoing was reported (obviously, inaction is going to be best from a media perspective);
6. Whether the employee (whistleblower) complied with the employer's reporting procedures, when they first reported the matter;
7. The public interest in the matter.

## WHAT IS NOT CONSIDERED WHISTLEBLOWING (IN THE EYES OF THE LAW)?

As above, reports of wrongdoing made by people who are not employees or workers are not protected by the PDA. Reporting personal grievances is also not counted as whistleblowing – unless the grievance is a matter of public interest. The Ethics Institute defines a grievance as 'any feeling of discontent, unfairness, or injustice which employees may have in respect of their work conditions, against a manager or supervisor, or a fellow worker.'

But many public interest disclosures about wrongdoing or misconduct are made by people who are simply concerned citizens or community members. Although these are not covered by the PDA, they might reasonably be considered by the media (and the public) to be 'whistleblowers'. In these cases, other legislation can often be used for some form of protection.

## OTHER LEGISLATION THAT PROTECTS WHISTLEBLOWERS AND PUBLIC INTEREST DISCLOSURES IN SA

There are several other pieces of legislation that, to a greater and lesser degree, provide some protection for whistleblowers. All of them have differing internal requirements and it should be noted that disclosure to journalists is not necessarily what these Acts have in mind, although some do expressly mention the media.

1. Section 159 of the Companies Act;
2. Section 31(4) of the National Environmental Management Act (*which does permit disclosure to the media, subject to stricter requirements*);
3. Section 61 of the Marine Living Resources Act;
4. Section 60 of the National Forests Act;
5. Section 51 of the National Nuclear Regulator Act (*which does permit disclosure to the media, subject to stricter requirements*), and;
6. Section 9B(1) of the Pension Funds Act (*which also references third party disclosure*).

The 'environmental acts' (2-4) are interesting because they provide for rewards to be paid to whistleblowers. There have been a lot of calls for something like that to be extended to whistleblowers in SA more generally, but that's not currently the case.





## RESOURCES ON BLOWING THE WHISTLE!

*These free resources can be used by journalists and sources who are considering sharing protected or confidential information with the intention of exposing wrongdoing, corruption or criminal activities. While most of the guides address whistleblowing in the context of the Protected Disclosures Act, many of the same principles can be applied to other sources sharing information that is of public interest and importance.*

- **PPLAAF South Africa Whistleblower Protection Book**

<https://www.pplaaf.org/wp-content/uploads/Final-RSA-WB-Protection-Guidebook.pdf>

- **PPLAAF. Whistleblowing: Guidelines for journalists.** <https://www.pplaaf.org/2023/07/26/south-africa-whistleblowing-guidelines-for-journalists.html>

- **The Ethics Institute. Whistleblowing Management Handbook.**

[https://www.tei.org.za/wp-content/uploads/2020/09/Whistleblowing-Management-Handbook\\_Final-for-Web-.pdf](https://www.tei.org.za/wp-content/uploads/2020/09/Whistleblowing-Management-Handbook_Final-for-Web-.pdf)

- **Corruption Watch. The Whistleblower's Handbook.**

<https://www.corruptionwatch.org.za/wp-content/uploads/2015/05/Corruption-Watch-Whistleblower-handbook.pdf>

- **The Ethics Institute. Whistleblowing First Responder Guide.**

[https://www.tei.org.za/wp-content/uploads/2023/04/Final\\_Whistleblowing-First-Responder-Guide\\_E-book\\_978-0-6397-6767-3.pdf](https://www.tei.org.za/wp-content/uploads/2023/04/Final_Whistleblowing-First-Responder-Guide_E-book_978-0-6397-6767-3.pdf)



## EXERCISE

# CASE STUDY: THE GUPTA LEAKS

In early 2017, two men (known only as 'John' and 'Stan') shared a batch of computer files containing over 100,000 emails with journalists at AmaBhungane and the Daily Maverick. The emails were part of a trove of documents found on a computer hard drive that had been handed in for repair but never collected. The contents of the files directly implicated the well-connected and wealthy South African Gupta family in State Capture – this describes forms of systematic corruption that extend beyond single or limited acts of fraud and theft, and which include influencing and changing public policy and institutions in order to benefit a small group of people – instead of the public.

The cache of information, known as the 'Gupta Leaks' (see more at [gupta-leaks.com](http://gupta-leaks.com)) served to confirm the family's improper influence and connections with senior officials, government departments, and even international financial organisations. The documents contained on the hard drives were later submitted as evidence to the State Capture Commission, contributing to the resignation of the heavily implicated President Jacob Zuma, and prompting the Gupta family to flee the country shortly after, in 2018.

AmaBhungane and the Daily Maverick played a crucial role in assisting the two whistleblowers, and (later joined by News24) investigating and publishing the information revealed by the Gupta Leaks – but this was not without complications. While the two agencies were working on their investigations, and trying to protect the safety of the two whistleblowers by getting them out of the country, a sample of the emails was prematurely leaked to two other news organisations, prompting the *Sunday Times* and *City Press* to 'scoop' their colleagues by publishing a mini expose on the Gupta family. It was later confirmed that the source of the premature 're-leak' was businesswoman Magda Wierzycka, who the journalists had approached to assist with the

costs of protecting the whistleblowers. At the time, an editorial note from amaBhungane and the Daily Maverick commented that ‘those who caused the sample to be leaked to the two newspapers appear to have put expediency above the whistle-blowers’ safety.’

## EXERCISE



Read the following news articles about how the Gupta Leaks were revealed, and then use the questions below as prompts for discussion about the processes that were followed.

1. <https://amabhungane.org/editorial-the-guptaleaks-revealed/>
2. <https://www.citizen.co.za/news/south-africa/magda-wierzycka-forced-flee-sa-weeks-before-gupta-leaks-report/>
3. <https://www.moneyweb.co.za/moneyweb-podcasts/success-in-business-magda-wierzycka/>
4. <https://www.dailymaverick.co.za/article/2018-08-15-guptaleaks-whistle-blowers-speak-out-for-the-first-time/>

### Questions/discussion:

- a) Would you describe John and Stan as ‘whistleblowers’?
- b) Do you think the amaBhungane and Daily Maverick journalists were obliged to protect John and Stan’s identities? Did other people who were not journalists have similar obligations?
- c) Should the news outlets have published stories about the leaks immediately, or should they have waited longer to verify the contents?

# THE WHISTLEBLOWER SPECTRUM: MOTIVES, OBSTACLES AND CONSEQUENCES

Blowing the whistle on corrupt, criminal, harmful or irregular activities can involve long or complicated timelines, with events that might date back years or even decades, and a variety of role-players. For journalists and editors, it can be helpful to try and understand the context in which information about an alleged wrongdoing is being shared, and to consider what might have motivated your source to report this to you or your newsroom (or, equally, what might have prevented them from reporting it before).

In this section, we suggest you consider ‘motive’ as a standard part of your investigation and verification processes, and not as a basis for making a value judgement – having a clear idea of why a person chooses to blow the whistle, and why they do so at a particular time, can provide important details that can help you to check the information you are being given. Knowing the ‘full picture’ in advance also gives you and the whistleblower an opportunity to future-proof your stories against counter-claims, or malicious attempts to undermine your whistleblower’s character in an attempt to spoil or derail the story.





# WHY IS WHISTLEBLOWING IMPORTANT TO SOUTH AFRICA?

Ideally, we would want to live in societies where politicians, state services, the private sector, and individuals all operated in a transparent, considerate and ethical manner. The reality, though, is that crime and corruption (often accompanied by violence) are widespread – and are certainly not restricted to one country! In 2023, South Africa ranked 83rd out of 180 countries in the Transparency International Corruption Perceptions Index, meaning that slightly more than half of the countries in the world were considered to be more corrupt than South Africa... and just under half of the globe was thought to be less corrupt than us.

The Corruption Perceptions Index doesn't measure actual corruption (this is almost impossible to determine, given the inherently secret nature of this kind of fraud), but rather people's perceptions and beliefs about dishonesty. Perceptions are not always a match with reality, but they play an important role in informing either the building or the undoing of our trust in each other, and in our leaders. It's in this context that whistleblowing often plays an invisible role: by exposing wrongdoing, it promotes values of transparency, accountability, and integrity, and ultimately fosters a culture of accountability. Blowing the whistle on mismanagement and wrongdoing ultimately ensures that public and private entities operate ethically, and this strengthens the foundations of a just and accountable society. Reporting on crime and corruption also may lead to legal action and have a significant deterrent effect – or even aid in the recovery of money or assets.



# WHAT MOTIVATES A WHISTLEBLOWER?

Journalism often likes to turn the world into dramatic, binary narratives: good versus evil, something that can be summed up in a five-word, eye-catching headline. In reality, we know most of the stories we cover are more complex than this, but we also understand it's impossible to convey everything when you only have 400 words, or a 30-second news slot. This complexity applies to the types of sources we use too. For example, public relations representatives and government spokespeople aren't objective or independent sources, and we understand implicitly that they are there to perform a specific role on behalf of their client or employer. When it comes to sources who are reporting a wrongdoing, it's equally important to consider what prompted them to come forward. This is not because a 'virtuous' source is always going to be more reliable than an unscrupulous one; this isn't always the case, and sometimes seemingly well-meaning whistleblowers get the facts wrong because they believe so passionately in a cause. Other people might also decide to 'do the right thing' in exposing a crime, but for less noble reasons. Understanding what drives a source to blow the whistle encourages a journalist to see the whistleblower in a more realistic and pragmatic light, and this is a valuable tool when it comes to investigating your source and their claims (see next section).

## **RIGHT VS WRONG**

Whistleblowers – and by this we mean any person who tries to expose wrongdoing, corruption, and other harmful activities (so, not only a legally protected disclosure) – are often motivated by a strong personal sense of right and wrong. They may have deep-rooted religious or cultural or community values that underpin these beliefs, for example a belief in the need for justice, or the importance of standing up for vulnerable people or communities. They may also have a strong sense of empathy, for other people who they see being negatively impacted by crime or wrongdoing, or even for the natural world, like people who blow the whistle against harmful environmental practices.



Whistleblowers who appear to be or are motivated by a sense of morality or justice are often the most compelling sources for journalists because they are often so passionate about their story – but it can be easy to be drawn into a narrative rhetoric of ‘right’ versus ‘wrong’, which might obscure important facts and details. Just because a person feels strongly about a matter doesn’t always make it true, or accurate.

## **OBLIGATION**

Many whistleblowers are compelled to report wrongdoing because of how they see their professional roles and obligations – for example, an accounting officer who is responsible for compliance is obliged to report on non-compliance. Many professions (including accountants, lawyers, doctors, engineers and so on) have a formal code of conduct, which provides guidelines for how its members are expected to behave; for example, ‘do no harm’ might be part of the code of ethics for healthcare practitioners but also applies to many academics and researchers. An engineer or an architect might, similarly, be obliged to report on a structural defect or hazard in a building site.

## **BETRAYAL**

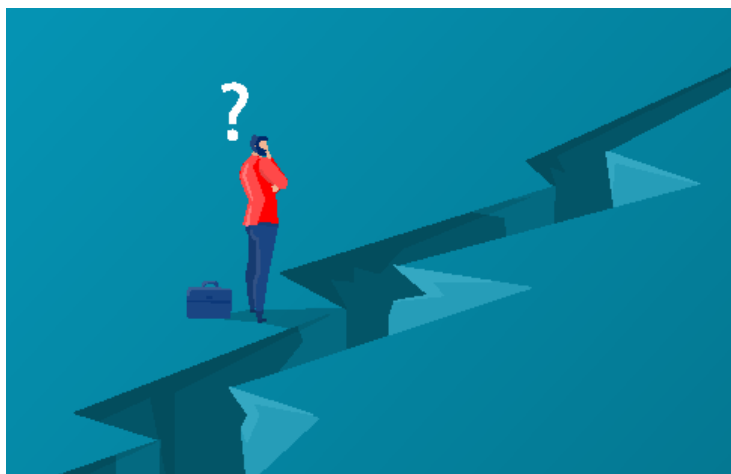
People also ‘blow the whistle’ on their peers, employers and people in power because they feel personally betrayed, or because they hope to benefit from another person or party being implicated in wrongdoing – or because they hope to protect themselves from any penalties or consequences. For example, a person might report on a misbehaving colleague at work because they see it as an opportunity to get a promotion or an increase, and to remove any ‘competition’ – or even because they are disappointed that their ‘wrongdoing’ colleague didn’t offer them the opportunity to get involved! A number of whistleblowers started off as wrongdoers, and then had a change of heart (for moral reasons, or because they were suddenly worried about getting caught), and then decided to blow the whistle on other people involved in the same crime... Sometimes these whistleblowers are also willing to accept the consequences of their own actions, but other times they may hope to be excused from any penalties or disadvantages.

# BARRIERS TO BLOWING THE WHISTLE!

While considering what motivates someone to become a whistleblower, reporters should also keep in mind that there are just as many reasons why a person doesn't report wrongdoing, and a number of potentially serious obstacles and challenges faced by the people who do eventually report on crime or misconduct. Many of these fears are, unfortunately, supported by the real-life experiences of whistleblowers around the world (see box).

Many whistleblowers (even the well-meaning ones) are initially reluctant to report on wrongdoing, because they understand it will draw negative attention to them, or perhaps because they hope that the bad behaviour will improve or go away in time without their intervention. It's not unusual for a source to wait sometimes for an extended period of time before alerting anyone to the wrongdoing. Unless the delay was deliberate, to give wrongdoers time to cover up their actions, reluctant whistleblowers should not be judged for being cautious!

If you or your newsroom are approached by a potential whistleblower, we recommend spending some time talking through each of the below scenarios, which will give both parties a more realistic perspective on the potential risks of going public with certain claims or information; this isn't just good journalism ethics, it's also good journalism and it will ultimately form part of your story planning and preparation.



## WHISTLEBLOWER WORRIES

Fear of losing their job

Longer-term financial and job insecurity

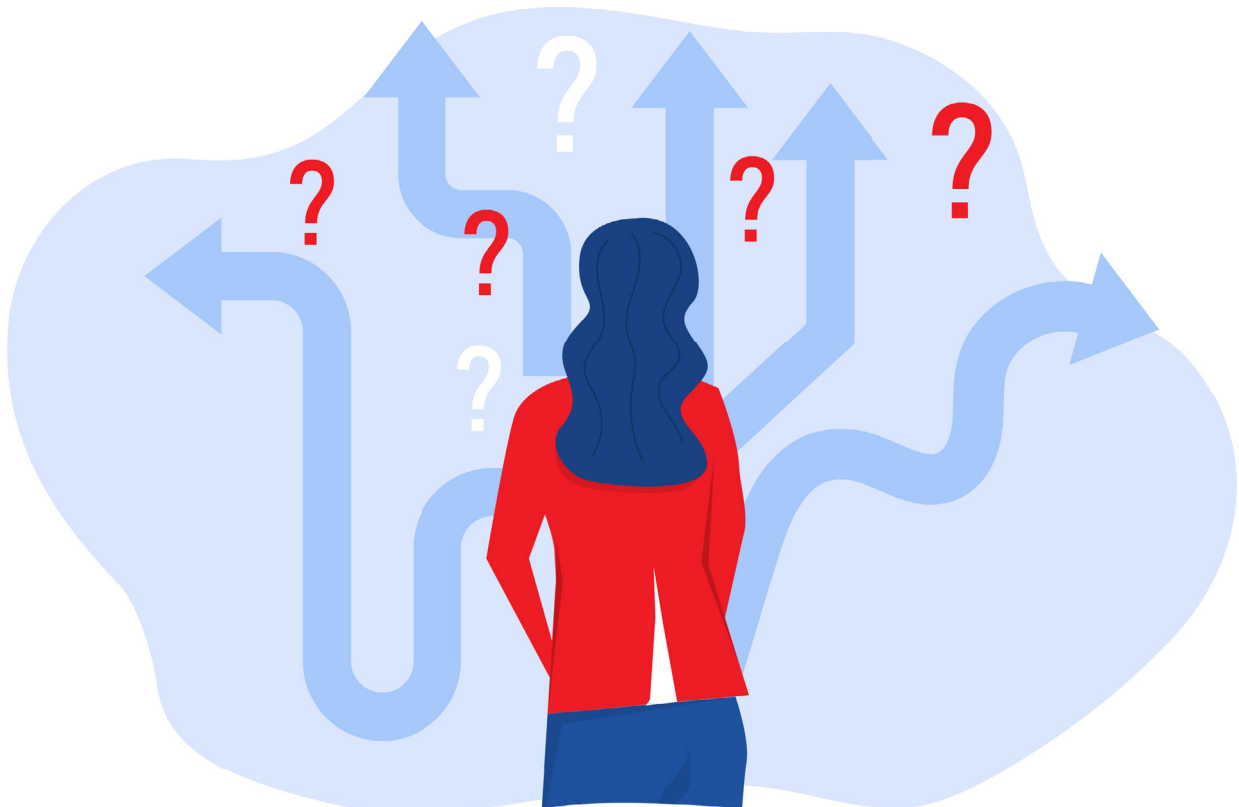
Fear of victimisation, isolation and intimidation

Fear for their family

Fear of breach of confidentiality  
(e.g., someone who promises to treat a report as confidential, but who then exposes it)

Lack of trust in the system

Fear that nothing will be done after the  
misconduct is reported



# WHAT ARE THE POTENTIAL CONSEQUENCES OF REPORTING MISCONDUCT OR WRONGDOING?

Experts and former whistleblowers have highlighted five key areas where whistleblowers commonly experience adverse consequences because of their reporting. Journalists and editors should keep in mind that a whistleblower may encounter threats or harms in more than one sphere, or at different times in the whistleblowing process.

## PHYSICAL

Many whistleblowers are threatened with or experience violence because of their reporting. In extreme cases (and this is unfortunately becoming more common in South Africa), whistleblowers have even been assassinated – either to prevent them from sharing their knowledge, or as ‘retribution’ for their actions, and to publicly intimidate future whistleblowers. In certain cases, whistleblowers may need to think about improving their security or physical safety, even hiring private protection. Whistleblowers also experience a variety of physical effects due to stress or anxiety, which could be worsened due to external factors like eating badly, lack of sleep, or substance abuse. A number of whistleblowers have reported developing alcohol or other substance dependency problems as a form of coping mechanism to deal with the stress and isolation of being a whistleblower.

## PSYCHOLOGICAL

Studies on whistleblowers show that an extremely high proportion of them (more than 80% in some cases) experience some or other form of mental distress directly related to the act of whistleblowing. These include severe depression or anxiety, feeling isolated, losing trust in other people, and having problems with maintaining family relationships. Many of these effects are intimately connected with other issues such as losing their job or losing their income or being threatened because of the whistleblowing. A number of whistleblowers also report experiencing post-traumatic stress disorder after the events.

## SOCIAL

Whistleblowers commonly report feeling isolated; while this might seem an obvious consequence in the workplace, it is not limited to just work colleagues. Sources have reported being cut off from their families and even by their places of worship. Family members may not share the same values as the whistleblower, or might not feel it's worth taking such a significant personal risk to report on corporate or state wrongdoing – and, as a result, they may not be supportive of the whistleblower's actions, which can be extremely distressing especially during a time when the whistleblower has few other means of support and encouragement. There may also be unintended knock-on issues; for example, if a whistleblower loses his or her job and can no longer pay a bond, or rent, or school fees, a family may have to move to another area or to another school, which can impact on the family's relationships with their own friends and communities.

## FINANCIAL

One of the most immediate consequences many whistleblowers experience is a sudden loss of income due to a loss of employment. This might be coupled with large and unexpected expenses – for example the costs of legal representation. The loss of income also has a domino effect on multiple other features including the ability to pay rent, buy groceries, pay school fees, pay for medical aid and life insurance, make car payments and even put fuel in the car. Each of these contributes to increased stress levels, and means that it becomes increasingly harder for the whistleblower to find simple ways to relieve or improve the stress (for example, if they lose their medical aid benefits they may not be able to afford therapy).

## EMPLOYMENT

Losing one's job can cause immediate financial, psychological, and physical harm to a whistleblower – things that the Protected Disclosures Act is designed to prevent (or at least remedy). But even successful cases of protected disclosures can take a long time, maybe even years, to resolve in the courts, often leaving the whistleblower unemployed for the entire time. Companies may also, ironically, be reluctant to hire someone with a history of 'blowing the whistle'.



## RESOURCES FOR WHISTLEBLOWERS



Journalists are not therapists, doctors, lawyers, bankers and should not even be friends with any of their sources – and there's no reason to try and perform any of these roles for a whistleblower (in fact, it can even harm the potential investigation and reporting on the case). Instead, if a journalist is working with a whistleblower who needs assistance or support of any kind, the responsible thing to do is to refer the whistleblower to one of several organisations who can offer independent and professional guidance in exactly these circumstances.

The **Whistleblower House** ([whistleblowerhouse.org](http://whistleblowerhouse.org)) is a non-profit organisation dedicated to helping whistleblowers with legal services, financial support, psychological support, and even the physical protection of whistleblowers and their family. Whistleblowers can apply for support by contacting the Whistleblower House directly.

Other organisations like the **PPLAAF** (the Platform to Protect Whistleblowers in Africa) may offer assistance with legal matters (but won't necessarily assist with things like household bills).

**The Ethics Institute** has published a handy Whistleblowing First Responder Guide (see the References section) which includes guidelines on how to respond to and handle situations where whistleblowers are reporting illegal activity – although this guide is not written for journalists, it includes expert advice which editors and reporters can easily adapt to individual matters.

Sources who are reporting information about alleged human rights abuses can seek support and assistance from the Southern African Human Rights Defenders Network, which is the regional coordinator of the Pan-African Human Rights Defenders Network known as **African Defenders** ([africandefenders.org](http://africandefenders.org)).



# BEST PRACTICES

Over the next few pages, we have included recommendations for basic journalistic steps and processes that should be followed for each claim or source when it comes to a potential whistleblower. We want to add the reminder that these steps should be completed every single time, and should not be bypassed because of deadlines, a rush to get a headline, to publish first before your competitors, or because your source is pressuring you. As we have seen in previous cases, being impatient to make the front page can often compromise the safety of the sources, and can unravel the entire story.

Journalism relies on building relationships with sources, and it's natural that these sources might approach someone they already know and trust when they have important information to share – particularly information that could place the source at risk. But reporters should be cautious when receiving confidential information from a source with whom they have a pre-existing relationship – because this might influence the investigation or verification processes. In these circumstances, both the story and investigation should ideally be handed over to an independent third party, or, if this is not possible, the journalist should work closely with their editor/s to ensure they remain objective, and don't cut corners or skip steps because they 'trust' a source.

## **ESTABLISH BOUNDARIES AND VERIFY YOUR SOURCE**

Before investigating allegations of wrongdoing, reporters and newsrooms should establish clear boundaries and guidelines with their whistleblower/source. This includes making it clear, upfront, that you will need to investigate and verify both the source/informant and their claims – but that you will attempt to do this in a non-intrusive manner, and specifically in a way that does not expose them to additional risk or harm. This is essential due diligence in any investigation and reporting process, and should never be skipped or bypassed because of urgency, fear of being scooped, or because you already know the source.

## YOUR INITIAL CHECKS SHOULD INCLUDE:

**Verifying their identity:** are they who they say they are? Can you find a digital footprint such as social media accounts, etc. that prove the source's identity – and which have not been created in the last few weeks!

**Verifying their role or credentials:** if they claim to work for a government department, can you find their name or photograph on an official website, or in a department newsletter? Be cautious when using sites like LinkedIn as these can trigger alerts on other people's pages or sites.

**Any other relevant information:** Has the person contacting you been in the press before? Has anyone else previously covered the story or information your source is providing? Is your source a 'professional' whistleblower (i.e., do they make a habit of 'reporting' on colleagues or employees)?

## RED FLAGS

Claims that rely only on the whistleblower's word, with no other supporting evidence or witnesses, should be treated with caution. Reporters should also watch out for sources who are inconsistent in their version of events, or who can't provide significant detail about important occurrences. Sources who are vague, evasive, and inconsistent should always be a red flag for a journalist.



# STEP 1: BUILD A TIMELINE

Working with a whistleblower to build a timeline can help you check and verify their story, and also provide contextual details that might ultimately support (or disprove) the whistleblower's claims. This kind of information is important as it shifts the narrative away from the whistleblower and on to the facts of the allegations.

Ask your source to provide a detailed timeline of the events that took place relating to their potential whistleblowing – this initial exercise should focus on **days, dates, times, incidents and people** rather than documents or detailed information, or claims of right versus wrong.

Focus on **who, when, and where** (the 'why' and 'how' will come later). Ask your source to start at the beginning, and talk you through the sequence of events that took place. If they start to jump around and muddle up different times, try to get them back to a structured timeline (moving from the past into the present day). Working with this kind of structure can be helpful for both journalists and whistleblowers, as developing a chronology can help the conversation or interview, and it might give the whistleblower a sense of control and order in what is often a chaotic and disruptive experience.

Keep in mind that a source's ability to adhere to a logical time structure might worsen when the person is in a highly emotional state – or a whistleblower might get obsessed with minute, even irrelevant details, which seem very important to them but are not important to the story or case. If a source becomes highly emotional or gets sidetracked, try to pause the interview/discussion (offering a glass of water or even a cup of tea might help to calm emotions), and then start again.

The timeline exercise can be done more than once. Repeating the exercise can help to fill in missing details, but it also provides a means for journalists to check their source's claims by watching out for inconsistencies and contradictions.

## HOW TO CHECK TIME AND PLACE:

Timeline narratives should provide a lot of checkable information, not all of it directly related to the whistleblowing claims – but all of which can help confirm the credibility of the claimant and the information. For example, if the whistleblower says they attended a conference on a certain date, you might be able to check and verify this using publicly available information. Look for facts like specific dates, public events like conferences or workshops, flight or other travel details including the name/s of hotels or conference venues, and even weather information like rain, heatwaves, flooding, snow, or extreme cold. Ask your source to describe seemingly irrelevant details like meals, or getting a cup of coffee. These details may eventually form part of your in-depth investigation, but initially they help you to verify the plausibility of the chain or sequence of events your source is describing.

## HAVE THEY REPORTED THE IRREGULARITY?

As part of your timeline discussion, it's important that you determine whether your source has previously reported the alleged wrongdoing to anyone else (other than the press), including whether or not they reported it internally through their organisation. If they have not done so, ask them why they have not reported it, and try to determine whether there is a reasonable case for them to have approached a journalist with their information (see Section 1 of this book), rather than one of the officially designated authorities.



# STEP 2: FOLLOW THE EVIDENCE

Once you have verified your source's identity and constructed a basic and timeline with your source, you need to start looking at the evidence they have to support their claim/s. In most instances, you will also need to do this in ways that do not draw attention.

**Does the whistleblower have any evidence?** This might be in the form of documents, photographs, digital files, audio recordings and so on. It also might be the case that the whistleblower has no physical or hard evidence, only what they claim to have seen or experienced themselves (testimony). It might also be difficult for the whistleblower to obtain evidence like financial records without being noticed. When assessing the claims and evidence, take the whistleblower's context into account.

**Is there any publicly available information that would support the whistleblower's claim?** Annual reports and other documents may provide proof, or at least support the version of events that the whistleblower is presenting.

**Are there any other witnesses or people who might support the whistleblower's claims or information?** Depending on the type of information, there may be other people who are also aware of or who have witnessed the alleged wrongdoing – they may not even be aware that the behaviour is irregular, but they can confirm the whistleblower's timeline of events or incidents. Reporters should ask their sources for the names of any other people who have knowledge of the matter, and who might be willing to discuss it. A priority here is of course to protect the confidentiality of your source, but this also cannot be at the expense of verifying the story or the information.



Don't rely on a single source for a high-stakes story. When the story is important, don't rely on a single journalist either.

# STEP 3:

## SAFETY AND SECURITY

### (FROM A JOURNALISM PERSPECTIVE)

When it comes to managing, investigating/verifying and working with confidential sources, journalists should think of safety as a continuum, starting with basic, everyday precautions and building up to more serious protective measures and processes on a needs-use basis. One of the challenges is that the more security you put in place, the more onerous and complicated even basic everyday activities can be. Security experts at the New York Times, for example, recommend keeping easy-to-use digital safety practices in place all the time, and only employing more extreme methods when they are really needed. The same should apply to physical safety protocols.

Always consider the **context** (where are you physically working, what is the story about, who is blowing the whistle, who is being accused or implicated?) and the import of the information – for example, evidence about an international arms deal is likely to be complex, and to involve actors with access to sophisticated technology. The bigger the story, the more you might have to consider additional safety measures.

Finally, when it comes to planning for the safety of both your source and yourself or your reporters, the key is to **have a plan in advance**, so that you know what to do if your or your source's threat level changes. Reporters and sources/whistleblowers should also include their family members in these plans – because a spouse's car or a teenager's cell phone or email address could also be vulnerable if malicious actors decide to monitor you or try to harm you.



Journalists and editors should work out a safety plan in advance, at the start of an investigation. Trying to find emergency contact numbers when you are in an emergency is never ideal.

## PHYSICAL SAFETY

Most South Africans already have a set of basic everyday safety practices in place – like locking the doors of a car when driving, storing bags in the boot rather than on the passenger seat, or keeping a cell phone hidden rather than holding it out in plain sight.



But when it comes to reporting on confidential information, provided by a source who might need to remain anonymous or at least have their identity protected, physical safety and security practices require a little more thought. As a start, it's a good security measure to let your colleagues know when you are going out on a story, where you will be travelling, and when you are expected to return. You could even share your details through a consent-based/opt-in location tracker. But if you are working with a source who needs to remain anonymous, this would not be a good option – and you might even need to disable location trackers if you already have them installed on your phone, or use an alternative mode of transport if you have a location tracker installed in your car.

The point here is that when working on a whistleblowing story, journalists and editors will need to consider the safety of the reporter *together with the safety of the source*. Whistleblowers should also get independent and possibly professional assistance with determining their own security risks and vulnerabilities (see Resources in Section 2).

**Meeting a source or informant:** The safest meeting places are often in public, where there are lots of other people – like a busy shopping mall, or a public park where many people walk their dogs. This is because it will seem less unusual for your source to be in a 'normal' public place, and also because it provides open opportunities for covert conversations or even document exchanges. Keep in mind, though, that if your source is seen sitting at a coffee shop having an animated conversation with a known journalist then this might pose a risk – so adapt your meeting locations and habits accordingly.

**Improve your basic security plan:** Even in a high-crime country like South Africa, it's easy to become complacent about certain security measures. Start upping your protection by simply being more aware of your environment – this means avoiding being distracted by your phone when you are driving near your home or your place of work, and taking note of your immediate environment including other people (or vehicles) within the environment. Depending on the kind of story being covered and the level of potential threat, you might also want to have an emergency contact list of the security companies and police stations in your area – keeping in mind that most police stations no longer have working landlines, and you will need to locate a working mobile number. Finally, make sure that your doors, windows and other security features (like security gates) are indeed locked when you are at home or in the office; if you have security alarms, set them whenever you are at home.

**Develop a basic threat response plan:** Work with your editor or other colleagues to model possible threats, and how you might respond to them. For example, if a police car (or a car with blue lights claiming to be the police) asks you to pull over, what should you do and what are your rights? If you are going to an area to meet with a source, can you identify 'safe zones' that you can use in an emergency (for example a petrol station, a police station, a hospital), and familiarize yourself with the routes and locations to these places.



End-to-end encryption (E2E) apps mean your message or data is encrypted when it gets sent to another person, and decrypted only when it arrives on their device (so it cannot be decrypted by anyone intercepting your message).



## DIGITAL SAFETY: FROM BASIC TO 'BEAST' MODE

Below are lists of digital safety practices that range from 'basic' (you should already be doing these, and these can be adopted for everyday use) to the high-alert 'beast' mode – this is when you are already or believe you might be under a high risk of attack, including digital surveillance, hacking and so on, or that your physical digital devices might be taken from you and used to unlawfully take your information.

### BASIC

- Add a password to your personal computer or any computer you use for your records and investigations. Make sure you don't re-use the same password on multiple accounts and are not using an easily guessable combination.
- Enable two-factor authentication (2FA) on all of your electronic accounts (for example, your password + a verification code that gets emailed or texted to you). Implement this for both your mobile and computer logins
- Don't click on any unknown links.
- Don't use a shared or communal computer to communicate with your sources, or to store or share information. Shared computers should also not be used to log in to secure browsers like Tor.
- Run regular scans and virus checks on your computer.
- Update all your apps and programmes (on mobile and desktop devices), so that you have the latest versions of software (which will also usually include security updates).
- Use secure end-to-end encrypted (E2E) apps for communication – this means your message or data is encrypted when it gets sent to the other person, and decrypted only when it arrives on their device (so it cannot be read or decrypted by anyone intercepting your message). Both Signal and Whatsapp have E2E but Signal's platform offers other protections in terms of the privacy of the user and the device. Journalists should keep in mind, however, that E2E encryption does not prevent physical interception of your messages – which can be shared through screenshots, by taking a person's phone, or by reading over a person's shoulder.



## INTERMEDIATE

*When starting to put stronger security measures in place, remember that it is not usually necessary to secure*



*everything – decide in advance which files or programmes are most important to make more secure or more inaccessible, and focus on these.*

- Using a passkey or password security tool or app can make your logins more secure (but this can also take more time and might not work seamlessly when you need to log in to your work email from your phone for example).
- Introduce secondary password or passkey protections on confidential documents. For example, if you have important information on your desktop computer, add a password to the document or the folder so that it's not accessible or visible to simply anyone who succeeds in accessing your desktop.
- Use secure browsers like Tor ([torproject.org](https://torproject.org)) to search and work online without being tracked or surveilled. [Note that if your computer is being monitored, using Tor will not prevent surveillance from seeing that you are using the site – only what you are viewing once you are in. Keystroke loggers will also still keep track of your typing, even when using Tor].
- Turn off location services on your mobile phone, and review your apps and permissions.
- Disable biometric passwords like face or touch identification, and create and use a strong password instead.
- Change your lock screen notifications/settings on your mobile phone so that messages, replies and other potentially sensitive information do not display on your locked screen and only display when you open your device using your password.
- Travel to meet with your source using public transport rather than a private vehicle (which will usually have a tracking device installed) or a transport app (which will similarly track your journey).
- Don't connect to any WiFi networks without using a VPN (virtual private network).
- Work with your back to a wall, not a window (make sure your computer or phone screen cannot be seen by other people).
- Remember to log out of your mail and other apps when finished, and to delete your browser history.

## BEAST

*These are more extreme digital security methods that can be implemented by most individuals even without specific help from a cybersecurity expert. However, if you are working on a high-impact and*

*high-risk story, it may be worthwhile consulting professional security experts to securely store/protect your data.*



- Encrypt your data (the Global Cyber Alliance or GCA has a guide on how to do this here: <https://gcatoolkit.org/journalists/encrypt-your-data/>) and consider storing encrypted data on a protected USB stick or similar remote location rather than on your own desktop.
- Enable lockdown mode on your mobile phone (make sure you know how to disable it too, as this can severely restrict your access to essential features, even making certain emergency calls).
- Set your mobile device to delete all data after 10 failed attempts.
- Use a separate cell phone to communicate with your source/s instead of using your own mobile devices. Keep in mind that RICA requirements may mean that even a 'burner' phone could be traced back to you or to the source. The second mobile device should also be kept securely – if your source is discovered with a second cell phone, for example, this might lead to some uncomfortable questions for them. This device should ideally not be a smart phone but rather a more basic mobile device with fewer apps that might track your movements.
- For more secure meetings, digital devices should be left behind entirely for the duration of the trip (even leaving your device in the car can leave a digital footprint, and suggest that your footprint and the source's footprint might have come near each other).
- Use a secure and anonymous information-sharing site like SecureDrop (currently used by News24 in South Africa) to receive and share information anonymously. Keep in mind, however, that sites like this can still be detected through certain surveillance apps (even if the content of the drop is unknown, surveillance tools like keystroke loggers might detect that the drop site has been accessed). Secure drop sites should never be accessed from shared or public computers.

# BE A JOURNALIST NOT A JUDGE

One of the reasons we caution journalists to think about the language they use to describe potential whistleblowers is that words can sometimes imply a verdict – and when it comes to whistleblowers, there are often many nuances and grey areas, and it's not always black or white or right and wrong. It's also not up to a journalist or editor to determine the guilt or innocence of someone, but rather to present the facts in an objective, accurate and transparent manner.

Reporters need to keep in mind that whistleblowers might be doing 'the right thing', but they could be doing this for a number of reasons, and whistleblowers are not always clearly the 'good guys' in the story. Often they are disgruntled employees, or guilty parties looking for a way to avoid some of the consequences of their actions. Both altruism and self-interest might be in play when it comes to a whistleblower, and it's important to pursue the facts of the case and the claims, rather than whether the person making the claims is likeable or not. Look at what the whistleblower is doing now, instead of judging them and dismissing them for what they might have done in the past. This is also something that can be fluid; reporters often start working on a story believing their source is a noble hero, and later it emerges that the whistleblower had also been involved in the irregular activity. This might change the narrative of the story, but it doesn't necessarily change the importance of the whistleblowing.

One strategy for this might be to focus on what the whistleblower is exposing, rather than on the person blowing the whistle – what are the social, economic, political or environmental impacts of the wrongdoing? If you think of a whistleblower as one of many potential sources in a story that is of public interest, how else would you tell the same story?

Another caveat is for journalists to avoid getting too emotionally involved with the source. This can happen easily when a journalist is excited about the story, and about the person making the whistleblowing claims, but if journalists lose objectivity they might also be compromised in their ability to protect their source, or deliver a credible story. Whistleblowers may also rely heavily on the journalist for support and encouragement, particularly if they are isolated from other people, and can become needy – or expect constant and instant attention. It's important for journalists to have empathy, but not become emotionally involved.

## MALICIOUS WHISTLEBLOWING

There are a number of documented cases where 'whistleblowing' type disclosures have been used to try and damage the reputation of a person or institution, undermine or threaten a source, and to attack the credibility of a story and/or the journalist and newsroom responsible for publishing the story. For example, anti-corruption personnel working in state institutions might be falsely accused of corruption, simply as a means to stop them from investigating cases of genuine corruption! While the Protected Disclosures Act has sanctions for bad-faith reporting, this doesn't necessarily prevent these kinds of tactics. Journalism can be used for malicious purposes – sometimes without the journalist's knowledge – by providing contradictory versions of a story (undermining the whistleblower's claims), by leaking sensational stories that are designed to distract audiences from an important disclosure (for example, celebrity gossip might get more attention than an investigative article), or by sharing information and publishing stories that undermine the reputation and character of a genuine whistleblower.

Most of these hazards can be identified and avoided by following the research and verification steps on the previous pages.

# WHAT HAPPENS NEXT?

Whistleblowing isn't just a once-off event – it can take place over an extended period and can take even longer to resolve (if it is resolved at all). This means that journalists and editors shouldn't only report on whistleblowing when a big case comes up, or when a specific case is in court, but should try and report on whistleblowing processes throughout the year. Civil society organisations say that this kind of advocacy is crucial for improving public perceptions of whistleblowers, and drawing attention to the existing mechanisms and legal protections for reporting these kinds of disclosures.

**Consistency is more important than headlines:** Covering stories about whistleblowers throughout the year is more important than occasional features. (Use some of the recommendations below to come up with additional story ideas for your news diary.)

**Build relationships with civil society organisations:** Read up about and make contact with the civil society organisations working to support whistleblowing and fight against corruption in South Africa (most of them are included in this book). These groups are often excellent sources for stories on their own, and can also provide insightful comment when covering a story about exposing irregular activities.

**Write about the broader consequences of crime and corruption:** If money gets misappropriated from National Lottery funds, it doesn't just get turned into a fancy mansion owned by the family member of a local official. It also often means that many charities or NPOs who do need the money are left under-resourced. Covering the wider consequences of irregular practices, corruption and crime can make audiences more aware of the wide-reaching impacts of these actions, and the importance of blowing the whistle.

**Write about everyday heroes and smaller/localised stories:** While large-scale corruption tends to get the largest headlines, audiences are also likely to pay attention to local news stories that expose problems in the areas where they live and work – these might include pollution or hazardous materials being dumped in a local river or park, the management of local community resources like clinics, schools, and even police stations, or the behaviour of local politicians (from ward councillors up). Whistleblowers in local communities often take exceptional risks to draw attention to seemingly ‘small’ stories that have big impacts on residents.

**Report on the existing mechanisms for dealing with the problem (and follow up):** Many corporate and state enterprises or institutions have existing formal mechanisms for reporting on irregularities or corruption, but very few stories on whistleblowers take the time to explore and explain these mechanisms – and whether they work, or are ineffective. For example, it might be helpful to write about anti-corruption hotlines in a large financial services company; or to explain how the police service’s Independent Police Investigative Directorate (IPID) is tasked with internal investigations. It’s also valuable to follow up when cases are instituted against civil servants or public sector employees – we often read about police officers being charged with crime or corruption, but very rarely get regular follow-ups about the status of the cases and whether or not there have been any convictions (or, we only read about convictions but are not usually informed about charges that have been dropped or dismissed, or cases that have stagnated).

**Report on anti-corruption processes:** There are a multitude of strategies, structures and support systems that have been developed in order to prevent and to detect corruption and wrongdoing in South Africa. Speak to representatives from the state, private sector, and civil society to report and follow up on anti-corruption strategies and actions – whether it is the National Anti-Corruption Strategy, or a new funding programme to support local anti-corruption initiatives.

**Create a diary to follow up on older stories, especially the smaller ones:** Use an old-school journalism practice to keep a diary of interesting cases – and add regular reminders (monthly, or every three months depending on the type of case) to follow up on a matter to find out if there has been any update or progress, for example if there is an arrest or charge made relating to the types of wrongdoing that might fall under general ‘whistleblowing’ practices.

# RESOURCES

## ORGANISATIONS

**The Ethics Institute:** [tei.org.za](http://tei.org.za)

**The Whistleblower House:** [whistleblowerhouse.org](http://whistleblowerhouse.org)

**OUTA:** [outa.co.za](http://outa.co.za)

**Corruption Watch:** [corruptionwatch.org.za](http://corruptionwatch.org.za)

**Platform to Protect Whistleblowers in Africa:** [pplAAF.org](http://pplAAF.org)

## PUBLICATIONS

**PPLAAF South Africa Whistleblower Protection Book**

<https://www.pplAAF.org/wp-content/uploads/Final-RSA-WB-Protection-Guidebook.pdf>

**PPLAAF. Whistleblowing: Guidelines for journalists.**

<https://www.pplAAF.org/2023/07/26/south-africa-whistleblowing-guidelines-for-journalists.html>

**The Ethics Institute. Whistleblowing Management Handbook.**

[https://www.tei.org.za/wp-content/uploads/2020/09/Whistleblowing-Management-Handbook\\_Final-for-Web-.pdf](https://www.tei.org.za/wp-content/uploads/2020/09/Whistleblowing-Management-Handbook_Final-for-Web-.pdf)

**Corruption Watch. The Whistleblower's Handbook.**

<https://www.corruptionwatch.org.za/wp-content/uploads/2015/05/Corruption-Watch-Whistleblower-handbook.pdf>

**The Ethics Institute. Whistleblowing First Responder Guide.**

[https://www.tei.org.za/wp-content/uploads/2023/04/Final\\_Whistleblowing-First-Responder-Guide\\_E-book\\_978-0-6397-6767-3.pdf](https://www.tei.org.za/wp-content/uploads/2023/04/Final_Whistleblowing-First-Responder-Guide_E-book_978-0-6397-6767-3.pdf)



Kleyn et al. (2021) **South African Whistleblowers: Tribulations and Triumphs**. Gordon Institute of Business. [https://content.gibs.co.za/cmscontent/media/emhjxlai/kleyn\\_south-african-whistleblowers.pdf](https://content.gibs.co.za/cmscontent/media/emhjxlai/kleyn_south-african-whistleblowers.pdf)

South African Human Rights Commission. nd. **Frequently asked questions on whistleblowers**. <https://www.sahrc.org.za/home/21/files/Human%20Rights%20FAQ%20Whistle%20Blowers%20Booklet.pdf>

## ADDITIONAL REFERENCES

Groenewald, L. **Whistleblowing Management Handbook**. The Ethics Institute. [https://www.tei.org.za/wp-content/uploads/2020/09/Whistleblowing-Management-Handbook\\_Final-for-Web-.pdf](https://www.tei.org.za/wp-content/uploads/2020/09/Whistleblowing-Management-Handbook_Final-for-Web-.pdf)

Kleyn et al. (2021) **South African Whistleblowers: Tribulations and Triumphs**. Gordon Institute of Business. [https://content.gibs.co.za/cmscontent/media/emhjxlai/kleyn\\_south-african-whistleblowers.pdf](https://content.gibs.co.za/cmscontent/media/emhjxlai/kleyn_south-african-whistleblowers.pdf)

Public Service Commission. n.d. **A Guide for Public Sector Managers Promoting Public Sector Accountability Implementing the Protected Disclosures Act**. [https://www.psc.gov.za/documents/docs/guidelines/PSC\\_odac\\_update.pdf](https://www.psc.gov.za/documents/docs/guidelines/PSC_odac_update.pdf)

PPLAAF. 2021. South Africa. <https://www.pplAAF.org/country/southafrica.html>

Commission of Inquiry into allegations of state capture, corruption and fraud in the Public Sector including organs of State, 2018. Volume 1. [https://www.statecapture.org.za/site/files/announcements/673/OCR\\_version\\_-\\_State\\_Capture\\_Commission\\_Report\\_Part\\_1\\_Vol\\_1.pdf](https://www.statecapture.org.za/site/files/announcements/673/OCR_version_-_State_Capture_Commission_Report_Part_1_Vol_1.pdf)

Van der Velden et al. "Mental Health Problems Among Whistleblowers: A Comparative Study." *Psychological reports* vol. 122,2 (2019): 632-644. doi:10.1177/0033294118757681