VOL 36 NO 2 2023

SOUTH AFRICAN JOURNAL OF CRIMINAL JUSTICE

TABLE OF CONTENTS

ARTICLES

RECENT CASES

Table of Contents

ARTICLES

RECENT CASES

SUBSCRIPTION — INTEKENING

Subscription:
R1 591.00 (including VAT but excluding postage and packaging)
Intekengeld:
R1 591.00 (BTW ingesluit maar sonder posgeld en verpakking)

Postage and packaging charges/Posgeld en verpakking koste:
Within the RSA/Binne die RSA — R327.58 per subscription/per inskrywing
Outside the RSA/Buite die RSA — R759.35 per subscription/per inskrywing

Subscriptions should be directed to the publisher:
JUTA Law, PO Box 24299, Lansdowne, 7779, Republic of South Africa
Telephone: 021 659 2300
E-mail: cserv@juta.co.za

Inskrywings moet gerig word aan die uitgewer:
JUTA Law, Posbus 24299, Lansdowne, 7779, Republiek van Suid-Afrika
Telefoon: 021 659 2300
E-pos: cserv@juta.co.za

Exclusive Distributors in North America:
Gaunt, Inc., Gaunt Building, 3011 Gulf Drive,
Holmes Beach, Florida 34217-2199, USA
Telephone: 941-778-5211
E-mail: info@gaunt.com

POLICY STATEMENT

The *South African Journal of Criminal Justice* is an accredited, specialist legal journal publishing articles, comments, surveys of recent cases and book reviews in English in the field of criminal justice, with a particular emphasis on southern Africa. The focus of the journal is on criminal law, criminal procedure, evidence, international criminal law and criminology. All articles and comments submitted for publication are reviewed by independent assessors to ensure that the Journal publishes only contributions of the highest quality, based upon original research. International scholars in criminal justice are represented on the editorial panel. The Journal, which appears three times a year, is indexed in South African Periodicals and the International Bibliography of Book Reviews of Scholarly Literature and abstracts from the Journal appear in Criminal Justice Abstracts.

Contributions to the *South African Journal of Criminal Justice* on topics related to criminal law and criminal justice are welcome and should be sent preferably via email to Prof Shannon Hoctor (email: svhoctor@sun.ac.za or LAWJOURNALS @sun.ac.za) or addressed to the Editor-in-Chief, *South African Journal of Criminal Justice*, Faculty of Law, Stellenbosch University.

Authors of articles shall receive a PDF copy of their article.

THIS JOURNAL SHOULD BE CITED AS (2023) 2 *SACJ*

SOUTH AFRICAN JOURNAL OF CRIMINAL JUSTICE

ISSN 1011 - 8527
Typeset by Peter Howe
Printed and bound by

HOUSE STYLE

When preparing contributions, contributors are requested to observe the following conventions:

(1) Submissions should be in English and in Times New Roman font, 12-font size double-spacing. Footnotes and quotations are single-spaced in 10-font size. MSWord is preferred. The name, address and phone number, academic qualifications, professional and academic status held by the author to be included on a separate page.

(2) Absent exceptional circumstances, **articles** should be no more than 10 000 words in length. **Comments** and **case notes** should be no more than 5 000 words in length. **Book review** lengths depend on the nature of the review.

(3) All articles must be accompanied by an abstract of no more than 200 words in length.

(4) Electronic copy should be in its final form as corrections on proofs will be limited to grammatical and stylistic errors or changes necessitated by legislative developments.

(5) Authors should pay meticulous attention to the accuracy of case names, citations and other references, judges' names and quotations. It is the author's responsibility to ensure that the house style is adhered to and articles will be returned to authors to correct for failure to observe the house style.

(6) It is assumed that an article submitted to the *South African Journal of Criminal Justice* has not been submitted to another publisher or journal. It is the policy of Juta and Company Ltd not to publish material that has already been published elsewhere. Please note that, on publication, copyright in all material is vested jointly in Juta and Company Ltd and the contributor.

(7) The following style must be observed for contributions to be accepted for publication:

(a) Levels of headings should be clearly indicated and marked H1, H2, H3 etc (where the number indicates the level of heading).

(b) Gender-neutral language should be used.

(c) As a general rule abbreviations should not be used and names of countries or organisations must be spelled out in full (thus United Nations instead of UN). Note that full stops are not used following any abbreviations.

(d) In **articles**, references to cases, journals, statutes and books are to appear in footnotes, numbered consecutively throughout and ending with a full stop. In **comments** and **case notes** the references are incorporated in the text in round brackets.

(e) References should be cited in the following manner:

(i) Cases

S v De Blom 1977 (3) SA 513 (A).

S v Makwanyane 1995 (2) SACR 1 (CC).

There is no need to refer to 'and Others' or 'and Another'.

(ii) *Journals*

JM Burchell 'Wilful blindness and the criminal law' (1985) 9 *SACJ* 261.

(**Note:** the author's initials precede the surname, no space between initials; the title of the article is in single quotation marks; the year of publication is in brackets; the volume number of the journal must be provided; the officially recognised journal title is italicised; the page on which the article commences and the page on which the citation appears must be included.)

K Askin 'Sexual violence in decisions and indictments of the Yugoslav and Rwandan tribunals: Current status' (1999) 93 *AJIL* 97 at 98n8.

(iii) *Books*

CR Snyman *Criminal Law* 5ed (1990) 555.

(**Note:** the author's initials precede the surname, no space between initials and edition number; the word 'page' (or 'p'), the publisher and place of publication of books are not included.)

(iv) *Statutes*

Criminal Procedure Act 51 of 1977.

(**Note:** do not use only the number and year (Act 51 of 1977))

Sections of an Act are referred to by the abbreviation 's' and plural 'ss'.

Subsections by 'subsec' and 'subsecs', except at the beginning of a sentence where the word is written in full ('Section' or 'Subsection').

(v) *Theses*
A Dhlamini *Family Violence in South African Criminal Law* LLM (Natal) (1960) 30.

(vi) *Law Commission*
South African Law Commission Discussion Paper 102 (Project 107) 'Sexual Offences: Process and Procedure' (2002) at para 2.3.4.

(vii) *Internet references/citations*
A Dworkin 'The United States and the International Criminal Court: A briefing' *Crimes of War Project*, 15 May 2002, available at *http://www.crimesofwar.org/onnews/news-us-icc.html*, accessed on 27 February 2003. (**Note:** Citation from the official, hard copy compilation is preferred. Where necessary, internet citations are acceptable but must be meticulously checked for accuracy and must be complete. The actual website is to be written in italics without brackets and the date on which the site was accessed must be reflected. If no page references are available, then the author must locate the citation by means of paragraph and/or section headings.)

(f) Subsequent references:

(i) *Cases*
S v De Blom supra (n000) at 123B-C.
(**Note:** supra is not underlined; 000 is the number of the footnote in which the case is first referred to with no spaces between the brackets; the page referred to is indicated by 'at' and (if necessary) the inclusion of side letters in upper or lower case, as in the judgment, with no spaces.)

(ii) *Journal articles*
Burchell op cit (n000) 123.

(iii) *Books*
Snyman op cit (n000) 234.
Note: only the author's surname is used; op cit is not italicised; 000 is the number of the footnote in which the work is first referred to.

(iv) *Statutes* are repeated in full in subsequent references.
Note: In all instances, 'Ibid' is used only when repeating the immediately preceding reference exactly; page numbers, authors' names, section numbers, etc are superfluous and incorrectly used with ibid.

(g) Quotations should be in single quotation marks ('Breakwater Declaration'). Quotations within quotations are in double quotation marks (' "Breakwater Declaration" '). Quotations longer than three lines are to be indented, single-spaced in 10-font size.

(h) The style of the Journal avoids the use of capital letters. Thus, as a general rule, write 'a court', 'the judge', 'the minister', 'the government', 'the state'. Capitals should be used where referring to individual institutions with given names: 'the Appellate Division', 'the Natal Provincial Division', 'the United Nations', etc. Examples:

1 CR Snyman *Criminal Law* 5ed (1990) 555.
2 Ibid.
3 JM Burchell 'Wilful blindness and the criminal law' (1985) 9 *SACJ* 261.
4 *S v Makwanyane* 1995 (2) SACR 1 (CC).
5 *S v Makwanyane* supra (n4) at 478I-J.
6 Snyman op cit (n1) 179.
7 Burchell op cit (n3) 262.
8 Section 2 of the Criminal Procedure Act 51 of 1977. Cf s 29.
9 A Dhlamini *Family Violence in South African Criminal Law* LLM (Natal) (1960) 30.
10 Dhlamini op cit (n9) 78.

Cyber-warrant searches and the admissibility of seized smartphone data evidence at trial

CONSTANTINE THEOPHILOPOULOS*

ABSTRACT

A validly issued cyber-warrant is a primary investigating tool in the seizure of smartphone data content and may be the only lawful method of obtaining relevant data-file evidence about the cyber-offence culpability of a co-perpetrator, accomplice, or accessory. A cyber-warrant for the seizure and search of a portable handheld smartphone, or minicomputer, must be drafted in a manner that is procedurally different from the warrant for the seizure of a desktop or laptop computer. This article critically examines the warrant procedures for accessing and searching relevant data files stored in a smartphone's default storage mediums and downloaded applications. These technical procedures are described in the Cybercrimes Act, indirectly in the Electronic Communications and Transactions Act, the Criminal Procedure Act, and related Acts. This procedural analysis is based on a revised principle of smartphone cyber-intelligibility, and the application of the sub-principles of cyber-offence particularity and data-access specificity. The substantive issue of cyber-privacy and the procedural issue of chain-of-data evidence custody is briefly examined.

1 Introduction

There is a considerable disconnect between the traditional criminal procedures which define a compelling order such as a state-issued warrant, or subpoena *duces tecum*, which allows for the search, seizure, and admissibility at trial of physical articles, as opposed to the same for incorporeal digital information stored in a data file on a smartphone in the form of a digital data message. This procedural disconnect has been previously and indirectly addressed by academic

* BSc LLB (Wits) LLM LLD (SA); Associate Professor, Interim Director and supervising attorney, Law Clinic, University of the Witwatersrand. ORCID: https://orcid.org/0000-0003-4336-1044.

https://doi.org/10.47348/SACJ/v36/i2a3

authority,[1] and the Law Commission Paper 99 on computer related crime.[2] This divide continues to exist despite the enactment of the Cybercrimes Act,[3] and, previously, the Electronic Communications and Transactions Act.[4] The procedural divide exists principally because the search warrant procedures in the above two Acts are an amended cut-and-paste version of the traditional common law warrant procedures codified in the Criminal Procedure Act.[5] These traditional common law-based search procedures may not be a good fit with modern developments in smartphone technology.[6] *Goqwana v Minister of Safety and Security NO*,[7] held that a warrant is a 'substantive weapon in the State's armoury' which embodies awesome procedural powers as well as formidable constitutional and evidentiary consequences. With these evidentiary consequences in mind, it may also be argued that the warrant procedures of the Cybercrimes Act and Electronic Communications and Transactions Act fail to legally accommodate the technology built into modern smartphones. In particular, these two Acts fail to coherently define the unique procedures necessary for a new kind of technologically based 'seizure', 'access', 'search' and the chain of evidence custody process needed in order to 'preserve' a data file seized from a smartphone. In other words, the common law principle of intelligibility, as set out in *Minister of Safety and Security v Van der Merwe,*[8] which defines how a physical article is to

---

1 JGJ Nortje and DC Myburgh 'The search and seizure of digital evidence by forensic investigators in South Africa' (2019) 22 *PER/PELJ* DOI http://dx.doi.org/10.17159/1727-3781/2019/v22i0a4886; C Theophilopoulos 'The admissibility of data, data messages and electronic documents at trial' (2015) 3 *TSAR* 461 at 463; GP Bouwer 'Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' (2014) 27 *SACJ* 156-171; V Basdeo 'The legal challenge of search and seizure of electronic evidence in South African criminal procedure: a comparative analysis' (2012) 25 *SACJ* 195-212.

2 South African Law Commission Discussion Paper 99 (Project 108) 'Computer Related Crimes: Preliminary Proposals for Reform' (2001).

3 Sections 29-34 of the Cybercrimes Act 19 of 2020.

4 Sections 82-83 of the Electronic Communications and Transactions Act 25 of 2002.

5 Sections 20-26 of the Criminal Procedure Act 51 of 1977.

6 *Katz v United States* 389 US 347 (1967) at 360-362, noting that the judicial system must continually seek to interpret and evaluate the changing nature of the constitutional right to privacy in the face of evolving technology.

7 2016 (1) SACR 384 (SCA) at paras [13], [30] per Willis JA, the issue of a search warrant must be tempered by the constitutionally enshrined rights of a warrant recipient to personal dignity, privacy, freedom and security; *Magajane v Chairperson, North West Gambling Board* 2006 (2) SACR 447 (CC) at para [74], stating that a search warrant must limit privacy intrusion and clearly inform the recipient of the warrant's legality and search limits.

8 *Minister of Safety and Security v Van der Merwe* 2011 (2) SACR 301 (CC) at paras [39], [55]-[56].

be searched for and seized must be materially amended to account for the technological complexity of a seizure and search of a smartphone. This article will re-examine the unique jurisdictional requirements of a warrant (hereinafter cyber-warrant) in respect of (i) its purpose in governing the scope of a cyber-search; and (ii) the procedures which should guide the technological parameters of the seizure, access, and search of smartphone data files relevant to a cybercrime. In particular, this article is narrowly concerned with the seizure and search of a cyber-article before the issue of a preservation order. This article does not examine s 44 of the Cybercrimes Act which concerns the procedures for the disclosure of data after the issue of a preservation order.

In addition, this article will briefly examine the various evidentiary defences which a recipient of a cyber-warrant may invoke during the course and conduct of a cyber-search. A smartphone, and a computer, contain a large amount of stored personal information.[9] A subject of an overbroad search may invoke a number of entrenched constitutional rights as a defence, including (a) an unreasonable and unjustifiable infringement of the right to dignity (s 10 of the Constitution) and privacy (s 14 of the Constitution),[10] (b) an attorney acting on behalf of a subject may raise attorney-client privilege,[11] (c) a subject may raise the privilege against self-incrimination when the object of the search is a pre-existing incriminating data file stored on the drive of a

[9] *Riley v California* 573 US 373 (2014) paras 375, 394-395, 'a cell phone collects in one place many distinct types of information – an address, a note, a bank statement, a video that reveals more in combination than any isolated record' and amounts to a 'significant cache of sensitive personal information'; *US v Djibo* 151 F. Supp. 3d 297 (EDNY 2015) at 310, a smartphone contains 'the combined footprint of what is occurring socially, economically, personally, psychologically and spiritually in the owner's life'.

[10] Section 14 of the Constitution, 1996, privacy includes the right not to have person or home searched, property or possessions seized, and privacy of communication infringed. The USA Constitution, Fourth Amendment, protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, and no warrant shall be issued except on probable cause. See s 51 of the Electronic Communications and Transactions Act 25 of 2002, which lists several privacy concerns which must be adhered to by a data controller. See also W Nortje 'Warrantless search and seizures by the South African Police Service: Weighing up the right to privacy versus the prevention of crime' (2021) 24 *PER/PELJ* 27p.

[11] *Minister of Safety and Security v Bennett* 2009 (2) SACR 17 (SCA); *S v Safatsa* 1988 (1) SA 868 (A) at 885, attorney-client or legal professional privilege is a fundamental right central to a fair trial.

https://doi.org/10.47348/SACJ/v36/i2a3

smartphone, computer or on the cloud,[12] and (d) a subject may raise a defence that the chain of evidence custody in preserving a seized data file was not properly adhered to rendering such electronic evidence inadmissible at trial.[13]

2 Foundational requirements of a cyber-warrant

A traditional search warrant must be issued by a judicial officer with due diligence and only after careful scrutiny (i.e. with due technical rigour and exactitude) to ensure that the circumstances in which the search, access and seizure is to be carried out exhibits an appropriate degree of specificity which renders the warrant intelligible to its named recipient.[14] All the material and legal facts which explain the purpose of the warrant must be placed before the judicial officer to ensure that the warrant does not amount to an unreasonable and unjustifiable infringement of the recipient's dignity, privacy and other constitutional rights.[15] According to the common law principle of intelligibility, all the jurisdictional facts concerning the offence, the physical premises to be searched, the articles to be seized, the identity of the authorised officer, and the identity of the recipient of the warrant must be clearly articulated in the warrant.[16] A smartphone cyber-warrant has materially different foundational requirements. Before drafting a cyber-warrant, the designated police official must carefully consider what kinds of evidence are intended to be discovered during a seizure and search of

[12] Section 35(1)(*c*) and 35(3)(*j*) Constitution, 1996, an arrested person cannot be compelled to make a confession or admission that can be used in evidence against that person, and an accused cannot be compelled to give self-incriminating evidence at trial. Section 203 Criminal Procedure Act 51 of 1977, no witness in a criminal proceeding shall be compelled to answer any question if the answer would expose the witness to the risk of a possible future prosecution.

[13] See s 29(2) and (3) of the National Prosecuting Authority Act 32 of 1998; s 29 of the Criminal Procedure Act 51 of 1977.

[14] *Goqwana v Minister of Safety and Security NO* supra (n7) at para [30], intelligibility means that a warrant must be issued with care, after scrutiny, and not reflexively upon a mere checklist approach*; Powell NO v Van der Merwe NO* 2005 (5) SA 62 (SCA) at para [50].

[15] *Thint (Pty) Ltd v National Director of Public Prosecutions* 2008 (2) SACR 421 (CC) at para [126], a judicial officer must ask himself/herself whether it is reasonable for the state to seek a search warrant and not to employ other less invasive means to obtain the targeted relevant evidence. The judicial officer must objectively determine whether the state may be able to obtain the evidence using a less invasive means before issuing the warrant.

[16] *Minister of Safety & Security v Van der Merwe* supra (n8) at paras [55]-[56]*; Powell NO v Van der Merwe* supra (n14) at para [59], according to the intelligibility principle a warrant must specify its object and must do so intelligibly and narrowly within the bounds of the empowering statute. A valid warrant allows police to seize the physical computer and legitimately access its electronic content.

https://doi.org/10.47348/SACJ/v36/i2a3

a smartphone or any other digital device. The police official must also determine where the targeted evidence is located – on the smartphone, or on a service provider server, or on the iCloud, etc. A cyber-search strategy must be based on uncovering the following kinds of relevant admissible evidence:

(i) A smartphone itself may constitute physical evidence of an offence where the smartphone has been stolen (hardware seizure).
(ii) A smartphone may contain stored data on its hard drives relevant to an offence (data evidence seizure).
(iii) A smartphone can be used as an instrument in the commission of an offence (software, programs and metadata seizure).

Therefore, the principal purpose of a cyber-warrant is to seize a cyber-article that may be relevant and admissible as prima facie evidence of an offence. A secondary purpose of a cyber-warrant is to identify whether the recipient personally entered the relevant data evidence into the smartphone's hard drive, or whether a third party with access to the smartphone did so. It will also be necessary in respect of some cyber-offences to determine whether the smartphone was hacked and whether a virus program was responsible for the commission of the offence unknown to the smartphone owner or user.

The designated search officer, or the assisting s 29(3) investigator, should be aware that a smartphone search must not only concentrate on current running applications and stored undeleted data files, but that deleted data may also amount to relevant evidence. For example, data remnants of fully or partially deleted data files do remain on the hard drive and may be seized where relevant. Smartphone use creates metadata that may be relevant to what data files have been created, accessed, edited, or deleted during the time frame in which an offence was committed. Browser, e-mail, chat, photo, or video apps contain files that may reveal online nicknames or passwords. A smartphone's operating programs contain data detail about internet usage, the use of peripheral external hard drives and other digital equipment. A primary question to be answered in this article is whether a cyber-warrant's requirements as set out in chapters 3 and 4 of the Cybercrimes Act reasonably take into account the intelligibility principle (hereinafter a cyber-intelligibility principle) in respect of the technological forms of seizure, access and search of a smartphone within the evidentiary framework set out above. The traditional procedures of a physical search and seizure of a physical article situated in physical premises need to be replaced by procedures compatible with the physical seizure of a smartphone, or computer, and the subsequent digital access and an on-site or off-site IT forensic search of a digital device's storage mediums, programs, and applications. The descriptive term

https://doi.org/10.47348/SACJ/v36/i2a3

'data evidence' and 'digital device' is preferred to 'electronic evidence' or 'electronic device' as the word electronic is broad and may equally refer to an electronic radio, clock, watch, or programmable vacuum-cleaner, etc. The label 'cyber' is used to distinguish the principle of cyber-intelligibility from the common law principle, as is the label cyber-warrant or cyber-search. The word 'cyber' is used here purely because of its citation as such in the Cybercrimes Act.

3 Smartphone jurisdiction requirements

A principal flaw with a cyber-warrant's jurisdictional application (i.e. jurisdiction - the legal power of an investigatory state organ to induce compliance with a compelling order in a definite area) as defined in s 25 read with ss 30(4)-33(1) of the Cybercrimes Act is that it remains mired in the common law-based definition of territorial jurisdiction as described in chapter 2 of the Criminal Procedure Act. This type of territorial-based jurisdiction only partially accommodates the technological advances in cloud computing and internet globalisation which permits a smartphone, or computer user, to store data messages on cloud servers situated in multiple foreign jurisdictions (i.e. cloud data jurisdiction). The question here is one of trans-border seizure. In terms of the cyber-intelligibility principle can a smartphone search warrant issued within a South African court jurisdiction by a South African judicial officer, in respect to a South African recognised offence, be applied to seize, access, and preserve smartphone data stored in a foreign jurisdiction? Where a state organ uses a legally seized smartphone, or computer, in South Africa to access data stored on a server in another sovereign country, it is exercising a long-arm extraterritorial jurisdiction, which may well render the seized data evidence inadmissible at trial. A review of current legislation does not answer this question with any degree of clarity, and a number of circumstantial inferences must be made in order to bridge this gap.

The four core jurisdictional requirements set out in the Electronic Communications and Transactions Act,[17] and Cybercrimes Act,[18] were inherited from the traditional common law principles as set out in chapter 2 of the Criminal Procedure Act. The chapter 2 principles explain that (i) a search warrant is validly issued when the seized article is situated in physically defined premises, or is in the possession, or control of a person within the area of territorial jurisdiction over which the issuing judicial officer exercises effective control (s 21 of the

[17] Sections 83(2) and s 90 of the Electronic Communications and Transactions Act 25 of 2002.

[18] Section 24 of the Cybercrimes Act 19 of 2020.

https://doi.org/10.47348/SACJ/v36/i2a3

Criminal Procedure Act), (ii) the state may seize any article relevant to an offence committed within the territorial borders of South Africa, (or by a South African citizen in a foreign jurisdiction, on a South African flagged aircraft or ship), for the purpose of admitting the article as evidence at a criminal proceedings (s 20 read with s 21 of the Criminal Procedure Act), (iii) the state may seize any relevant article without a warrant either by consent of a targeted person, or on the arrest of a person, or under reasonable suspicion that a delay in obtaining a warrant would defeat the object of a search (ss 22-23 of the Criminal Procedure Act), and (iv) in effect a search warrant authorises a designated state official to enter any premises, and to use reasonable force to overcome any resistance, in order to search and seize any article relevant as evidence (ss 24-29 of the Criminal Procedure Act). These four core requirements are entirely based on the principle of effectiveness, territorial jurisdiction, and the search of a physical location (e.g. premises, ship, aircraft, container, etc). While these core requirements are procedurally effective for the seizure of a physical smartphone used in the commission of an offence within South Africa, and effective for the access of data and metadata evidence stored on the seized smartphone's hard drive – they are not procedurally adaptive or effective when the data/metadata evidence has been uploaded to the cloud and stored in servers in multiple foreign jurisdictions.

Other legislation setting out jurisdiction requirements for a search and seizure are equally deficient in respect of the seizure of smartphone or computer-stored data files as evidence. For example, s 13(6) of the South African Police Services Act,[19] allows for the 'authorised search and seizure control of illegal cross-border movement of people or goods' and s 13(8)(*a*)-(*d*) for the 'authorised roadblock/checkpoint search and seizure of any object'. These sections cannot readily be adapted to the seizure of an 'object' such as a smartphone, or a computer, and the procedures to be applied in preserving these seized digital devices as evidence. Especially where the evidentiary relevant data is located on the device's hard drive, or on a cloud server situated in South Africa, or in a foreign location. Similarly, s 29 of the National Prosecuting Authority Act,[20] concerning a search warrant issued to an investigatory director, is silent about the procedures dealing with a seizure, access, search and preservation of smartphone data. For example, s 29(1)(*c*) uses antiquated sentences such as 'make copies of or take extracts from any book or document' bearing on an investigation. As a consequence of these legislative lacunae, may it be reasonably inferred that a police investigator, or an investigating director, in

[19] Section 13(6)-(8) of the South African Police Services Act 68 of 1995.

[20] Section 29(1)-(11) of the National Prosecuting Authority Act 32 of 1998.

https://doi.org/10.47348/SACJ/v36/i2a3

possession of a validly issued cyber-warrant, or on reasonable cause, has the procedural authority to exercise investigatory jurisdiction over relevant cloud-based data stored on a foreign server after seizing and searching a smartphone, or computer, in South Africa? Alternatively, the wording in the relevant sections of the South African Police Services Act, and the National Prosecuting Authority Act, should be amended to make these Acts compatible with the new technologically influenced cyber-warrant procedures of the Cybercrimes Act. For example, the reference in the South African Police Services Act to an 'object' should be supplemented with a reference to a s 1 'cyber-article' as it is defined in the Cybercrimes Act. Similarly, a reference to a cyber-article should be included in the National Prosecuting Authority Act. Chapter 4 of the Cybercrimes Act should also be amended to include a specific cross-reference to the said Acts. Presently s 27 of the Cybercrimes Act only refers to the Criminal Procedure Act.

Sections 82(1)(*c)* and 83 of the Electronic Communications and Transactions Act permits a cyber inspector to enter any South African premises, access any information system, and seize and preserve any relevant data messages as evidence. Again, the Electronic Communications and Transactions Act does not clearly set out whether a cyber inspector's warrant powers are limited to the seizure of relevant data stored on a South African based server (or from a South African based service provider) or whether these warrant powers may be extended to the seizure of data evidence stored on a server in a foreign jurisdiction. Section 29 of the Cybercrimes Act incorporates traditional common law language to give jurisdiction to a South African court to try any cybercrime committed in the 'territory of South Africa' or 'on board a South African ship, etc' or where the person to be charged 'is a citizen, or resident, or company registered in South Africa'. Sections 27-29 of the Cybercrimes Act allows a police official in terms of a validly issued cyber-warrant to seize, access and search any article in the jurisdictional territory of the issuing judicial officer's or 'within the Republic'. Again, it is unclear, according to a revised cyber-intelligibility principle, whether the seizure of a smartphone in South Africa, in terms of a validly issued cyber-warrant, allows an investigating officer to directly access, grab, download and preserve for evidentiary purposes relevant data-files stored on a cloud server based in a foreign jurisdiction. Especially when there is a reasonable suspicion that data will be immediately deleted thereby defeating the reason for the search. While ss 48 and 51 of the Cybercrimes Act, read with chapter 2 of the International Co-Operation in Criminal Matters Act,[21] allow for mutual cross-border access to relevant seized data

[21] Chapter 2 of the International Co-Operation in Criminal Matters Act 75 of 1996.

https://doi.org/10.47348/SACJ/v36/i2a3

stored on a server in a foreign jurisdiction, the state-to-foreign state procedures set out in these sections are administratively complex, costly, and time consuming.

4 The search of smartphone data relevant to a cyber-offence

Section 1 of the Cybercrimes Act defines a cyber-article capable of being seized and searched as 'data, or a computer program, or a computer data storage medium, or a computer system'. A s 1 cyber-article may be reasonably summarised as:

> 'any digital programmable device (which produces or reproduces storable data by way of a pre-determined set of logical and arithmetical instructions contained in a computer program) capable of inter-connection with other computer systems via an electronic communication network and which allows for the exchange of data messages, metadata, and traffic data'.

A smartphone falls within this summarised definition as it may be technically referred to (i) as a mini or portable computer system containing a data storage medium, and (ii) which is capable of connecting to a telecommunication network and (iii) capable of transmitting or receiving indirect communications via such a network.[22] A future high court should interpret a s 1 cyber-article in a manner which allows for a separate definition for a smartphone and other portable devices such as tablets, etc. A separate definition for a smartphone, as opposed to a computer, is justified as the functional usage of these digital devices vary. A smartphone is hand sized and may lack the gigabit storage capacity of a computer or even a laptop. A smartphone has also been defined as a portable pocket 'extension of the individual user's mind worthy of constitutional privacy protection against intrusion',[23] and that a forced seizure and access to a smartphone amounts to a breach of an individual's mental autonomy.[24]

---

[22] See s 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 and the definition of a cellular phone; *Riley v California* supra (n9) paras 393, 396-397, a cell phone could easily be called a camera, video player, rolodex, calendar, library, diary album, television, map, and newspaper. A cell phone search will expose the state to far more information than the most exhaustive physical search of premises.

[23] K Vold 'Is your smartphone an extension of your mind?' *VICE*, 2 March 2018, available at *https://www.vice.com/en_us/article/qvemgb/is-yoursmartphone-an-extension-of-your-mind* accessed on 7 March 2023.

[24] M Lynch 'Leave my iphone alone: Why our smartphones are extensions of ourselves' *The Guardian*, 19 February 2016, available at *https://www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves* accessed on 7 March 2023. See C Theophilopoulos 'The privilege against self-incrimination and the distinction between testimonial and non-testimonial

https://doi.org/10.47348/SACJ/v36/i2a3

In order to be legally seized as an item of admissible relevant evidence, a s 1 cyber-article must be concerned, or connected with, or used, or intended to be used, in the commission of a cyber-offence, or any other offence (recognised as such by South African law). The cyber-offences defined in chapter 2 of the Cybercrimes Act are precisely tailored to account for the unlawful manipulation of the unique technological features of a computer or smartphone. Chapter 2, part I, types of cybercrimes target the manipulation of a computer program and/or data and are roughly divided into four groups. First, offences that punish unlawful hacking or access, use, functioning, copying, and interception of the data and the programs of a computing system (ss 2-4 and 11). Secondly, offences that punish unlawful interference with the data (i.e. deletion, alteration, damage) and/or functionality, availability, confidentiality and integrity of the computer programs and storage mediums of a computer system (ss 5-6 and 11). Thirdly, an offence that targets the unlawful acquisition and possession of a password, code, pin, user-authentication, biometric data, etc, to access and manipulate the data, programs, and storage mediums of a computer system (ss 7 and 11 read with s 37(2)(*a*). Fourthly, common law specific fraud-related offences suitably modified to include cyber-fraud, forgery and uttering, and extortion (ss 8-10).

Chapter 2, part II, cybercrimes target malicious communications and unlawful disclosure of data messages to a person, or group of persons, which incites damage to property or violence, which threaten a person with violence or damage to property, and which discloses intimate data images without consent (ss 13-16). Other cyber-offences include the use of a digital device to steal incorporeal property (s 12) and in part III, s 17, the unlawful conspiring with another person to aid, abet, induce, incite, instigate, instruct/command, or procure another person to commit a cyber-offence as defined in part I or part II above.

A designated police official, when drafting a search warrant and a magistrate, or other judicial officer, when issuing a smartphone seizure and search warrant should, according to the cyber intelligibility principle, consider the functional and usage differences between a smartphone and a computer. For example:

(1) *Storage capacity*: The software programs of a desktop or laptop computer permits a recipient of a search warrant to flexibly hide relevant data messages anywhere in a folder, file, sub-file, or data document and in many differently located storage mediums. These folders, files, or data documents can be misleadingly labelled and individually password locked. However, a smartphone is designed

evidence' (2010) 127 *SALJ* 107 at 118, for the jurisprudential meaning of personal mental autonomy.

https://doi.org/10.47348/SACJ/v36/i2a3

as a mobile operating system containing software that consists of specific kinds of default applications for ease of communication, socialising, and entertainment use. The recipient of a smartphone search warrant has limited options regarding the hiding of relevant data in a smartphone. Relevant data evidence can easily be searched for and located in call logs, text and chat messages, WhatsApp, e-mail, notes, calendar, photo and video gallery, internet browsing history, GPS data, and other defined downloaded apps, etc.

(2) *Method of seizure*: A desktop computer, or even a laptop, is not easily portable and therefore is more likely to be seized and searched by entering a suspect's premises on the authority of a written warrant, whereas a portable smartphone is more likely to be seized when a suspect is, on reasonable suspicion or by consent, personally searched either at a roadblock, at a crime scene, or while running away from a crime scene. This may also require a male officer to search a male suspect and a female officer for a female suspect.[25] Furthermore, a smartphone is easily hidden and a burner or starter pack phone easily discarded.

(3) *Type of offence*: A computer and a smartphone contain different types of software applications for different kinds of usage purposes. This means that a computer is more likely to be connected to and used in a different range of offences to that of a smartphone. A smartphone is more likely to be used to commit part II malicious communication types of cybercrimes (since this is the predominate technological feature of a smartphone), including cyber stalking/bullying, cyber defamation, using the camera and audio application to film, store, and distribute intimate images or pornography. Smartphone settings, including GPS, call logs, browsing history, social network information, tower locations and location history data, provide relevant evidence about acts of preparing for a crime or executing a crime such as drug trafficking and prostitution, etc.

(4) *Camera and video evidence*: The majority of South Africans carry a cell phone of one type or another. Most cell phones contain a camera with video and audio features. It is common for witnesses present during the commission of a crime to photograph or video-record criminal conduct in real time. Such image and video evidence is clearly relevant to a crime and may be the subject of a seizure and search. Usually in terms of a s 29 warrant but in some circumstances in terms of s 31 with consent of the person.[26]

[25] In terms of s 36(2) of the Cybercrimes Act 19 of 2020, a search must be conducted with decency and in an orderly manner with due regard to the rights of other persons. See also s 29 of the Criminal Procedure Act 51 of 1977.

[26] Section 31 by consent, s 32 on reasonable belief, and s 33 on arrest, Cybercrimes Act 19 of 2020.

https://doi.org/10.47348/SACJ/v36/i2a3

(5) *Operation and functionality*: A smartphone, unlike a computer, cannot function independently and must be linked to a service provider's cellular telecommunication network. Multiple cyber-warrants may be required, one directed to the smartphone user or owner, and a subpoena directed to the service provider.[27]

Essentially, a smartphone's portability and its unique digital architecture make it an efficient instrument for the preparation of a crime, the commission of a crime, a real time record of a crime in progress, and as a storage medium for relevant data and metadata evidence of a crime. Portability also makes a smartphone easily disposable, and its contents easily deleted. Therefore, a search warrant may require an on-site seizure to secure the physical phone (i.e. a data acquisition step), but an off-site examination to access, search to locate relevant data, duplicate, and preserve relevant data evidence (i.e. a data analysis step).[28] The practical reasons for taking a smartphone off-site for examination must be clearly set out in the cyber-warrant.[29] The reasons may include the fact that a hasty on-site search and access to a smartphone's hard drive may risk damaging the authenticity and integrity of the targeted data evidence. A computer system and its operating programs continually read and write to a smartphone hard drive thereby continually altering the metadata stored on the drive. Internet-connected smartphones are also at risk of third-party online hacking and manual or automatic deletion while an on-site examination is in progress. A password, passcode or biometric-protected smartphone will usually need to be examined off-site by a qualified IT expert to crack or bypass these security features, as bypassing security features is a forensically time-consuming process. Alternatively, in some circumstances it may be urgently necessary to make an on-site examination. This may be done by using a forensic software program to create a duplicate (also referred to as a mirror image copy) of the data stored on a hard drive that is

[27] A s 34 service provider may assist with information about a subscriber's name, address and credit card details, the IP address assigned to the subscriber including data about opened, unopened, draft and sent e-mails, logs showing when a subscriber logged on and off its service, etc.

[28] A s 25 'seizure' means to (a) remove any part of a computer system, (b) render inaccessible any data, program, storage medium or any part of a computer system to preserve evidence, (c) make/retain a copy (duplicate) of data or a computer program, and (d) make/retain a printout of the output of data or a computer program.

[29] A s 37(2)(*a*) 'access' to a computer program or storage medium through the use of forensic software, decryption key, device or equipment must be made in a manner and for the purpose specified in the cyber-warrant.

https://doi.org/10.47348/SACJ/v36/i2a3

identical to the original.[30] A copy that 'duplicates every bit and byte of the targeted drive in exactly the order appearing on the original'.[31] It may also be necessary to preserve and safeguard the relevant data of a seized smartphone and this may be achieved by placing the phone in a Faraday pouch or by removing the smartphone battery.[32]

5 Accessing smartphone data via a written cyber-warrant

The requirements for a validly drafted cyber-warrant and the procedures which a magistrate (i.e. judicial officer) must follow in issuing a cyber-warrant must be interpreted in a manner which accounts for the specific technology, communicative and entertainment purpose, and general information usage of a smartphone. A magistrate must also consider how a smartphone's data content is accessed and preserved in order to be admissible evidence at trial. The Cybercrimes Act allows for several distinct procedural stages in the execution of a seizure and search whether by warrant or on reasonable suspicion. For example, the written warrant procedure sets out the following steps:

(i) Section 29 empowers a designated police official to physically seize a cyber-article widely defined as a computer system, computer program and storage mediums. [33]

[30] A forensic access and analysis of a smartphone will usually involve a two-stage process. First, making a duplicate of the data on the seized hard drive. Secondly, analysing the data content of the duplicate to identify the relevant data evidence. Because a multifunctional digital smartphone contains many gigabytes of data it will be necessary to use some type of key word search or forensic software to locate, identify, and isolate the relevant types of evidence described in the cyber-warrant.

[31] OS Kerr 'Searches and seizures in a digital world' (2005) 119 *Harv L Rev* 531-586. See *S v Miller* 2016 (1) SACR 251 (WCC) at para [17], a designated police official may admit as evidence at trial data and metadata obtained from a service provider by a valid warrant which has been correlated by a software program (e.g. Analyst Notebook) to provide a summarised version of relevant evidence about (i) contacts between various cell phone numbers, (ii) the identity of subscribers to these numbers, (iii) the length of the conversation between these numbers, (iv) where the cell phones are geographical located, and (v) the time frame in which these conversations occurred. Also, police who have validly seized smartphones and SIM cards may access the content of these articles.

[32] A Faraday pouch shields a device by preventing penetration by any electronic signals, thereby preventing a third party from remotely accessing a smartphone and wiping relevant data.

[33] *Young v Minister of Safety & Security* 2005 (2) SACR 437 (SE) at paras [29]-[31], where a designated police official has left the premises during a day search to fetch equipment required to copy computer files and had returned in the evening did not constitute a second or unauthorised search.

https://doi.org/10.47348/SACJ/v36/i2a3

(ii) Section 29(2) read with s 25 empowers a designated police officer (with the assistance of a s 29(3) investigator where necessary),[34] to access any relevant cyber-article. To search through storage mediums, programs, applications and via human manipulation to analyse the stored data.
(iii) Section 29 read with s 25 permits not only the physical seizure of the smartphone but also includes the forensic creation of a duplicate original and the seizure or retention of the duplicate as admissible evidence at trial.
(iv) Sections 41-42 empower a designated police official to ensure that the seized and accessed data evidence is properly preserved.[35]

In practice, the cyber-warrant procedures likely to apply to the seizure of a smartphone is s 29(2)(*a*)-(*e*) which permits a designated police official to enter and search any premises, to search any identified person, or any person reasonably believed to be capable of providing relevant information. Section 29(2)(*g*), read with s 25, permits the seizure of a cyber-article identified in a warrant by removing, or rendering inaccessible, any part of a computer system to preserve data evidence. A duplicate may be made of any seized computer program or data. Section 29(2)(*f*) & *(h*), read with s 25, in broad language permits access to a seized smartphone's data by way of any device (including any instrument, equipment, or any accessories and components thereof), decryption key, password, or computer system (including any computer data, program, or storage medium) to access and search any cyber-article described in the warrant. However, the Cybercrimes Act may be criticised for being deficient in respect to the seizure of a smartphone in the following respects:

(a) Its seizure procedures are simply a revised version of the traditional warrant procedures set out in the Criminal Procedure Act. It also uses broad language in describing the execution of these procedures. This may present a magistrate with some interpretive problems when applying the principle of cyber-intelligibility to the issue of a valid cyber-warrant for the seizure of a smartphone.

[34] An investigator is not a police officer and may subject to the direction and control of a designated police official, assist with the seizure, access, and search of a cyber-article (see ss 31(2), 32(3) & 33(4)). Technical or other assistance may also be rendered where reasonably necessary by an electronic communications service provider, financial institution, or person in control of premises or a computer system (s 34).

[35] *Ntoyakhe v Minister of Safety & Security* 1999 (2) SACR 349 (E), seizure of an article also implies the continued detention of the article for evidentiary purposes at trial.

https://doi.org/10.47348/SACJ/v36/i2a3

(b) It is silent on how the ss 82-83 warrant procedures of the Electronic Communications and Transmissions Act supplement the cyber-warrant procedures.[36]
(c) It does not clearly set out step by step what kind of chain-of-evidence custody structure must be maintained to render the seized and preserved data evidence admissible at trial.[37]

According to *Oosthuizen v Magistrate, Hermanus*,[38] the objective test of cyber-intelligibility requires that a valid cyber-warrant must be drafted in clear language and with due cyber-specificity and cyber-particularity. A valid warrant must contain all the legally necessary objectively defined jurisdictional facts which must be set out with reasonable cyber-intelligibility and without being vague or strikingly broad in identifying the cyber-article to be seized. In other words, particularity is required as to the manner in which a smartphone is identified, seized, and accessed by a designated police official. The specificity basis of a validly issued cyber-warrant is that the seized smartphone must be linked, on reasonable grounds, to the commission, or suspected commission, of a specified chapter 2 (part I through to III) cyber-offence, or any other common law or statutorily defined offence.[39] The purpose of a cyber-warrant is to permit the physical seizure of a smartphone for a number of investigatory and evidentiary reasons:

(i) The smartphone itself may serve as physical evidence of the commission of an offence, and it may also serve as the starting point of the chain-of-evidence custody process.[40]
(ii) A smartphone must first be legally seized to validly access any relevant stored data evidence on its hard drive.

[36] In terms of s 29 reference is made to supplementary search procedures of the Customs and Excise Act 91 of 1964, the Tax Administration Act 28 of 2011 and the Customs Control Act 31 2014 but not to the criminal warrant procedures of the South African Police Act 68 of 1995 or the National Prosecuting Authority Act 32 of 1998.

[37] *Oosthuizen v Magistrate, Hermanus* 2021 (1) SACR 278 (WCC) at para [89], a mirror image (duplicate) taken from a seized iPhone must be sealed and furnished to the Registrar of the Court.

[38] *Oosthuizen v Magistrate, Hermanus* supra (n37) at paras [39] and [43].

[39] *Keating v Senior Magistrate* 2019 (1) SACR 396 (GP) at paras [46] and [49], the validity of a warrant depends on the facts-in-issue. An objection that a warrant is overbroad must be considered in relation to the offence under investigation and the modus operandi of the offence.

[40] Each individual smartphone has an easily proved unique identity number, or IMEI number, allowing it to be the starting point of the chain of evidence custody check list.

https://doi.org/10.47348/SACJ/v36/i2a3

(iii) Where the stored data amounts to relevant evidence of an offence, such data evidence must be preserved by way of a validly issued preservation direction in order to be admissible at trial.

(iv) A s 29(3) investigator assisting the designated police officer in accessing a smartphone may be subpoenaed as an expert witness to testify about the evidentiary relevance, authenticity, and integrity of the data seized and preserved (s 53(3)).[41]

(v) A s 53 expert witness may be required to testify orally by subpoena or via a written affidavit about any interpretation of data, the design and functioning of a computer system or a communication network, or smartphone software engineering or programming.

(vi) Section 29(2)(*g*)-(*h*) read with s 25(*c*)-(*d*) permits the forensic making and retention of a duplicate copy of seized data. The duplicate is defined as an 'original' for evidentiary purposes. In terms of ss 14 and 15 of the Electronic Communications and Transactions Act, the integrity of the duplicate original is assessed by examining whether it has remained complete and unaltered (except for changes in metadata as the duplicate is accessed for analysis),[42] from the time it is first generated to the time it is produced, or displayed, as relevant evidence at trial.

These smartphone cyber-warrant requirements must be strictly adhered to in order to prevent any trial objection based on an unjustifiable infringement of a personal right to smartphone privacy or personal user

[41] *Keating v Senior Magistrate* supra (n39) at para [35], in an age when technology and expertise is becoming increasingly specialised it is unrealistic to expect a state agency at any time to possess all of the technical expertise necessary to conduct a successful search; *Grammaticus (Pty) Ltd v Minister of Police* (8694/17) [2017] ZAGPPHC 342 (22 March 2017), at paras [33]-[36], a non-police expert may be present at a search to advise a designated police officer on identifying and downloading the relevant data evidence from seized computer equipment, but cannot execute a warrant or carry out a lawful seizure and search; *S v Miller* supra (n31) at para [56], ss 81 and 86 of the Electronic Communications and Transactions Act 25 of 2002 authorises a designated police officer to search any digital device. The designated police officer may make use of a cyber inspector to assist in the search, but the police are not obliged to follow a rigid bureaucratic procedure to access digital information as opposed to non-digital evidentiary material. In terms of s 24(2) of the Independent Police Investigative Directorate Act 1 of 2011, it is also possible to include officials of the Independent Police Investigative Directorate (IPID) in the list of officials to execute a warrant.

[42] In terms of s 14(2)(*a*) of the Electronic Communications and Transactions Act 25 of 2002, the duplicate remains complete and unaltered except for 'the addition of any endorsement and any change which arises in the normal course of communication, storage and display'.

https://doi.org/10.47348/SACJ/v36/i2a3

dignity, the defence of illegally obtained evidence,[43] or to pre-empt an invocation of attorney-client privilege,[44] or the privilege against self-incrimination. Also taking into account the evidentiary problem that privileged data documents may be difficult to separate from other relevant data documents during a search. Furthermore, there is no case authority on how the privilege against self-incrimination will apply to preserved data files containing incriminating evidentiary data.[45] Generally, when paper documents are searched for and physically seized on premises, an appointed third party is at hand to examine and determine which documents or files contain privileged information. A smartphone may contain thousands of data documents hidden in various data files and applications. In order to sift through these data files to ensure that privileged data information is not seized, it may be necessary to appoint an objective 'filter third party' tasked with reviewing data files and separating privileged data files from non-privileged data files. To ensure that no objection to the seized data evidence is raised at trial it may also be procedurally necessary to have defence counsel review the output of the filter third party to identify those data documents against which the defence intends to raise a trial objection.

6 Accessing smartphone data without a cyber-warrant

A smartphone's portability and its telecommunication technology largely determine the way it is used. While a search of a suspect's premises during an ongoing police investigation may uncover a smartphone, the more likely manner of seizing a smartphone is when it is in the possession, control, or upon a person. It is more likely to be searched for and seized by a police officer without a written warrant, under reasonable suspicion, when apprehending a suspect at a crime scene, fleeing from a crime scene, or at a roadblock, etc,

[43] Section 37 of the Cybercrimes Act 19 of 2020 'wrongful searches and seizures' read with s 35(5) of the Constitution, data evidence obtained by way of an illegal seizure and search is inadmissible if it renders a trial unfair or is determinantal to the administration of justice.

[44] See *Minister of Safety & Security v Bennett* 2009 (2) SACR 17 (SCA), where seized privileged documents were kept in sealed boxes, taken off-site and only opened in the presence of the defence attorney – a search strategy not applicable to data documents; *Bogoshi v Van Vuuren NO; Bogoshi v Director, Office of Serious Economic Offences* 1996 (1) SA 785 (A) at 793, privileged documents are not liable to be seized by a s 20-25 Criminal Procedure warrant.

[45] See C Theophilopoulos 'State compulsion of smartphone security features and the privilege against self-incrimination' this issue 2 of *SACJ* 2023 at 282. See Theophilopoulos op cit (n24) 131-140. See also C Theophilopoulos 'Defining the limits of the common law, South African and European privilege against self-incrimination' (2014) 25 *Stell L Rev* 160-186.

https://doi.org/10.47348/SACJ/v36/i2a3

in terms of ss 32-33 of the Cybercrimes Act. These two sections allow for the seizure of a cyber-article without a warrant (i.e. based on a reasonable belief that delay would defeat the object of the search),[46] but that subsequent access to the cyber-article must be made in terms of a written or oral warrant (hereafter defined as an access warrant).[47] However, these two sections do allow for access to a smartphone after seizure without the necessity of an access warrant under the catch-all grounds of 'exceptional circumstances' or 'urgency'.[48] In essence, the cumulative effect of these two sections, is that it allows a designated police official a window of opportunity, on the somewhat vague catch-all of reasonable suspicion, in which to seize and access a smartphone without applying for a written warrant. What constitutes a ground of exceptional circumstance, or urgency, is not set out in the Cybercrimes Act and in respect to a smartphone will have to be hammered out by the courts in due course. A possible ground of urgency in seizing and accessing a smartphone could be to prevent the destruction of smartphone data evidence. Urgency may be reasonably based on the fact that:

(i) A modern smartphone's storage mediums are turned over many times during its use span. A user may on a regular basis manually wipe files and applications in order to free up storage space. Some types of smartphones have a default setting for the automatic deletion of old text messages after a certain period of time has elapsed.
(ii) It may be impossible to obtain any specific data content of smartphone usage as all South African service providers do not store such content on their company servers, or at best, delete such content after a few days.[49]
(iii) However, where smartphone data is stored for any length of time, it is usually stored on cloud servers situated in a foreign jurisdiction. As noted above in paragraph three timeous access to

[46] Section 32(1)(*a*)-(*b*) Cybercrimes Act 19 of 2020. See *Ndabeni v Minister of Law and Order* 1984 (3) SA 500 (D), reasonable belief to be determined objectively based on an assessment of all the facts, and onus on the state to show that reasonable grounds existed at the time of the police search and seizure. See also *Mincey v Arizona* 437 US 385 (1978) at 393, a warrantless search is reasonable when the exigencies of the circumstance require it and the needs of law enforcement are compelling.

[47] Section 32(1) and (2) read with s 30(1) of the Cybercrimes Act 19 of 2020.

[48] Section 32(1)(*a*)-(*b*) and s 32(2)(*a*)-(*b*) of the Cybercrimes Act 19 of 2020.

[49] To prevent a service provider from deleting data content from its servers, as is the usual business and logistic practice, ss 41-43 of the Cybercrimes Act preservation of data directions oblige a targeted service provider to preserve data for a period of 21 days but not exceeding 90 days. However, a police investigation, and a decision to search and seize, may take longer than the statutory allowed time periods.

https://doi.org/10.47348/SACJ/v36/i2a3

a foreign-based server by a state organ may be time-consuming and costly.

In other words, while a s 41 expedited preservation of data direction may be executed on a user, or service provider, it may be too late to prevent the remote automatic or time delay deletion of data from a suspect's smartphone. It may also be too late to prevent a suspect from remotely key encrypting access to data held on a cloud-based server.[50]

7 Conclusion

The constitutional privacy and dignity concerns of a warrant recipient is one of the principal reasons why a magistrate may refuse to issue a smartphone cyber-warrant.[51] Modern smartphones contain many gigabytes of storage capacity which translates into millions of personally intimate text messages or data documents, and thousands of photos and videos. Smartphone users expect a certain legitimate expectation of privacy when purchasing a smartphone, and for this reason all smartphones contain various kinds of security features such as password, passcode, or biometric protections.[52] A smartphone cyber-warrant cannot simply amount to a vaguely worded fishing expedition intended to allow access to a seized smartphone so as to hunt around in its various applications, programs, and storage mediums on the odd chance of finding incriminating data. A cyber-warrant must be sufficiently particular as to the nexus between the cyber-offence and the seized data. In order to address the cyber-intelligibility principle

[50] Section 29 of the Regulation of Interception of Communications and Provision of Communication-related Information 70 of 2002, provides for a decryption direction to be executed against a decryption key holder to disclose a decryption key or to provided decryption advice.

[51] *Goqwana v Minister of Safety and Security NO* supra (n7) at para [13]; *Oosthuizen v Magistrate, Hermanus* supra (n35) at para [7], the issue and execution of a warrant implicates conflicting interests - the state interest in prosecuting crime and the individual's right to privacy and dignity; *Thint (Pty) Ltd v National Director of Public Prosecutions* supra (n15) at para [79], (i) when issuing a warrant the judicial officer must exercise a discretion which allows for the protection of a recipient's privacy concerns, (ii) the scope of the warrant must not be too broad to unreasonably infringe on privacy interests, (iii) a review court may strike down an unreasonably broad warrant and order the return of any illegally seized articles, and (iv) an accused is entitled to object to the admission of illegally seized articles as evidence which will render trial unfair. See also *Katz v United States* supra (n6) at 360-362, (i) in a case circumstance (e.g. the seizure and access of a smartphone for evidence relevant to a cyber-offence) is there an actual expectation of privacy, (ii) is the expectation of privacy one that society is prepared to recognise as reasonable, and (iii) even reasonable expectations of privacy may be defeated by electronic as well as physical invasion.

[52] *Riley v California* supra (n9).

https://doi.org/10.47348/SACJ/v36/i2a3

and smartphone privacy concerns the author makes the following suggestions:

(i) A smartphone cyber-warrant must be sufficiently particular to prevent giving a designated police official an unreasonably broad discretion in determining what computer programs, storage mediums, data, files or apps to cherry-pick and seize. A warrant lacks particularity and may possibly amount to an unjustifiable infringement of privacy when the scope of the cyber-search is limited only by a police official's discretion. A warrant also lacks particularity when the designated police official merely states that in his/her experience and training as a detective there is likely to be relevant data evidence on a suspect's smartphone.

(ii) A cyber-warrant must be case specific and must clearly describe the type of cybercrime, or other offence, being investigated, and the type of electronic data files to be searched for. For example, where the offence relates to the illegal disclosure of intimate images such as child pornography, the access warrant should be flexibly limited to a seized smartphone's photo storage, video and audio apps, e-mails, or other image related computer programs. Possibly including access to text messages within the time frame in which the image-based offence was committed. Where cyber-stalking, or other malicious communication is at issue, the access warrant should be limited to text and chat messages, call logs, e-mails, and other similar apps which enable smartphone technology to be used in the planning and commission of the criminal communication.

(iii) A cyber-warrant lacks specificity and particularity and unjustifiably infringes a subject's right to privacy (i.e. a reasonable expectation of privacy) when it refers to the catch-all seizure of 'any computer programs and storage mediums', 'any and all computer equipment', 'all relevant electronic information to be gained from internal storage components and memory cards or sim cards', 'all cell phone electronic information', or 'all electronic equipment including iPhones desktop computers, laptops and iPads', etc.[53]

(iv) A cyber-warrant must be drafted with three distinct procedural steps in mind. First, the procedural step to seize the smartphone as an item of physical evidence. Secondly, the step to compel the

[53] *Oosthuizen v Magistrate, Hermanus* supra (n37) at paras [69]-[79], a reference to information stored in all electronic equipment - even where an attempt is made to limit such reference to a specific iPhone, laptop, desktop, or iPad is too broad. A warrant must identify the data content to be seized as precisely as possible to limit any inroads into a recipient's privacy and to prevent a general ransacking of his/her digital devices; *Craig Smith v Minister of Home Affairs* 2015 (1) BCLR 81 (WCC) at para [94], a warrant is overbroad when it refers to any computer including laptops and external hard drives or all computer related equipment and peripherals.

https://doi.org/10.47348/SACJ/v36/i2a3

production of a password or encryption key where it is envisaged that it may be difficult to unlock or bypass the security features of the seized smartphone. Thirdly, ensuring that the seized relevant data is properly analysed, stored, and the correct chain-of-evidence custody is followed.

(v) To preserve the chain-of-data evidence custody, a forensic investigator analysing the seized duplicate must maintain a chronological record of how and when the data was accessed. A custody record must include a unique identification number/label for the seized data, the authorised person who placed the data in official storage, when and how the data is accessed, by whom and for what reason. The record must also contain a regularly updated list of metadata changes made whenever data is accessed and exposed to human observation or interaction.

A validly and timeously issued cyber-warrant is an extremely important investigatory tool in the fight against cyber-crimes. The lawful seizure of relevant smartphone data files is critical in determining the culpability of co-perpetrators, accomplices, and accessories in a criminal investigation. Smartphone files, data, and metadata may provide prima facie evidence of participation, criminal planning, commission of an offence and motive. Therefore, it may be useful to set out some of the most common types of smartphone data, and metadata, which may aid a designated police officer in a case-specific investigation, and which serve as a general guide for the drafting of a valid cyber-warrant in accordance with the cyber-intelligibility principle:

(i) *Data connecting co-participants and establishing a timeline for an offence:* Call and text messaging logs, SMS, user account information, notes, reminders, calendar, e-mails, WhatsApp, Facebook, Twitter, photos, contact, internet protocol address, etc.

(ii) *Data establishing a participant's degree of culpability and knowledge of an offence:* Multimedia posts, chat and instant messaging, e-mails, internet browsing history, internet protocol address, access to dictionary information, etc.

(iii) *Data establishing the planning, design and commission of an offence:* media-related posts including photos, video, audio, internet browsing history and specific files which contain relevant information about the facts-in-issue of an offence, etc.

(iv) *Data connecting a smartphone user to a particular offence:* GPS, Wi-Fi, Bluetooth, other synchronising logs, location sharing apps such as Facebook, Snap Chat, etc.

The Cybercrimes Act is intended to provide the cyber-tools for combatting cyber-offences but refers in ss 29(1)(*a*)-(5), 30(5)(*a*) through to s 33 to a written *ex parte* application, with attached written

https://doi.org/10.47348/SACJ/v36/i2a3

affidavits, before a judicial officer and the issue of a written search warrant. Ironically, the Act does not make provision for an online application process and online hearing before a judicial officer in chambers. Also, s 27 states that the Criminal Procedure Act applies to the chapter 4 warrant procedures of the Cybercrimes Act. However, chapter 4 makes no specific reference to the applicability of other relevant Acts such as the South African Police Act and the National Prosecuting Authority Act. This article also makes the argument that the traditional principle of intelligibility (including its sub-elements of particularity and specificity) must be materially amended to take into account the technologically complex and materially different types of seizure and search techniques required for accessing and preserving relevant smartphone data. Finally, much of this article's content about smartphone seizure, access and search procedures applies equally to a computer or a laptop. In many of the warrant procedures set out above the word smartphone may be replaced with the word computer without losing legal coherency.

https://doi.org/10.47348/SACJ/v36/i2a3

www.juta.co.za

SAJCJ0091

juta