

https://dspace.org/

State compulsion of smartphone security features and the privilege against selfincrimination

Constantine Theophilopoulos

https://hdl.handle.net/10539/39710
DHET

Downloaded from a DSpace repository. https://dspace.org/

VOL 36 NO 2 2023

SOUTH AFRICAN JOURNAL OF CRIMINAL JUSTICE

TABLE OF CONTENTS

ARTICLES

VC Mlomo-Ndlovu and WFM Luyt Bed space management as a strategy for managing overcrowding in the corrections environment in South Africa **169**

Ntokozo Mnyandu Are we there yet? A look at the remaining questions on physician-assisted suicide and physician-administered euthanasias **203**

Constantine Theophilopoulos Cyber-warrant searches and the admissibility of seized smartphone data evidence at trial **228**

Brent Willock Psychoanalytic psychology, sleep medicine, and the law: Scientifically reviewing Oscar Pistorius' culpable homicide/murder conviction **250**

Constantine Theophilopoulos State compulsion of smartphone security features and the privilege against self-incrimination **282**

RECENT CASES

Adriaan Anderson General principles and specific offences **304**

Pieter du Toit Criminal procedure **317**

Jo-Marí Visser Law of evidence **329**

Annette Van der Merwe Sentencing **341**

Table of Contents

ARTICLES

Bed space management as a strategy for managing overcrowding in the corrections environment in South Africa
VC Mlomo-Ndlovu and WFM Luyt 169

Are we there yet? A look at the remaining questions on physician-assisted suicide and physician-administered euthanasia
Ntokozo Mnyandu 203

Cyber-warrant searches and the admissibility of seized smartphone data evidence at trial
Constantine Theophilopoulos 228

Psychoanalytic psychology, sleep medicine, and the law: Scientifically reviewing Oscar Pistorius' culpable homicide/murder conviction
Brent Willock 250

State compulsion of smartphone security features and the privilege against self-incrimination
Constantine Theophilopoulos 282

RECENT CASES

General principles and specific offences
Adriaan Anderson 304

Criminal procedure
Pieter du Toit 317

Law of evidence
Jo-Marí Visser 329

Sentencing
Annette Van der Merwe 341

Letter to the editor 361

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

EDITORIAL TEAM

SV HOCTOR
Editor-in-Chief
Professor of Law
Stellenbosch University

W FREEDMAN
Professor of Law
University of KwaZulu-Natal

R KUHN
Editorial Assistant
University of KwaZulu-Natal

EDITORIAL BOARD

PJ SCHWIKKARD
Professor of Law at the University of Cape Town

GP KEMP
Professor of Law at the University of the West of England

D VAN ZYL SMIT
Professor of International and Comparative Penal Law at the University of Nottingham

E VAN DER SPUY
Emeritus Associate Professor in Criminology at the University of Cape Town

M REDDI
Acting Deputy Vice Chancellor and Head of College of Law and Management Studies and Professor of Law at the University of KwaZulu-Natal

A KLIP
Professor of Criminal Law and Criminology at Maastricht University

SS TERBLANCHE
Honorary Professor of Law at the University of KwaZulu-Natal

D CHIRWA
Dean and Professor of Law at the University of Cape Town

G WERLE
Professor of German and International Criminal Law and Procedure at the Humboldt University, Berlin

F JESSBERGER
Professor of Criminal Law, Hamburg

P KOEN
Judge of the High Court of South Africa, KwaZulu-Natal Division

VM PONNAN
Judge of Appeal, Supreme Court of Appeal of South Africa

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.

State compulsion of smartphone security features and the privilege against self-incrimination

CONSTANTINE THEOPHILOPOULOS*

ABSTRACT

There is currently a lacuna in statutory and case law about the legal nexus between smartphone technology in the form of password/code or biometric-locked smartphone security features and the privilege against self-incrimination. This paper examines whether a recipient of a cyber-warrant, subpoena, or other compelling order, may invoke the privilege against self-incrimination in the face of a state order compelling the production of a security feature in order to unlock a smartphone and forensically access stored incriminating data files as admissible relevant evidence at trial. This paper examines the legal nexus by critical reference to relevant South African legislation, comparative international law, the Fifth Amendment privilege, and the foregone conclusion doctrine as described by the USA Supreme Court in *Fisher v United States, Hubbell v United States* and other federal courts.

1 Introduction

A smartphone contains a critical amount of personal information stored and filed as data messages in its various infrastructure data caches. Automatic built-in applications such as voice and video calling, photo storage, SMS text messaging, including voluntarily uploaded applications such as Facebook, Telegram, Instagram, WhatsApp, X and TikTok to name a few, can store a lifetime's worth of personal information which define a person's personality, business habits and social interactions with family, friends, and others. A criminal suspect's smartphone is likely to contain easily identified relevant data evidence in the form of data messages and metadata linking a suspect to a

* 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/i2a5

possible crime.[1] Therefore, a police investigation may target a suspect's smartphone via a search cyber-warrant, an interception warrant, or a decryption direction and a prosecutor may subpoena a witness to appear and give oral evidence about the stored data contents of a smartphone at trial. A prosecutor may also, via a subpoena *duces tecum,* compel a witness to produce at trial relevant data messages in the form of data files downloaded from a smartphone in the witness's possession or control. The two principal issues to be analysed in this article are (a) whether the state may compel the disclosure of a password/code, or biometric feature, to seize, access, search and preserve data messages, stored in a suspect's smartphone or on a service provider server, during a police investigation.[2] Alternatively, may the state compel a subpoenaed witness to unlock security protected relevant private data files and produce such unlocked data files at a criminal trial, and (b) what legal defences may a suspect, accused, or witness employ in preventing the state from compelling access to locked data files stored on a smartphone relevant to the *facta probantia* of a criminal charge.

A designated police official is statutorily entitled to target, search, seize, access, or intercept relevant smartphone data and/or metadata.[3] In addition, a designated official may compel the disclosure of a decryption key in order to access security protected smartphone data or use forensic software tools to break security features which protect access to data files stored on a smartphone's storage mediums.[4] However, with new generation smartphones it is becoming increasingly difficult to bypass complex key encrypted or complex password/code-protected data files. It may also be procedurally costly, and

---

1 *Riley v California* 573 US 373 (2014) at 375, 394-395, 'a smartphone 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'.

2 Password or passcode: may be defined as a smartphone security feature consisting of a random combination of either numbers, letters, or symbols. Biometric data: a digital feature which measures a unique physical characteristic such as a fingerprint or recognises a specific facial feature or an iris scan.

3 Sections 81-83 of the Electronic Communications and Transactions Act 25 of 2002; s 25 read with s 29 of the Cybercrimes Act 19 of 2020.

4 Sections 29(2)(*b*) and 37(2)(*a*) of the Cybercrimes Act 19 of 2020, forensic access and analysis of a password/code or encryption key locked smartphone involve, (i) forensically unlocking, breaking, or bypassing smartphone security locking features where possible, noting that for many key encrypted digital devices it may prove impossible to break the encryption in order to access relevant data, (ii) making a duplicate copy (i.e. an image mirror copy) of the original seized hard drive, and (iii) analysing the data content of the duplicate copy to identify the relevant data evidence.

https://doi.org/10.47348/SACJ/v36/i2a5

time consuming, to seize and preserve smartphone data files for the following reasons:

(i) It may be procedurally difficult to obtain specific data and metadata 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.[5]
(ii) Where such data is stored for any length of time, it is usually stored on cloud servers situated in multiple foreign jurisdictions. Timeous access to a foreign servicer is time consuming and costly.[6]
(iii) In practice, the state is usually obliged to first seize an individual's smartphone in order to access its stored data.[7]
(iv) A further complication is that some older generation smartphones (i.e. including starter pack phones) usually have a limited storage space and users on a regular basis manually delete data files and applications to free up storage space. Some smartphones have a default setting for automatic deletion of old text messages after a certain period.

For these practical procedural reasons, it is often difficult for the state in issuing a subpoena or a cyber-warrant, to show with reasonable particularity, in terms of a revised principle of cyber-intelligibility,[8] that text messages and other stored data still exist and are located on the suspect's smartphone or on a service provider's server.

The state compulsion of personal and private written information as relevant admissible evidence for the purpose of a criminal prosecution implicates a number of fundamental due process procedural rights,

[5] Sections 41-43 of the Cybercrimes Act 19 of 2020 permit (i) a state issued expedited preservation of data direction, (ii) a formally written preservation of evidence data direction, or (iii) an oral request for a direction based on urgency. Data targeted by any of these directions may be preserved for a maximum period of 90 days.

[6] Chapter 5 read with s 51 of the Cybercrimes Act 19 of 2020 sets out a complex and time-consuming procedural mechanism for making an access and seizure of data request to a foreign state. Data may well have been deleted or key encrypted before the successful completion of the foreign request procedures.

[7] Sections 29-33 and 41-44 Cybercrimes Act 19 of 2020, a cyber-warrant requires several procedural steps, (i) seizure of the physical cyber-article, (ii) access and search of the stored data contained in the smartphone's storage mediums and apps, (iii) an on-site or off-site forensic analysis of the seized data and (iv) properly preserving the seized cyber-article and its relevant data.

[8] See C Theophilopoulos 'Cyber-warrants searches and the admissibility of seized smartphone data evidence at trial' this issue 2 of *SACJ* 2023 at 228; *Goqwana v Minister of Safety and Security NO* 2016 (1) SACR 384 (SCA) paras [13] & [30]; *Oosthuizen v Magistrate, Hermanus* 2021 (1) SACR 278 (WCC) t paras [39] & [43], the objective test of cyber-intelligibility requires that a valid cyber-warrant targeting a smartphone must be drafted clearly and with due cyber-offence particularity and data access specificity.

https://doi.org/10.47348/SACJ/36/i2a5

namely, a suspect's s 14 constitutional right to privacy,[9] an accused's s 35(1)(*c*) and 35(3)(*j*) constitutional right against self-incrimination,[10] and a witness's statutory privilege against self-incrimination as defined in s 203 of the Criminal Procedure Act (hereafter the privilege).[11] This article is primarily concerned with the witness's or accused's invocation of the privilege, or right against self-incrimination, as a defence against the state's attempt to compel the production of a password, passcode, or biometric locking feature, which prevents a third party's access to the data located in a smartphone's storage hard drive. The physical attachment of a suspect's smartphone and other data storage devices by the police as a consequence of a validly issued search warrant raises the question of whether the search amounts to a reasonable infringement of a named suspect's right to privacy. A search warrant invokes specific procedural issues of scope central to the right of privacy, whereas a validly issued subpoena, or decryption direction, raises the question about its procedural or substantive relationship to a witness's right against self-incrimination.

This article is not concerned with the substantive right to privacy, except where privacy interests influence the privilege, and is instead narrowly focused on the procedural nature of the right against self-incrimination and its legal effect on the state's compulsion of smartphone data and metadata.[12] In particular, whether a witness or a suspect raise the defence of privilege when the state attempts to compel the production of password/code or biometrically locked private data files stored on a smartphone which contains incriminating data content by way of (i) a subpoena *duces tecum*, (ii) a warrant of seizure and

[9] Section 14, 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.

[10] Section 35(1)(*c*) and 35(3)(*j*) of the 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.

[11] Section 203 of the 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.

[12] Section 34(1) of the Cybercrimes Act 19 of 2020 states that any juristic entity or person, *other than the person who is suspected of having committed the offence*, who refuses to assist a police official during a warrant search shall be guilty of an offence. The exception in italics may be interpreted to cover a possible invocation of the privilege by a suspect; s 29(3) of the National Prosecuting Authority Act 32 of 1998, no seized evidence or information shall be admitted at a subsequent criminal proceeding against a person whose answers will incriminate him or her.

https://doi.org/10.47348/SACJ/v36/i2a5

search,[13] or interception warrant,[14] and (iii) a decryption direction.[15] According to this author, there is presently a jurisprudential lacuna in this area of South African procedural and adjective evidence law which may be validly filled by reference to comparative international law and a suitably modified application of the United States Supreme Court's interpretation of the 'foregone conclusion' doctrine.

2 The nature of a data message stored in a smartphone's data files

Section 1 'the definition clause' of the Electronic Communications and Transmissions Act,[16] defines any digital or binary-based representation of information as 'data'; and when data is generated, sent, received, or stored by electronic means it is converted into a 'data message'. A communication made by way of a data message is referred to as an 'electronic communication'. The system by which a data message is generated, communicated, stored, displayed, or processed is characterised as an 'information system'.[17] In other words, an 'originator' (i.e. the smartphone operator) is a person who generates or sends a data message and an 'addressee' (i.e. the recipient of a smartphone call, video or message) is the person intended to receive the data message sent by the originator. A smartphone originator may attach to, incorporate in, or associate an 'electronic signature', a 'digital photo' or 'social media video' with a data message. For the purpose of this article and paraphrasing s 1 – a data-file (containing various data documents including data forms of videos, photos or text messages) may be defined as evidence in the form of a data message when it is generated, sent or received by a smartphone and subsequently either automatically or manually stored in its digital format in a smartphone.

[13] See the warrant procedures in s 29 of the Cybercrimes Act 19 of 2020 and s 83 of the Electronic Communications and Transmissions Act 25 of 2002. See also ss 21-29 of the Criminal Procedure Act 51 of 1977; s 29 of the National Prosecuting Authority Act 32 of 1998.

[14] Section 40 of the Cybercrimes Act 19 of 2020 read with ss 1, 16(4) and 18(3) of the Regulation of Interception of Communications and Provisions of Communication-related Information Act 70 of 2002, permits a third party to intercept, monitor, view, or divert any real-time telecommunication by way of an interception device.

[15] Section 1 read with s 29 of the Regulation of Interception of Communications and Provisions of Communication-related Information Act 70 of 2002, a decryption direction compels a decryption key holder to disclose a decryption key in his/her possession to allow access to encrypted data on a smartphone.

[16] Section 1 of the Electronic Communications and Transmission Act 25 of 2002.

[17] Section 1 of the Cybercrimes Act 19 of 2020, an information system or 'computer system' consists of two or more inter-connected computers able to exchange data and other functions with each other and other computer systems. According to this definition a smartphone is essentially a portable minicomputer.

https://doi.org/10.47348/SACJ/36/i2a5

According to the author an evidentiary useful definition of a data file, as it is stored on a smartphone and accessed by a smartphone originator (i.e. operator) during the commission of a cybercrime, may be summarised as:[18]

> 'digital data contained in the form of a data message, generated by a smartphone originator, as input, by means of a computer information system (i.e. a programmable digital data processing device)[19] operating a software programme capable of creating, storing,[20] and reading a data message, through a person's senses, and which is communicated to a smartphone addressee as output, and which may be produced at trial in the form of an accurate data document, graphics or pictorial visual display, audio recording, or a written printout'.

The high court in *Ndlovu v Minister of Correctional Services*,[21] has adopted an unimaginative and traditional approach to the statutory admissibility and evaluation of a data file as admissible evidence which is predicated on the principle that a data file in the form of a data message is the functional equivalent of a written paper-based document. This means that a data file stored in a smartphone data storage medium is admissible as evidence at a criminal trial when it is relevant (i.e. when its degree of probative value outweighs any procedural prejudice, costs, or time-consuming legal or technological collateral issues which may arise as a result of its reception). Where the data file is being admitted at trial as an item of real evidence then a party need only establish relevance.[22] However, where the data file is being admitted for the evidentiary purpose of proving the truth of the information content of the data message then in order to admit the information content of a data document at trial (*in casu*

[18] See C Theophilopoulos 'The admissibility of data, data messages and electronic documents at trial' (2015) 3 *TSAR* 461 at 463.

[19] Section 1 of the Regulation of Interception of Communications and Provisions of Communication-related Information Act 70 of 2002, the word 'device' may be interpreted to mean a cellular phone capable of connection to a telecommunication network which is used by a customer to transmit or receive indirect communications over such network.

[20] A data document may be stored on a hard drive or in the cloud – although the Cybercrimes Act and the Electronic Communications and Transmissions Act makes no mention of cloud storage.

[21] *Ndlovu v Minister of Correctional Services* [2006] 4 All SA 165 (W) 171; the Electronic Communications and Transmissions Act is wide-ranging in its treatment of electronic information, and its aim is to place electronic evidence on the same footing as traditional paper-based transactions. See also *S v Ndiki* 2008 (2) SACR 252 (Ck); *LA Consortium & Vending v MTN Service Provider* 2011 (4) SA 577 (GSJ) at para [19].

[22] A data document may be admitted as real evidence, (i) to prove the existence of the data document, or (ii) to admit automatically generated data which does not require the input of a human mind.

https://doi.org/10.47348/SACJ/v36/i2a5

– in the form of a computer generated printout) the three traditional evidentiary requirements of a written paper document must be met. These three evidentiary requirements are (i) relevance (ii) originality and (iii) integrity (i.e. authenticity) as defined in ss 12 through 15 of the Electronic Communications and Transactions Act.[23] It may well be argued that the common law evidentiary relationship between the privilege and a pre-existing written document will materially influence the developing cyber relationship between the privilege and a data document contained in a data file stored on a smartphone's hard drive storage medium.

3 State compulsion and the privilege

3.1 Prohibiting the state compulsion of incriminating evidentiary facts (the substantive and procedural scope of the privilege)

The statutory privilege has been interpreted as a fundamental procedural protection for a witness during cross-examination,[24] and as a necessary protection for a witness's freedom, dignity, and privacy during trial proceedings,[25] an interpretation which mirrors that of the accused's right to silence as an entrenched fundamental constitutional right. Accordingly, the principal jurisprudential justification for the privilege is as a procedural protection for a witness, first, as a shield against state coercion/compulsion of an involuntary admission or confession and secondly, as a legal guarantee ensuring a fair adversarial balance during examination-in-chief and cross-examination at trial. In theory, the privilege should apply to all compulsory state processes which seek to induce any manner of incriminating testimony from a witness. However, in practice the privilege has been subjected to a steady erosion in both its procedural scope and its evidentiary application on the rationale that the public interest in ensuring a fair legal proceeding is, '[ ] best served by narrowly limiting the circumstances in which information relevant to litigation may be lawfully withheld. Justice

[23] *Ndlovu v Minister of Correctional Services* supra (n21) at 172-3.

[24] *S v Botha (2)* 1995 (2) SACR 605 (W) at 609c; *Rio Tinto Zinc Corp v Westinghouse Electric Corp* (1978) 1 All ER 434 (HL) at 464; *R v P(MB)* [1994] 1 SCR 555 at 579, the privilege may be invoked whenever an individual in civil or criminal proceedings is required to answer self-incriminatory questions under a legal compulsion.

[25] *Pyneboard Pty Ltd v Trade Practices Commission* (1983) 57 ALJR 236 at 243, the privilege has been constitutionally entrenched in the Fifth Amendment of the United States Constitution; in s 7 read with ss 11(c) and 13 of the Canadian Charter of Rights and Freedoms; art 6(1) of the European Convention on Human Rights. See also ss 25(d) and 27(1) of the Bill of Rights Act 109 of 1990 (New Zealand).

https://doi.org/10.47348/SACJ/36/i2a5

is better served by candour than by suppression [*as amended*]'.[26] A primary theme of this article is to critically examine whether a similar reasonable limitation may be applied to the privilege in respect to the state's compulsion of relevant private incriminatory information in the form of a data document or data file stored on a witness's password locked smartphone. The privilege is a twofold abstract procedural and evidentiary principle, first it explains the procedural limits of a witness's refusal to cooperate with the state, and secondly it provides the witness with a shield against the compulsion of relevant and admissible self-incriminatory evidence. The privilege has also been narrowly construed to apply only to communicative or testimonial oral self-incriminatory evidence. Non-testimonial incriminating evidence and all other procedures for collecting this type of evidence fall outside the privilege's protection.[27] The testimonial versus non-testimonial divide is a critical pivot point in the various arguments for and against the application of the privilege to password or biometric protected data documents stored on a smartphone or other digital storage device or server.[28]

Essentially the privilege may be claimed by any witness appearing in the witness box as a result of a validly issued and served subpoena, or subpoena *duces tecum,* in both civil and criminal proceedings.[29] The privilege must be expressly invoked on a question-by-question basis by the witness or the witness's legal representative.[30] The privilege is not a general privilege against all incriminatory types of questioning, it is a personal and specific privilege invoked as a defence in the face of state inspired questions which require a self-incriminating oral answer and which may place the witness at risk of a possible criminal charge. The witness may not rely on the privilege to protect against answers which tend to incriminate a third party.[31] In the seminal case *Ferreira v Levin;*

[26] *Waugh v British Railways Board* [1980] AC 521 (HL).

[27] See C Theophilopoulos 'The privilege against self-incrimination and the distinction between testimonial and non-testimonial evidence' (2010) 127 *SALJ* 107 at 120.

[28] See C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 461- 481.

[29] *Rio Tinto Zinc Corp v Westinghouse Electric Corp* (1978) AC 547 at 573, per Lord Denning, who attempted to draw a distinction between a witness and a party to a civil suit, but the current English position remains unaltered, namely, that both a witness and a party are entitled to the privilege.

[30] *Waddell v Eyles and Welsh* 1939 TPD 198; *Magmoed v Janse van Rensburg* 1993 (1) SA 777 (A) at 104c; *Spokes v Grosvenor Hotel Co* [1897] 2 QB 124; *Warman International Ltd v Envirotech (Aust) Pty Ltd* (1986) 67 ALR 253 at 265; *Serves v France* (1999) 28 EHRR 265 para 47. See also C Theophilopoulos 'Defining the limits of the common law, South African and European Privilege against self-incrimination' (2014) 25 *Stell LR* 160-186.

[31] *Tate Access Floors Inc v Boswell* [1991] Ch 512.

https://doi.org/10.47348/SACJ/v36/i2a5

Vryenhoek v Powell NO,[32] the Constitutional Court held that compelled self-incriminatory oral evidence obtained from an examinee during the course of a legal proceeding (*in casu* an insolvency inquiry) could not be adduced in a subsequent criminal trial, otherwise it would amount to an unjustifiable infringement of the right to a fair trial entrenched in s 35(3) of the Constitution.[33] According to *Ferreira* whether the state may make derivative evidentiary use of incriminatory facts (cherry-picked from the compelled testimony of a subpoenaed examinee in a quasi-judicial proceeding) at a subsequent criminal proceeding is subject to a court's discretion. This discretion is exercised on the merits of each individual circumstance and examined against the standard of a constitutional commitment to a fair trial.[34] In particular the court's discretion has to be exercised, first by balancing the individual's privilege not to disclose self-incriminatory evidence against the state's legitimate need for such evidence (i.e. an argument based on a public policy consideration). Secondly, by taking into account the differences between (i) circumstances where such evidence would have been identified by other alternative means, and circumstances where it would not,[35] and (ii) the difference between incriminatory physical evidence (i.e. real evidence) to which the privilege does not attach and compelled oral evidence conscripted from a witness (i.e. testimonial evidence) where a witness has been forced to utter self-incriminatory evidence (as opposed to merely locating or identifying it).[36] This article is concerned primarily with the second point and will critically evaluate the procedural relationship between the state's attempt to compel incriminating data files stored on a user's smartphone and the invocation of the privilege by a user targeted by a compelling order. The Constitutional Court did not expressly state whether the privilege may be invoked by a subpoenaed witness in respect to pre-existing written private documents containing incriminating content. Similarly, no subsequent South African superior court has ruled on the relationship between the privilege and a pre-existing data message containing incriminating data content. Therefore, guidance may be sought in existing USA jurisprudence where the Supreme Court has specifically dealt with this issue. Reference to USA precedent on this issue is pertinent as federal and circuit judicial interpretations of the

[32] *Ferreira v Levin; Vryenhoek v Powell NO* 1996 (1) SA 984 (CC).

[33] *Ferreira v Levin; Vryenhoek v Powell NO* supra (n32) at paras [92], [96], [114], [121], [157] and [159].

[34] *Ferreira v Levin; Vryenhoek v Powell NO* supra (n32) at para [153]; *see also Parbhoo v Getz NO* 1997 (4) SA 1095 (CC) at 10-11.

[35] *Ferreira v Levin; Vryenhoek v Powell NO* supra (n32) at para [112].

[36] *Ferreira v Levin; Vryenhoek v Powell NO* supra (n32) at para [136].

https://doi.org/10.47348/SACJ/36/i2a5

Fifth Amendment have previously served as persuasive precedent for South African courts.[37]

3.2 Defining the evidentiary divide between testimonial and non-testimonial incriminating facts

There are several substantive differences in the manner in which the core requirements of the privilege are applied to the admissibility of written incriminating documents as relevant evidence by Anglo-American adversarial jurisdictions. For example, the English common law makes no distinction between self-incriminatory communications in an oral or written form. In *Rank Film Distributors Ltd v Video Information Centre*,[38] the House of Lords unambiguously held that a defendant could invoke the privilege against a validly issued court order (*in casu* – an Anton Piller search and attach order) which sought the disclosure and production of certain specified incriminating private documents. However, under the precedent set out by the European Court of Human Rights in *Saunders v United Kingdom*,[39] the present English approach has been amended to exclude the privilege from all pre-existing incriminating private documents which have not been coerced against the will of the individual. (Although it is worth noting that since 'Brexit' the UK has also excluded the appeal jurisdiction of the European Court of Human Rights and may well revert to its former common law position.) In *C Plc v P*,[40] the Court of Appeal reached two conclusions, first that the principal justification for the privilege was to prevent a witness from making oral self-incriminatory admissions, or dubious confessions, under compulsion during criminal proceedings, and secondly that logically the privilege could not apply to a subpoena in civil proceedings which compelled the disclosure of independent written incriminating documents that existed prior to the compulsion. In addition, the court applied a balancing test holding that the rights of the public, particularly children (*in causa* the issue being the disclosure of documents containing child pornographic images), were more important than the defendant's right against self-incrimination.

---

[37] See *Ferreira v Levin; Vryenhoek v Powell NO* supra (n32). See also *S v Thebus* 2003 (6) SA 505 (CC) at paras [53]-[55], [91], [97] which makes copious direct and indirect references to American jurisprudence about the Fifth Amendment.

[38] (1982) AC 380.

[39] (1992) 22 EHRR 313 at 337.

[40] [2007] 3 All ER 1034, noting that it would be contradictory to allow a witness to claim a privilege in respect to an incriminating document on the ground that it would expose the witness to a possible criminal charge when the state is free to search and seize the same document for the purpose of prosecuting the offender. Also, the invocation of the privilege would direct the state's attention to the privileged document which could then be seized by way of a disclosure order.

https://doi.org/10.47348/SACJ/v36/i2a5

A right which the defendant could if criminally charged evoke at a subsequent criminal trial.

The Canadian Supreme Court in *R v S (RJ)*,[41] adopted a similar approach to that in *Sanders* and *C Plc v P*, holding that derivative evidence (i.e. including a pre-existing written document) which would not have been obtained, or the evidentiary nature of which could not have been appreciated by the state, but for the testimony of the witness, should be excluded in terms of the privilege (i.e. as defined by s 7 of the Canadian Charter) in the interests of trial fairness. Such derivative evidence, although not created by the witness and therefore not self-incriminating, may become self-incriminatory when it forms part of the prosecution's case because of a prior state compelling order. The South African common law position has been interpreted by *Ex parte Minister of Justice: In re R v Matemba*,[42] as 'the production of documents … by a person ... in response to a subpoena [a *duces tecum* order] … or to other forms of process treating him as a witness… may be refused under the protection of the privilege [as amended]'. The Appellate Division, as it then was, justified the application of the privilege to a pre-existing written document by reasoning,

> '… though the document … be already in existence and not desired to be first written and created as by a testimonial act or utterance of the person in response to the process, still no line can be drawn short of any process which treats him as a witness, because…he would be at any time liable to make oath to the identity or authenticity or origin of the…[document] produced [*as amended*]'.

However, *Dabelstein v Hildebrandt*,[43] held that the grant of an order compelling the production of a pre-existing written document in appropriate circumstances, when tested against the limitation clause of the Constitution,[44] was necessary, proportional, and this type of order served a legitimate purpose in the legal system, provided that adequate safeguards were in place.

Accordingly, this author suggests that *Ferreira*, *Matemba* and *Dabelstein* may be interpreted to establish the following relationship between the privilege and a validly issued court order compelling the production of a pre-existing private written document with incriminating content as evidence:

(i) where an order contains a requirement for a party to 'point out and disclose' incriminating documents, the party may refuse to do

[41] [1995] 1 SCR 451 (SCC).

[42] 1941 AD 75 at 81, per Watermeyer JA.

[43] 1996 (3) SA 42 (C) at 66-67, where a validly issued Anton Piller order was held to be constitutionally valid.

[44] Section 39, Constitution, 1996.

https://doi.org/10.47348/SACJ/36/i2a5

so by invoking the privilege – on the basis that the conduct or act of the pointing out would expose them to a real and appreciable risk of a criminal prosecution;

(ii) whether any evidentiary use may be made of any document identified by a party and discovered as a consequence of a state compelled 'pointing out and disclosure' should be left to the discretion of the judge at a criminal proceeding brought against that party. According to the discretionary test set out by the Constitutional Court in *Ferreira* – a state compulsion to produce self-incriminating evidence, coupled with a direct use immunity agreement, and subject to a judicial discretion to exclude derivative evidence at the criminal trial, would not negate the right to a fair trial.[45]

Even though it requires a degree of interpretation, as suggested above, there is at least some case law about the relationship between the privilege and a court order requiring the compulsory disclosure of a pre-existing incriminating written document. However, the South African courts have yet to decide on the admissibility of a court ordered compelled production of a pre-existing incriminating private data document, contained in a data file, or as a data message, stored on the hard drive of a smartphone.

4 The privilege and password or biometric-protected stored data on a smartphone

4.1 The 'act of production' principle

The 'act of production' principle as a foundational element of the foregone conclusion doctrine was originally developed by the USA Supreme Court in *Fisher v United States*,[46] in the limited circumstance where a witness invoked the Fifth Amendment privilege,[47] as a procedural defence in justifying a refusal to disclose a pre-existing written private document (*in casu* – an accounting document relevant to a tax assessment) with incriminating content in the face of a state subpoena.[48] The *Fisher* foregone conclusion doctrine is based on the notion that the privilege does not attach to the incriminating content of a pre-existing document - but that in certain factual circumstances the privilege may attach to a compelled act of producing the pre-existing

[45] *Ferreira v Levin; Vryenhoek v Powell NO* supra (n32) at para [153] per Ackermann J.

[46] *Fisher v United States* 425 US 391 (1976).

[47] USA Constitution, Fifth Amendment: no person shall be compelled in any criminal case to be a witness against himself. See also the similar wording of s 35(3) Constitution,1996, and s 203 of the Criminal Procedure Act 51 of 1977.

[48] *Fisher v United States* supra (n46) at 391- 395, 411.

https://doi.org/10.47348/SACJ/v36/i2a5

document in response to a subpoena or other compulsory warrant. In particular, a compelled act of producing a pre-existing document is testimonial when it requires the recipient of a subpoena to testify to the existence, possession, and the authenticity of the pre-existing document. On the other hand, a compelled act of production is not testimonial when the state can prove that at the time of the compelled act of production it already knew, with reasonable certainty, of the existence and the location of the pre-existing document (i.e. as a foregone conclusion).[49] Essentially, when the state can prove it knew of the pre-existing document as a foregone conclusion at the time of the subpoena's issue, the suspect would merely be surrendering a pre-existing document but where the state could not prove it knew of the document's location or existence, the subpoena is merely a procedurally invalid fishing expedition, and the suspect's forced disclosure of the pre-existing document would amount to a testimonial act.[50] The 'act of production' principle is dependent on a nuanced distinction being drawn between a compelled non-testimonial act (to which the privilege does not attach) and a compelled testimonial act (to which the privilege attaches).

It is trite adversarial law that the state may compel the production of real or physical evidence and other non-testimonial incriminating evidence, but not a testimonial (i.e. oral) incriminating statement to which the privilege attaches.[51] For example, the privilege is not a legal defence against a state compulsion to provide a physical fingerprint, DNA sample, or to seize a smartphone, computer drive, or other digital device. The privilege is a legal defence against a state compulsion of an involuntary admission, confession, pointing out or other oral incriminating statements. With respect to pre-existing incriminating private data the American courts have had to creatively determine the procedural extent to which the Fifth Amendment privilege applies to protect a smartphone user from being compelled to produce, as evidence at trial, private incriminating data stored on a security-protected smartphone in daily use. The South African substantive and procedural lacuna about the legal nexus between a smartphone and the privilege is additionally complicated by a burgeoning security industry based on developing complex password and biometric protections for

[49] *Fisher v United States* supra (n46) at 411-412.

[50] *Fisher v United States* supra (n46) at 411, 'where the existence and location of the pre-existing incriminating papers are a foregone conclusion, the recipient of a state summons adds nothing to the sum of the state case by conceding that he/she has the papers'.

[51] *Minister of Safety and Security v Xaba* 2004 (1) SACR 149 (D); *Minister of Safety and Security v Gaqa* 2002 (1) SACR 654 (C); *S v Huma (2)* 1995 (2) SACR 411 (W) 416-149, the rights to privacy, dignity, and the right not to give self-incriminating evidence are not violated by the taking of non-communicative and passive body samples.

https://doi.org/10.47348/SACJ/36/i2a5

private data documents stored on a smartphone or in the cloud. These technologically complex security features have now reached a modern stage in development where it is becoming increasingly difficult to unlock or bypass a protected smartphone in order to seize, access and search relevant data as evidence, even with the use of forensic software specifically designed for this purpose.[52]

4.2 The *Hubbell* key-combination comparison

In *Doe v United States*,[53] (dissenting) and subsequently in *United States v Hubbell*[54] (for the majority), Supreme Court Justice Stevens developed a wall-safe analogy for determining whether, or not, a *Fisher*-defined act of compelling the production of a pre-existing incriminating document amounted to a non-testimonial or a testimonial act. Justice Sevens held that in certain circumstances a suspect's compelled act of producing a pre-existing document has testimonial implications.[55] He justified this ruling by arguing that a suspect may be legally compelled to surrender a key to a locked wall safe containing incriminating pre-existing documents as the compelled act of producing the key amounts to a simple physical act of reaching into a pocket and handing over the key to a law enforcement officer. The physical act of handing over the key is non-testimonial and does not implicate the Fifth Amendment privilege as it does not require a suspect to disclose their thoughts or the content of the mind. However, where a wall safe containing incriminating documents is manually or digitally protected by a combination password, a compelled act forcing a suspect to disclose the combination amounts to a testimonial communication. The compelled act of disclosing a combination password, verbally, or by deed, amounts to a forced disclosure of a suspect's own mind and thoughts and is testimonial in nature.[56] Justice Stevens also held that the Fifth Amendment privilege attaches to the act of producing a combination password because it compels a suspect to use their mind to assist the state in their prosecution.[57] The issue addressed in paragraph 4.3 below is whether, or not, *Fisher's* act of production principle, and

[52] Some modern smartphones contain an auto-lock function. For example, an Apple iPhone has an auto-lock feature which activates after five failed biometric scans. In some circumstances the police may be tempted to force or trick a suspect into taking a biometric scan, or even use the fingerprints of a deceased person to access a phone before it auto-locks.

[53] 487 US 201 (1988) at 203-204, the respondent invoked the privilege when subpoenaed about the existence and location of foreign bank accounts.

[54] 530 US 27 (2000) at 36-43.

[55] *United States v Hubbell* supra (n54) at 29-43.

[56] *Doe v United States* supra (n53) 219 J Stevens dissenting.

[57] *Doe v United States* supra (n53) at 219-222.

https://doi.org/10.47348/SACJ/v36/i2a5

Justice Seven's wall-safe analogy, may be used to legally justify the invocation of the South African privilege as a defence against the state's attempt (in the form of a validly issued cyber-warrant, subpoena or decryption direction) to bypass a party's locked smartphone security features, in order to seize pre-existing incriminating documents stored on a smartphone application in the form of an data file or other data messages. The issue is also informed by the balance which must be drawn between the state's use of forensic technology to obtain data evidence admissible against an accused at trial and the procedural and other due process rights by which an accused may defend themself.[58]

4.3 Accessing password-protected smartphone content

Two questions must be answered here in order to determine if the South African privilege applies to the compelled disclosure of password-protected incriminating smartphone data content:[59]

(i) Does a suspect's compelled act of producing a security password, or otherwise being forced to unlock a smartphone, in response to a legally issued cyber-warrant, subpoena, or decryption direction, amount to a non-testimonial act or to a testimonial act? In other words, will a South African court find that a compelled disclosure of a security feature by a suspect is analogous to a mere physical surrender of a key, or does it amount to a forced disclosure of the private content of a suspect's mind as protected by s 14 of the Constitution 1996?
(ii) Does a testimonial compelled act of production attract the privilege where the state can prove that the compelled act of producing a password falls within the scope of a suitably amended South African version of the foregone conclusion doctrine?

These two questions may be answered by reference to American circuit and federal court decisions. United States courts at the federal circuit and state level have answered the above two questions by applying

[58] *People v Kramer* 706 N.E.2d (NY 1998) 731 at 734, noting that a person does not tacitly waive their due process rights when using new forms of technology, 'technology cannot be allowed to outpace the array of checks and balances and protections affecting privacy intrusions important to individuals and society at large'.

[59] Provision is made in s 29 of the Regulation of Interception of Communications and Provisions of Communication-related Information Act 70 of 2002 for the state ordered compulsion of a decryption key; s 29(2)(*a*) and s 37(2)(*a*) & (*b*) of the Cybercrimes Act allow a police officer to make use of a decryption key. These sections are badly worded, and no reference is made to any of the constitutional or evidentiary privileges that a encryption key holder may invoke.

https://doi.org/10.47348/SACJ/36/i2a5

an amended *Fisher's* foregone conclusion and/or *Hubbell's* wall-safe analogy to the forced disclosure of a smartphone's security features in terms of a validly issued subpoena or cyber-warrant. In order to do so the US courts have held that a data document is the functional equivalent of a written document.[60] First, if the state wants to legally compel the production of an incriminating data file stored on a smartphone, without attracting the privilege, then it must prove, in terms of the foregone conclusion doctrine, that it knew that the file existed, that the smartphone owner had the file in their possession, and that it can through evidence *aliunde* authenticate the file. Secondly, if the state wants to compel a password in order to access a smartphone, then it must prove the same foregone conclusion elements for the password. At the federal level and in regard to encrypted data documents stored on the hard drive of a laptop, the Eleventh Circuit in *In re Grand Jury Subpoena Duces Tecum*,[61] held that a grand jury subpoena compelling a suspect to decrypt a computer hard drive and produce its incriminating pre-existing data content containing child pornography would amount to a testimonial act triggering the privilege's protection. The court held:

(i) A compelled act of decrypting a key-locked hard drive requires the use by the suspect of the content of their mind which amounts to a testimonial communication as the suspect is forced to disclose their knowledge of the possession, existence, and location of the incriminating data files including the capability to access encrypted portions of the file and to decrypt the same.[62]

(ii) The elements of the foregone conclusion doctrine could not be met, on the unique circumstances of the case, as the state could not prove it knew whether any data files existed on the hard drive, and consequently could also not prove (a) where the data files were stored, (b) whether the suspect could access the data files, and (c) whether the state could authenticate the compelled data files.[63]

The practical consequence of the Eleventh Circuit's decision is that an onerous procedural burden is placed on the state where it intends to

[60] The US and the South African law of evidence on the admissibility of written and electronic documents are similar in jurisprudential meaning. Both apply the traditional adversarial rules of originality, authenticity (or integrity) and in limited circumstances the best evidence rule. The rules applying to a claim of privilege are also similar in substantive content and due process procedure.

[61] *In re Grand Jury Subpoena Duces Tecum [dated March 2011]* 670 F.3d 1335 (11th Circuit 2012). See also *In Re grand Jury Subpoena Duces Tecum [dated April 2003]* 383 F.3d 905 (9th Circuit 2004) at 911.

[62] *In re Grand Jury Subpoena Duces Tecum [dated March 2011]* supra (n61) at 1346-1348.

[63] Ibid.

https://doi.org/10.47348/SACJ/v36/i2a5

admit smartphone data evidence compelled from a suspect. In order to admit such evidence, and to avoid triggering the privilege, the state is obliged to prove with reasonable particularity that it knew, at the time of issuing the subpoena, where the data file evidence was located, that the suspect was in possession of the data file evidence and had the capability of decrypting the password protected data-file.[64] In *Seo v State,*[65] the accused was charged with using her iPhone to stalk and intimidate a victim by sending him hundreds of harassing text messages. The arrested accused refused to provide the investigating officer with her iPhone password. The officer obtained two search warrants, the first to seize and search the smartphone and the second to compel the accused to unlock the phone. The Indiana Supreme Court held that a warrant requiring compulsory disclosure of a password in any form amounted to self-incriminating testimony (applying the logic of *Hubbell's* wall-safe key-combination comparison). The foregone conclusion doctrine did not apply as the state could not prove, on the facts of the case that the incriminating text messages existed or were in the accused's possession. The court also noted in passing that it was unclear whether the foregone conclusion doctrine should be applied to new forms of technology or data evidence stored in a smartphone. The court held further that compelling an accused to unlock a smartphone resulted in an unreasonable infringement of her privacy as it forced her to recreate the contents of her mind.[66]

In *Commonwealth v Davies,*[67] the Pennsylvania Supreme Court adopted a slightly different approach to that of the Eleventh Circuit and the Indiana Supreme Court, by narrowly focussing on the compulsion of a computer password as a data file document, and not on the compulsion of the computer stored data file content. The majority held that logically 'if one is protected from telling an inquisitor the combination to a wall-safe, it is a short step to conclude that one is protected from telling an inquisitor the password to a computer'. The dissent argued that where

[64] The South African principle of intelligibility has its equivalent in the second part of the USA Constitution's Fourth Amendment, 'a warrant shall be issued upon probable cause supported by oath or affirmation, and particularity describing the place to be searched, and the persons, or things to be seized'.

[65] 148 N.E.3d 952 (Ind 2020) at 953-955.

[66] *Seo v State* supra (n65) at 953-957. See also *Commonwealth v Baust* 89 Va. Cir 267 (Va. Cir Crt. 2014) at 55, compelling an accused to disclose his cell phone password amounted to a testimonial communication. The privilege has been equated by the American courts with 'the inviolability of the human personality'; *Murphy v Waterfront Commission* 378 US 52 (1964) at 55; 'a right to a private enclave where the [individual] may lead a private life'; *Miranda v Arizona* 384 US 436, 460 (1966); and is said to protect 'the conscience and dignity of man' *Ullmann v United States* 350 US 422 at 446 (1956).

[67] 220 A.3d 534 (Pa 2019) at 540-548.

https://doi.org/10.47348/SACJ/36/i2a5

the procedural issue is not one of compelling the production of stored computer content as testimonial evidence but rather a question of surrender – an order compelling a defendant to surrender a password does not usually require the defendant to involuntarily speak their guilt. The mere fact that a defendant must think in order to complete the compelled act of surrendering a password does not amount to an incriminating testimonial communication, nor is it an unreasonable infringement of the defendant's right to digital privacy.[68] In *State v Andrews*,[69] the New Jersey state court also focussed on a passcode as a form of a data document (and not on the stored data-file contents of the smartphone) to which the foregone conclusion doctrine and the *Hubbell* analogue should apply. The foregone conclusion should be applied to the compelled act of producing the password as a pathway to the contents of the smartphone as an end to itself, and not to the act of producing the smartphone content. The court held that a compelled act of producing a passcode was a testimonial act protected by the privilege. However, the testimonial value of the compelled act's and the privilege defence could be overcome, in certain circumstances, if the state could prove that the passcode's existence, possession, and authentication amounted to a foregone conclusion.[70] The court critically noted that focussing on the data file content stored on the smartphone, instead of the passcode itself, would create a problematic evidentiary distinction between smartphones protected by passwords and those protected by biometrics.[71]

4.4 Accessing biometric-protected smartphone data content

Biometric security features are different to password or passcode security locks because they are based on the digital formatting of a person's behavioural, physiological, and anatomical characteristics. A password is stored in an individual's mind (as it requires memory to type it into a phone) and is inherently private whereas biometric data features such as fingerprint, face recognition or iris scans are inherently public as they exist outside of an individual's mind. It is trite law that the state may compel an accused to submit to fingerprinting, DNA and blood sampling, identification parades, speech identification, photographs, body measurements, etc. Consequently, compelling an accused by way of a cyber-warrant to use their physical features to unlock a smartphone

[68] *Commonwealth v Davies* supra (n67) at 553-556.

[69] *State v Andrews* 234 A.3d 1254 (N.J 2020).

[70] *State v Andrews* supra (n69) at 1274.

[71] *State v Andrews* supra (n69) at 1274-1275.

may entirely bypass the privilege, as an act of compelling the use of a physical feature does not amount to a testimonial communication and does not trigger the privilege (applying the *Hubbell* wall-safe analogy – compelling the accused to use their biometric features to unlock a smartphone amounts to a physical non-testimonial surrender of a key and not to a testimonial mental disclosure of a combination password). Several US lower court decisions concerning the validity of vaguely defined warrants of search and seizure, have focussed on the procedures used by the state in compelling an individual to unlock a smartphone. For example, in terms of one such warrant, the state sought to compel four suspects to press their fingers to the fingerprint scanner of seized iPhones in order to unlock the phones. These courts have held that this type of warrant requirement was valid as it only physically compelled a suspect to place their finger on the scanner. This physical act was inherently non-testimonial (amounting merely to a physical surrender of a key to a wall-safe) as it did not require a suspect to communicate any incriminating information to the state.[72] A warrant requirement compelling a suspect to unlock a smartphone by biometric means (either by way of a fingerprint or facial scan) did not compel a suspect to be a witness against himself and therefore did not trigger the privilege.[73]

Alternatively, other lower courts have denied warrants based on compelling biometric access to a smartphone by focussing on a constitutional and due process rights approach. These courts argue that a smartphone stores intimate details of a person's private life. The constitutional rights to dignity, privacy and the due process privilege evolved specifically to prevent unreasonable and unfettered government intrusion into the intimate details of a person's life.[74] These courts have held that both biometrics and passwords have the same functional purpose in securing unwarranted access to a person's private phone.[75] To attach the privilege to the disclosure of a password protection but to deny it to a biometric protection is artificial and legally illogical. Furthermore, the compelled act of physically unlocking a phone by way of biometrics could also be interpreted as a testimonial communicative act as it concedes ownership and control over the

[72] *In Re Search Warrant Application* 279 F. Supp. 3d. 800 (ND. Ill 2017) at 802, 805-807, the fingerprint seizure is just that – the warrant officer seized a finger and applied it to the scanner, and that act does not make use of the content of the suspect's mind.

[73] *In Re Search Warrant Application* supra (n68) at 806 – 807. See also *In Re Search of [redacted] Washington DC* 317 F.Supp.3d. (D.DC 2013) at 526-527, 534-536.

[74] *In Re Search of a Residence in Oakland Ca* 354 F. Supp. 3d 1010 (N.D. Cal 2019) at 1014-1016 noting that citizens do not voluntarily waive their due process rights when using new forms of technology.

[75] *In Re Search of a Residence in Oakland Ca* supra (n74) at 1015-1016.

https://doi.org/10.47348/SACJ/36/i2a5

phone and that the individual is the custodian of the incriminating information stored on the phone.[76] An obvious example would be a lie-detector test which measures a subject's physical response to incriminating questions by monitoring heart rate, blood pressure, and other capillary reactions. This type of test which uses physical characteristics to infer a testimonial response clearly triggers the privilege, although in terms of the South African law of evidence such a biological assessment does not possess admissible evidentiary value.

5 Conclusion

There is presently no South African statutory or case law dealing specifically with the legal nexus between smartphone technology in the form of a password or biometric security feature and the invocation of the privilege in the face of a state-issued cyber-warrant, subpoena, or decryption direction. Section 81(2) and s 82 of the Electronic Communications and Transactions Act,[77] and s 29(1)-(2) of the Cybercrimes Act,[78] refer in broad language to a cyber-inspector, or a designated police official, having the warrant procedural power to 'seize' an article in the form of any information, or computer system, and 'access' and 'use' any instrument, device, equipment, password, decryption key, data, or computer system/programme or storage medium.[79] However, the word 'access' and 'use' in both Acts is written without specifying how such 'access' and 'use' is to be legally construed for the purpose of ensuring the admission of password-protected relevant data evidence at trial, especially in the face of a compelling state order and a consequential defence invocation of the privilege. A South African criminal court's decision for or against extending the privilege protection to password/biometric security technology is ultimately based on achieving a reasonable balance between the due process interests of an individual (i.e. protection of personal privacy data) and the crime control interests of the state (i.e. efficient

[76] *In Re Search of a Residence in Oakland Ca* supra (n74) at 1016. See Theophilopoulos op cit (n27) 120.

[77] Section 81-82 of the Electronic Communications and Transmission Act of 25 of 2002.

[78] Section 29 of the Cybercrimes Act 19 of 2020.

[79] Section 25 of the Cybercrimes Act 19 of 2020 defines 'access' as making use of a computer system to the extent necessary to seize, access and search a cyber-article. To 'seize' means to remove a computer system, to render it inaccessible, to copy data or programs and to retain a printout of such. S 29(2)(*g*)-(*h*) use can be made of any software, data, decryption key, or equipment to search, seize and access a cyber-article identified in a warrant.

https://doi.org/10.47348/SACJ/v36/i2a5

and cost-effective investigation of cybercrimes).[80] In order to reach a reasonable decision any future South African court will have consider the following unique practical and procedural aspects of smartphone technology:

(a) *Will a technological-based security feature be legally defined as a data document?* Clearly a pre-existing incriminating document stored on a data file on a smartphone drive may be properly defined as a data document. May a password or a biometric feature also be defined as a data document? May a state act of compelling the production of a password, or the compulsion or forced use of a biometric feature trigger the privilege?
(b) If a password/biometric feature is legally construed to amount to a data document, will a suitably amended South African version of the *Fisher* foregone conclusion doctrine and/or the *Hubbell* combination-key comparison be applied.
(c) *Privacy concerns will need to be considered*. A smartphone contains a significant amount of internal memory and can potentially store a massive amount of personal information and other data. This data may be stored on a phone's default system (e.g. phone, message, photo message, reminders and notes, etc) or on downloaded apps which contain a combination of voice, text and video features (e.g. Facebook, WhatsApp, Tiktok, X, etc.). A cyber-warrant compelling access to the data contained in a smartphone must ensure that the search protocol is clearly worded, and that access is limited to properly identified data relevant to the facts-in-issue of the criminal offence being investigated. A procedural and due process conundrum is how will a designated police official meet the standard of particularity and specificity (in terms of the principle of cyber-intelligibility), when targeting and seizing relevant data by way of a cyber-warrant when they are denied on-site or even off-site access to a locked smartphone data content?
(d) *Multiple levels of passwords must be considered*. While all smartphones have security features locking access to the entire phone, there are also internal passwords which may lock access to specific applications. A cyber-warrant compelling access to an entire smartphone may also need to include specific reference to these internal passwords.

[80] *Key v Attorney-General, Cape Provincial Division* 1996 (2) SACR 113 (CC) at para [13], the Constitutional Court recognised the tension between crime control and due process interests and cautioned against a rigid adherence to one at the expense of the other; *Goqwana v Minister of Safety and Security NO* supra (n8) at paras [13] & [30], while a compelling order is effective in combatting crime it must be balanced against the significant constitutional rights of personal dignity, privacy freedom and security.

https://doi.org/10.47348/SACJ/36/i2a5

(e) *Deletion and/or uploading of relevant evidentiary data*. While a smartphone contains a large internal memory, it is common for users to delete either manually, or to set for automatic deletion unwanted or incriminating data. In addition, data may be uploaded to key encryption-protected iCloud servers situated in multiple foreign jurisdictions. A cyber-warrant will need to be worded in a manner that specifically recognises these procedural difficulties.

The Supreme Court of Appeal in *Goqwana v Minister of Safety and Security*,[81] held that a search warrant gives the state 'awesome procedural powers' which result in formidable evidentiary consequences. The question to be decided by a future South African court is ultimately founded in the Law of Evidence and may be worded as 'what will be the evidentiary consequence of a refusal by a recipient to obey a lawfully issued cyber-warrant, subpoena, or decryption direction'? In other words, may an evidentiary adverse inference be drawn from the invocation of the privilege against self-incrimination as a defence against the compelled disclosure of a password or biometric feature required by a lawfully issued warrant, subpoena, or decryption direction in order to access incriminating data stored on a smartphone?

[81] *Goqwana v Minister of Safety and Security* supra (n8) at para [30].

https://doi.org/10.47348/SACJ/v36/i2a5

www.juta.co.za

SAJCJ0091

juta