Balancing Law Enforcement Interests and Privacy Rights Under Section 205 of the Criminal Procedure Act

PG du Toit* and M Watney**

Online ISSN 1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Authors

Pieter du Toit
Murdoch Watney

Affiliation

North-West University,
University of Johannesburg,
South Africa

Email

Pieter.dutoit@nwu.ac.za
mwatney@uj.ac.za

Date Submitted

03 March 2025

Date Revised

19 December 2026

Date Accepted

19 December 2026

Date Published

02 February 2026

Editor

Prof Germarié Viljoen

Journal Editor

Prof Wian Erlank

How to cite this contribution

Du Toit PJ and Watney M, "Balancing Law Enforcement Interests and Privacy Rights Under Section 205 of the Criminal Procedure Act" *PER/PELJ* 2026(29) - DOI http://dx.doi.org/10.17159/1727-3781/2026/v29i0a21436

DOI
http://dx.doi.org/10.17159/1727-3781/2026/v29i0a21436

Abstract

Section 205 of the *Criminal Procedure Act* allows a judicial officer to require the attendance before him or her of a person who is likely to give material or relevant information as to any alleged offence. The procedure enables a Director of Public Prosecutions or a duly authorised prosecutor to examine the witness in the presence of the judicial officer to obtain the information. Should the person furnish the information to the satisfaction of the Director of Public Prosecutions or prosecutor before the date of the inquiry, the obligation to appear at the inquiry falls away. The question arises as to whether this procedure offers adequate safeguards to protect against the infringement of a suspect's constitutionally protected right to privacy, especially when so-called historical records, such as financial statements and cell phone records, are handed over to authorities during a criminal investigation. In this contribution it is submitted that the intrusion into private lives of persons is best understood by analogy to search and seizure law, where the right to privacy in criminal investigations is prominently implicated, and the courts have developed specific procedural safeguards. It is argued that section 205 will not present challenges if the requirements for *ex parte* applications are properly adhered to and the rights to dignity and privacy are respected in the application thereof. In addition, the procedure requires proper judicial oversight to determine whether the circumstances warrant a subpoena to be issued.

Keywords

Section 205 of the *Criminal Procedure Act*; search and seizures; privacy; cell phone records; bank statements.

……………………………………………………….

1 Introduction

Section 205 of the *Criminal Procedure Act* 51 of 1977 (hereafter CPA) grants a judicial officer the power to compel the attendance before him or her of a person who is likely to give material or relevant information as to an alleged offence. The section provides as follows:

> 205 (1) A judge of a High Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection (4) and section 15 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, upon the request of a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the Director of Public Prosecutions, require the attendance before him or her or any other judge, regional court magistrate or magistrate, for examination by the Director of Public Prosecutions or the public prosecutor authorized thereto in writing by the Director of Public Prosecutions, of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the Director of Public Prosecutions or public prosecutor concerned prior to the date on which he or she is required to appear before a judge, regional court magistrate or magistrate, he or she shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.
>
> (2) …
>
> (3) The examination of any person under subsection (1) may be conducted in private at any place designated by the judge, regional court magistrate or magistrate.
>
> (4) A person required in terms of subsection (1) to appear before a judge, a regional court magistrate or a magistrate for examination, and who refuses or fails to give the information contemplated in subsection (1), shall not be sentenced to imprisonment as contemplated in section 189 unless the judge, regional court magistrate or magistrate concerned, as the case may be, is also of the opinion that the furnishing of such information is necessary for the administration of justice or the maintenance of law and order.

Although the procedure can be applied to gather information from an uncooperative or reluctant witness, it is frequently utilised to acquire cell phone records from telecommunications companies and financial statements from banks during criminal investigations.[1] Generally these

* Pieter du Toit. B Iur LLB LLM LLD. Professor, Programme for Forensic Accountancy, School for Accounting Sciences, Faculty of Economic and Management Sciences, North-West University (Potchefstroom Campus). E-mail: Pieter.dutoit@nwu.ac.za. ORCID: https://orcid.org/0000-0001-8783-0135.

** Murdoch Watney. BA Law LLB LLM (RAU) LLM (UNISA) Dip E-C Law (TJSL) LLD (RAU). Professor, Department of Public Law, University of Johannesburg. E-mail: mwatney@uj.ac.za. ORCID: https://orcid.org/0000-0002-1406-7623.

institutions are willing to supply the necessary information, provided it is requested through a legal subpoena, as doing so might affect their clients' privacy rights. Records gathered through this method can offer vital evidence against suspects and potentially result in their conviction. Section 205 of the CPA seems to allow subpoenas without adhering to the usual privacy protections required for search and seizure warrants.[2] The procedural safeguards for section 205 subpoenas have been largely developed by way of practice conventions that have been approved by the courts.[3] This article examines the question of whether section 205 appropriately balances the valid interests of law enforcement with the safeguarding of privacy rights, considering that search and seizure warrants are a recognised method of mitigating the impact of privacy breaches by authorities. The analysis focusses on the privacy rights of individuals whose information is obtained through section 205.

The article begins by examining the right to privacy within the scope of criminal investigations in general. Following this, the authors provide a brief discussion on the application of section 205 subpoenas in police investigations, particularly emphasising their relevance in the digital age. Subsequently the article assesses the procedural protections related to section 205 subpoenas, comparing these with the legal principles governing search and seizure warrants. Moreover, the article explores the strength of a suspect's legitimate expectation of privacy concerning historical data, which are typically demanded by a section 205 subpoena. Lastly, the article analyses the potential risks linked to the later use and sharing of information gathered under section 205, questioning if these practices adhere to constitutional limitations. This final point addresses specific concerns about privacy and the boundaries of investigative collaboration.

In *Nel v Le Roux*[4] the Constitutional Court upheld the constitutionality of section 205. Thus, the constitutionality of section 205 is not in question. However, in the *Nel* case the court approached the matter from the perspective of the person who is compelled to provide the information and held that the compulsion to answer questions did not unjustifiably infringe constitutional rights, provided that a "just excuse" existed as provided for in

1 Geldenhuys 2017 *Servamus* 17-18; Geldenhuys 2022 *Servamus* 13; Lochner, Benson and Horne 2012 *Acta Criminologica* 69-80; Lochner and Zinn 2014 *Acta Criminologica* 160-175. *Gcabashe v MTN Group Ltd* (53/2019) [2024] ZAGPPHC 233 (6 March 2024); *Panday v Minister of Police* 2012 2 SACR 421 (KZD); *S v Murphy – Main Judgment* (CC27/2018) [2023] ZAWCHC 186 (12 July 2023).

2 See para 3 below.

3 See para 3 below.

4 *Nel v Le Roux* 1996 3 SA 562 (CC) (hereafter the *Nel* case).

the section.[5] This contribution shifts the focus from the rights of the examinee (the party compelled to provide the information) to the suspect in respect of whom the information is sought. Inadequate safeguards can lead to the exclusion of evidence obtained in violation of the right to privacy.[6]

2 The right to privacy in criminal investigations

Section 205 is an important investigative tool that can infringe the privacy rights of suspects; for example, by exposing their personal finances. It is therefore necessary to briefly examine how our courts view the nature and scope of the right to privacy in the context of criminal investigations. The right to privacy in the context of criminal investigations has most prominently been considered in the context of search and seizure law.[7] As such, this aspect of the criminal procedure provides useful guidance regarding the permissible limits of state intrusion.

In addition to privacy protection at common law, the right to privacy is also guaranteed by section 14 of the *Constitution of the Republic of South Africa* of 1996 (hereafter the *Constitution*).[8] The right to privacy includes the right not to have one's person or home searched; one's property searched; one's possessions seized; or the privacy of one's communications infringed.[9] The Constitutional Court has implemented the two-step test established by the United States Supreme Court to assess if an individual holds a legitimate expectation of privacy regarding searches and seizures.[10] In this test, to exclude evidence after a search a party must prove both a personal expectation of privacy and that this expectation is deemed reasonable by society. Courts will assess if this legitimate privacy expectation is forfeited by considering factors like public exposure, abandonment, or consent in

---

5 *Nel* case paras [5]-[8]. Also see *S v Waite* 1978 3 SA 896 (O) 898E-F, where it was held that an examinee at a section 205 examination is entitled to claim the privilege against self-incrimination.

6 Section 35(5) of the *Constitution of the Republic of South Africa*, 1996 (the *Constitution*) provides: "Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice." See in this regard *Minister for Safety and Security v Van der Merwe* 2011 2 SACR 301 (CC) (hereafter the *Van der Merwe* case); *S v Dos Santos* 2010 2 SACR 382 (SCA).

7 *Van der Merwe* case paras [35]-[42]; Du Toit *et al Commentary on the Criminal Procedure Act* 2-1; Kruger *Hiemstra's Criminal Procedure* 2-7 – 2-11; *Powell v Van der Merwe* 2005 5 SA 62 (SCA) (hereafter the *Powell* case) para [59].

8 Currie and De Waal *Bill of Rights Handbook* 294-296; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit* 2000 2 SACR 349 (CC) (hereafter the *Hyundai* case) para [18].

9 Section 14 of the *Constitution*. Also see Currie and De Waal *Bill of Rights Handbook* 304, 313; *Minister of Police v Kunjana* 2016 2 SACR 473 (CC) (hereafter the *Kunjana* case) para [16].

10 *Bernstein v Bester* 1996 2 SA 751 (CC) (hereafter the *Bernstein* case) para [75], relying on *Katz v US* 389 US 347 (1967) 361 and *Abel v US* 362 US 217 (1960) 241.

obtaining the property in question.[11] Additional factors to consider are the nature of the information itself, the relationship between the party disclosing the information and the party asserting its confidentiality, the location where the information was acquired, the means by which it was obtained and the activity that connects the individual with the state.[12] The right to privacy "becomes more intense the closer it moves to the intimate personal sphere of the life of human beings, and less intense as it moves away from that core."[13] Therefore, whilst legislation permitting warrantless inspections of regulated businesses may be constitutionally acceptable, extending such searches to private homes generally is not.[14] In matters where legislation allowing for warrantless searches of homes without more was declared unconstitutional, the Constitutional Court typically remedied the defect by requiring either a search warrant or allowing a warrantless search if the persons whose rights are affected by the search give consent or if exigent circumstances exist.[15]

This framework for assessing the nature and extent of a person's legitimate expectation of privacy also forms the basis for evaluating the status of individuals from whom information is sought under section 205.[16]

3 Section 205 subpoenas in the digital era

Having considered the contours of the right to privacy in criminal investigations, we turn to section 205 as a tool for use in modern-day criminal investigations. In the pre-constitutional dispensation, section 205 had been widely and controversially employed, particularly to question individuals such as journalists. It was especially used as a mechanism to obtain information about their sources.[17] Questions relating to the use of section 205 subpoenas have become especially pressing in the digital era.[18] The types of information most often sought under section 205, such as subscriber records, location data, and transactional histories from cell

11 *Bernstein* case para [75].

12 *R v Plant* [1993] 3 SCR 281 293 (hereafter the *Plant* case).

13 *Hyundai* case para [18]. Also see the *Bernstein* case para [77].

14 *Magajane v Chairperson, North West Gambling Board* 2006 2 SACR 447 (CC) para [43]; *Gaertner v Minister of Finance* 2014 1 SA 442 (CC) para [35]; the *Kunjana* case para [18].

15 *Magajane v Chairperson, North West Gambling Board* 2006 2 SACR 447 (CC) para [43]; *Gaertner v Minister of Finance* 2014 1 SA 442 (CC) para [35]; the *Kunjana* case para [18].

16 See para 4 below.

17 *S v Miller* 2016 1 SACR 251 (WCC) para 21. For a discussion of the use of s 205 to compel journalists to provide information, see Brand 2006 *Ecquid Novi* 113-135.

18 Geldenhuys 2017 *Servamus* 17-18; Geldenhuys 2022 *Servamus* 13; Lochner, Benson and Horne 2012 *Acta Criminologica* 69-80; Lochner and Zinn 2014 *Acta Criminologica* 160-175. *Gcabashe v MTN Group Ltd* (53/2019) [2024] ZAGPPHC 233 (6 March 2024); *Panday v Minister of Police* 2012 2 SACR 421 (KZD); *S v Murphy – Main Judgment* (CC27/2018) [2023] ZAWCHC 186 (12 July 2023).

phone providers and financial institutions would today qualify as cyber articles in the form of data under the *Cybercrimes Act* (hereafter CCA).[19] Standard Operating Procedures (hereafter referred to as "SOPs") were published in compliance with the requirements of the CCA.[20] The SOPs demonstrate the continued use of section 205 subpoenas in criminal investigations. They emphasise the importance of distinguishing cases where a section 205 subpoena is suitable from those that necessitate a search warrant issued under either the CCA or the CPA.[21]

The use of search warrants issued in terms of the CCA does not replace the role of a section 205 subpoena.[22] In particular, when seeking "historical information" like bank or mobile phone records, section 205 is employed. For instance, to access mobile network records authorities can retrieve data associated with activities that reduced a user's airtime or data balance, including calls or internet usage.[23] Conversely, when it is essential to confiscate cyber articles, obtaining a search warrant under the CCA is required. This type of search focusses on revealing the actual contents of the device rather than just the metadata from service providers. A warrant issued according to the Act allows a skilled expert to extract and analyse data such as emails, text messages, photos, screenshots and voice notes from the device.[24] In other instances where an article does not meet the definition of a cyber article as provided for in the CCA, a search warrant in terms of the CPA must be obtained.[25]

19 In terms of s 1 of the *Cybercrimes Act* 19 of 2020 (CCA), a cyber article essentially includes data linked to the commission of a crime or data that has evidential value and "data" refers to electronic representations of information in any form.

20 Section 26 of the CCA. In terms of this section, the standard operating procedures (SOPs) must be followed by members of the South African Police Service and any individual or agency authorised to investigate offences under the CCA or crimes involving the use of cyber articles. A core objective of these SOPs is to ensure that the collection of evidence during cyber investigations is conducted in accordance with the law with due regard to individuals' rights to privacy and to a fair trial.

21 SAPS 2020 https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf (hereafter SAPS Standard Operating Procedures) para 7.2.1.

22 SAPS Standard Operating Procedures para 7.2.2.1.

23 SAPS Standard Operating Procedures para 7.2.2.1.

24 SAPS Standard Operating Procedures para 7.2.3.1.

25 SAPS Standard Operating Procedures para 7.2.3.2. Ultimately any search, access or seizure involving cyber articles must be assessed based on the specific circumstances of the case. See SAPS Standard Operating Procedures para 7.2.4. For a detailed discussion of the differences between search warrants issued in terms of the CCA and those issued in terms of the *Criminal Procedure Act* 51 of 1977 (CPA), see Du Toit 2002 *Obiter* 764-779.

4 Procedural safeguards for section 205 subpoenas

4.1 The search warrant analogy

Similar to search warrants issued under the CPA and various other laws, section 205 subpoenas are crucial for the police to fulfil their constitutional duties of preventing, combating and investigating crime.[26] This encroachment on individuals' private lives can be likened to search and seizure law, where privacy rights in criminal investigations are significantly involved, and over the years courts have established thorough procedural protections. These protections are designed to minimise the impact of infringing on personal rights.[27] Such a limitation may be achieved by specifying a procedure for the issuing of a search warrant or a subpoena and by reducing the potential for abuse.[28] The Constitutional Court has identified four such safeguards in the context of search warrants: (i) the jurisdictional requirements for issuing warrants; (ii) the significance of vesting the authority to issue warrants in judicial officers (judicial oversight); (iii) the ambit of the terms of the warrants; and (iv) the bases on which a court may set warrants aside.[29]

4.2 Jurisdictional requirements

Regarding the issue of jurisdictional requirements, the person summoned must be "likely to give material or relevant information" regarding an offence. The section does not state if this assessment is the responsibility of the prosecutor requesting the subpoena or of the judicial officer authorising it. It does not indicate whether a mere allegation that the person will probably be able to provide material or relevant information will suffice or whether reasonable grounds for such an allegation must be established.

In *S v De Vries* it was, however, held that “a preferable procedure would be for the investigating officer to set out in an affidavit the grounds on which the subpoena is sought and, if appropriate, identify therein the particular witness statements upon which the application is based.”[30] The court's mention of "a preferable procedure" underscores the ambiguity in the language of section 205. This sharply contrasts with the search warrant provisions under the CPA, which mandate that specific details proving the jurisdictional facts for a search warrant must be presented to the issuing

---

26 *Van der Merwe* case para [35]; s 205 of the *Constitution*.

27 *Van der Merwe* case para [36]; Du Toit *et al Commentary on the Criminal Procedure Act* 2-1; Kruger *Hiemstra's Criminal Procedure* 2-7 – 2-11; *Powell* case para [59].

28 *Van der Merwe* case para [36].

29 *Van der Merwe* case paras [35]-[37].

30 *S v De Vries* (67/2005) [2008] ZAWCHC 38 (11 June 2008) (hereafter the *De Vries* case) para [14]. (The case is also reported as *S v De Vries* 2009 1 SACR 613 (C), but the relevant paragraph is omitted from this law report.)

authority under oath.[31] Similarly, the CCA requires a written application for a search warrant and the setting out of the jurisdictional facts on oath or by way of affirmation.[32] In *Wessels v General Public Service Sectoral Bargaining Council* the court nevertheless outlined the procedure used in practice for the issuing of a section 205 subpoena as follows:

> In order to obtain a section 205 subpoena, the investigating officer must furnish the Senior or Control Prosecutor with an affidavit, detailing the reasons why the subpoena should be issued. The Senior or Control Prosecutor would then complete a section 205 statement/summons, which would then, together with the affidavit, be submitted to the Magistrate to sign and authorise the subpoena. Once authorised, the subpoena would then be handed over to the investigating officer, who would in turn will (sic) hand it over to the SAPS' technical support unit to approach the cell phone service providers to discover relevant cellular phone records.[33]

It is clear that, at the very least, sworn evidence must be presented to the judicial officer to demonstrate the possibility that the individual in question can offer evidence related to an offence.

4.3 Judicial oversight

Regarding judicial oversight, our courts have held that a judicial officer must carefully assess whether the issuance of a subpoena is justified before authorising it. Judicial officers are required to use their discretion by carefully assessing the details presented in the application. This oversight is essential due to the potentially significant repercussions linked to section 205.[34] Failure to comply with a section 205 exposes the recipient of the subpoena to a fine or imprisonment.[35] The judicial officer must therefore

---

31 Section 21(1)(a) read with s 20 of the CPA. The section requires that the decision to issue a warrant be made only if the affidavit in support of the application contains the following objective jurisdictional facts: (i) the existence of a reasonable suspicion that a crime has been committed, and (ii) the existence of reasonable grounds to believe that objects connected with the offence may be found on the premises or persons intended to be searched. See the *Van der Merwe* case para [39].

32 Section 29(1)(a) of the CCA.

33 *Wessels v General Public Service Sectoral Bargaining Council* (JR2211/12) [2019] ZALCJHB 361 (19 December 2019) para [7].

34 *De Vries* case para [14] where reliance was placed on *Haysom v Additional Magistrate, Cape Town; S v Haysom* 1979 3 SA 115 (C) 158F-G and *Matisonn v Additional Magistrate, Cape Town* 1980 2 SA 619 (C) para 65. In *Stevens v Investec Bank Ltd* (2012/32900) [2012] ZASGHC 1 (25 October 2012), the applicants applied for an interdict to preserve bank confidentiality pending the review of a section 205 subpoena. Satchwell J remarked as follows in this regard: "There is no doubt that a banker-client relationship requires the highest *uberrimae fides* and that confidentiality is one of the essential aspects of such a relationship of trust … Privacy in financial and banking affairs is often an important aspect of successful business enterprise in a competitive economy" (para [10]).

35 Section 205(4) of the CPA. Although s 205(4) does provide that no person shall be sentenced to imprisonment unless the presiding officer concerned is "also of the opinion that the furnishing of such information is necessary for the administration of justice or the maintenance of law and order"; see the *De Vries* case para [13].

exercise discretion after due consideration of the facts disclosed in the application.[36] Judicial oversight significantly enhances the protection of individual rights as judicial officers "possess qualities and skills essential for the proper exercise of this power, like independence and the ability to evaluate relevant information to make an informed decision."[37] It is argued, however, that judicial oversight should have a broader scope, necessitating an assessment of whether the invasion of privacy experienced by the individual from whom information is requested is warranted under the given circumstances.

4.4 The scope of the information required

Another important safeguard, especially concerning the privacy rights of a suspect, relates to the terms of the section 205 subpoena. As with a search warrant, these terms should not be too broad or general. Therefore, it is essential to specify the scope of the information needed in sufficient detail. The information sought should be limited to that which is relevant to the crime being investigated.[38]

4.5 Challenging the subpoena

Another important safeguard to consider is related to the grounds on which an aggrieved person may rely in a court challenge to the validity of a warrant.[39] In the *De Vries* case the state argued that the accused lacked *locus standi* to challenge the admissibility of evidence obtained through section 205 subpoenas as his right to privacy had not been violated. The state contended that the records or data requested through the subpoenas were not physically in the possession of the accused but were maintained by the cell phone provider, and therefore only the provider had the standing to challenge the subpoenas. Additionally, the state maintained that the accused's privacy was not jeopardised since the subpoenas did not request access to the actual content of phone calls or text messages. However, the

---

36 *Panday v Minister of Police* 2012 2 SACR 421 (KZD) para [7]. In this matter the section 205 subpoena was assailed because the issuing magistrate did not keep a proper record of the proceedings. The court held that no such formality is prescribed by section 205 (para [9]). The court referred to a circular issued by the judicial head of the relevant administrative region aimed at ensuring uniformity of practice relating to the keeping of records of search warrants and section 205 subpoenas (paras [11] and [12]). The court acknowledged that "the retention of the record of a request and the decision by the magistrate may facilitate the resolution of any queries raised in connection therewith and subsequently assist the magistrate to provide reasons for his decision" (para [15]). Since the applicant had been furnished with copies of the applications and the subpoenas, the correctness and completeness of which had not been contested, the court held that he had not suffered any prejudice (paras [17] and [18]). The application to set aside the section 205 subpoena was dismissed.

37 *Van der Merwe* case para [39].

38 *Van der Merwe* case para [40].

39 *Van der Merwe* case para [41].

court remained unconvinced. Bozalek J concluded that the records held by the cell phone company pertaining to the use of numbers associated with the accused granted the accused a valid interest to challenge the admissibility of the evidence gathered through the use of the section 205 subpoena. The court stressed that the absence of actual content of phone calls or text messages in these records did not imply that an individual's privacy rights were unaffected. It acknowledged that information about who someone communicates with by means of a phone, whether through incoming or outgoing calls, was generally regarded as personal and might be protected under constitutional privacy rights. The court noted that while a suspect could not initially stop a third party from providing information under a section 205 subpoena, the suspect could later contest its admissibility at trial. The underlying principle was that the right to challenge the use of such evidence persisted, especially when privacy concerns were involved.[40]

Notwithstanding the inherent shortcomings of section 205, it is unlikely that the subpoena will be set aside, provided that the judicially approved practice procedures were closely followed.

5 Expectation of privacy in historical records

When the two-stage test (outlined in paragraph 2 above) is applied, it becomes evident that an individual's legitimate expectation of privacy concerning historical data, being information typically accessed under section 205, is minimal. The privacy expectation of a suspect regarding cell phone records and bank statements may not be as high as that associated with the "inner core" of privacy, such as one's home and person. However, this does not imply that there is no legitimate expectation of privacy for data of these types. In the *Hyundai* case the court held: "Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied."[41] Similarly, financial records obtained from a bank are the sort of information a person may expect to remain confidential, "as they are part of the biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[42]

---

40 *De Vries* case para [12].

41 *Hyundai* case para [16].

42 In *Schreiber v Canada (Attorney General)* [1998] 1 SCR 841 para 42 the Supreme Court of Canada confirmed the finding of the court in the *Plant* case as quoted at 293. For a discussion of the *Schreiber* case, see Harvie and Foster 1997 *Man LJ* 421-448.

Also, the operation of statutes such as the *Regulation of Interception of Communications and Provision of Communication-related Information Act*[43] (hereafter RICA), the *Financial Intelligence Centre Act*[44] (hereafter FICA) and the *Tax Administration Act*[45] (hereafter TAA) support the view that a suspect has a limited expectation of privacy in historical records. In terms of RICA, electronic communication service providers are legally obliged to record and store the SIM card and personal information of customers.[46] Certain personal information regarding customers must also be verified.[47] Furthermore, if an activated SIM card changes hands, a customer must provide the relevant electronic communication service provider with the details of the person in receipt thereof.[48] If a cellular phone or SIM card is lost, stolen or destroyed, this event must be reported to the police.[49] With regard to FICA, "accountable institutions" like banks are required to carry out transaction monitoring, which is a crucial part of South Africa's framework for combating money laundering, terrorism financing, and proliferation financing.[50] They must also report suspicious and unusual transactions to the Financial Intelligence Centre.[51] The South African Revenue Service (SARS) possesses extensive authority to access banking information and can even direct a bank to withdraw funds from a client's account to guarantee adherence to tax responsibilities.[52] Legislative measures like these greatly diminish the reasonable expectation of privacy for customers. Nowadays, only the most naive individuals would assume that their banking details and phone call records are beyond scrutiny.

6 Information sharing and the risk of abuse

One area that necessitates further examination is the sharing of evidence and information gathered under section 205 among various law enforcement agencies nationwide.[53] For the purposes of this discussion, "evidence" is regarded as facts that are legally admissible to prove the facts

43 *Regulation of Interception of Communications and Provision of Communication-related Information Act* 70 of 2002 (RICA).
44 *Financial Intelligence Centre Act* 38 of 2001 (FICA).
45 *Tax Administration Act* 28 of 2011 (TAA).
46 Section 40(1) and (2) of RICA.
47 Section 40(3) of RICA.
48 Section 40(5) of RICA.
49 Section 41(1) of RICA.
50 See FIC 2023 https://www.fic.gov.za/2023/11/08/how-accountable-institutions-can-help-fight-financial-crime-by-reporting-to-the-fic/. Also see Part 3 of FICA.
51 Part 3 of FICA.
52 Section 179 of the TAA.
53 International mutual legal assistance in terms of the *International Co-operation in Criminal Matters Act* 75 of 1996 is not included in this discussion.

that are in dispute in a criminal case.[54] An example of evidence would be documents pertaining to an accused person's bank account and obtained from his financial institution by means of a section 205 subpoena and filed in the police case docket. "Information", on the other hand, relates to material or intelligence reports derived from evidence and in the example would be a report either oral or in writing indicating the flow of funds between accounts or the payment of amounts on certain dates into the bank account.

It is submitted that the evidence obtained in terms of a section 205 application may be shared between law enforcement agencies only if the evidence to be shared flows directly from the initial section 205 application. In the *Matisonn* case, the court held that "Once properly instituted, an enquiry into an alleged offence in terms of s 205 may be pursued, in my view, also in regard to associated or alternative or additional offences the possible commission of which may emerge from the evidence elicited in the investigation of the offence or offences alleged in the subpoena."[55]

In instances where the application for the section 205 subpoena, for example, indicated that the offence of fraud was being investigated and in the course of the same investigation charges of theft and money laundering were revealed, the utilisation of the evidence so obtained would be justified. However, it would not be possible to utilise the evidence for purposes of a separate and/or new investigation which was not a natural outflow from the original investigation.

Reliance is often placed by law enforcement agencies on the whole-of-government approach (WGA)[56] and section 73 of the *Prevention of Organised Crime Act* (hereafter POCA) to justify the inappropriate sharing of evidence.[57] However, a clear distinction should be drawn between the

---

54 Schwikkard and Van der Merwe *Principles of Evidence* 4; Zeffertt and Paizes *South African Law of Evidence* 3-5; Glover *Murphy on Evidence* 2; Tapper *Cross and Tapper on Evidence* 1-2.

55 *Matisonn v Additional Magistrate, Cape Town* 1980 2 SA 619 (C) 630F-G. Also see *S v Matisonn* 1981 3 SA 302 (A) 314D.

56 Whilst the importance of the whole-of-government concept is acknowledged, Brun *et al* reiterate the importance of the aim to "strike an appropriate balance between existing protections and information sharing to more effectively counteract crime while preserving legitimate individual rights to privacy" (Brun *et al Taxing Crime* 13). The importance of the protection of individual rights is thus emphasised: "Moreover, there should be an assumption that any agency, as a 'public body' representing the government, has 'a duty to act consistently with' any convention on human rights to which the government adheres, including as it relates to privacy rights of individuals" (Brun *et al Taxing Crime* 14).

57 *Prevention of Organised Crime Act* 121 of 1998. S 73 provides that "Notwithstanding the provisions of section 4 of the Income Tax Act, 1962 (Act 58 of 1962), and with regard to any other secrecy provision in similar legislation, whenever any investigation is instituted in terms of this Act, including an investigation into any offence referred to in Schedule 1, and an investigation into the property, financial

sharing of evidence and the sharing of information. Whilst the sharing of information could be justified in terms of WGA and section 73 of POCA in respect of new or unrelated investigations, this does not include the sharing of evidence.

The privacy rights of individuals expressly recognised in the common law and enshrined in the *Constitution* militate against the sharing of evidence obtained for a specific purpose in a specific investigation with law enforcement agencies to facilitate entirely new investigations. With reference to the example, it can be stated that banking affairs are included in the constitutional right to privacy and any invasion or infringement thereof can be countenanced only when it takes place within the parameters of or within strict adherence to section 36 of the *Constitution*.

In addition, applications for section 205 subpoenas are brought on an *ex parte* basis. As such, the applicant is required to disclose comprehensive information to the judicial officer in chambers.[58] An *ex parte* application by its very nature places only one side of a case before the judicial officer and therefore requires the utmost good faith from the applicant. Applicants in these applications of this type therefore have a duty to be completely transparent and honest.[59] If a full explanation is not made of the type of investigation that is intended to be undertaken, it cannot be said that full disclosure was made in the application. Simply using the evidence obtained for a specific application for another investigation would amount to an abuse of process.

It is submitted that section 73 of POCA cannot reasonably and justifiably limit section 14, particularly since the information gathered by the Directorate for Priority Crime Investigation can be used by SARS to lawfully acquire the necessary data under the extensive powers granted by the TAA, provided there is reasonable cause.

---

activities, affairs or business of any person, the Commissioner of the South African Revenue Services or any official designated by him or her for this purpose, shall be notified of such investigation with a view to mutual co-operation and the sharing of information."

58 In *Thint v National Director of Public Prosecution; Zuma v National Director of Public Prosecutions* 2000 1 SA 1 (CC) para [102] the constitutional court remarked as follows in respect of *ex parte* applications: "It is our law that an applicant in an ex parte application bears a duty of utmost good faith in placing all the relevant material facts before the court. The duty of good faith requires a disclosure of all material facts within the applicant's knowledge. The Supreme Court of Appeal reiterated in *Powell* that an applicant for a search warrant is 'under a duty to be ultra-scrupulous in disclosing any material facts that might influence the Court in coming to its decision'"; the *Powell* case para [72].

59 *Commissioner for the South African Revenue Services v Bachir* (87306/2014) [2016] ZAGPPHC 251 (22 April 2016); *Commissioner for the South African Revenue Service v Sunflower Distributors CC* 2015 JDR 2546 (GP) para [4].

6 Conclusion

Section 205 remains a key investigative tool in the criminal justice system and continues to support the collection of historical data that may be pertinent to criminal investigations. Although this provision predates the constitutional era, the safeguards developed through case law have permitted its ongoing application in a way that accords with constitutional standards. The comparison with search warrant jurisprudence illustrates that judicial supervision, the setting of jurisdictional preconditions, the requirement that the scope of the information requested be clearly defined, and the possibility of challenging the subpoena's validity together operate to limit unwarranted intrusions on privacy.

The discussion indicates that, while a person's reasonable expectation of privacy in relation to historical records is diminished, it does not disappear. The compulsory retention of specific categories of data by electronic communications service providers and financial institutions, along with the reporting obligations imposed by various pieces of legislation, contribute to this diminished expectation. Nonetheless, any restriction of privacy must still be constitutionally justifiable, particularly in *ex parte* applications, where the applicant must make full and candid disclosure.

The analysis further highlights concerns about the secondary use and sharing of information acquired under section 205. Although a degree of inter-agency cooperation may be warranted, using such evidence for purposes unconnected to the original application threatens constitutional guarantees and may amount to an abuse of process. It is submitted that the most appropriate means of strengthening the constitutional application of section 205 lies in the continued development of clear judicial guidance. Formal recognition of the evidential threshold for applications, the required degree of particularity, and limitations on the sharing of evidence obtained under section 205 would enhance legal certainty. In this way, section 205 may continue to operate effectively while maintaining the necessary balance between legitimate law enforcement objectives and the protection of privacy rights in accordance with the *Constitution*.

Bibliography

Literature

Brand 2006 *Ecquid Novi*
Brand R "Between Privilege and Subpoena: Protecting Confidential Sources" 2006 *Ecquid Novi* 113-135

Brun *et al Taxing Crime*
Brun J *et al Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes* (World Bank Group Washington DC 2022)

Currie and De Waal *Bill of Rights Handbook*
Currie I and De Waal J *The Bill of Rights Handbook* 6th ed (Juta Cape Town 2013)

Du Toit 2002 *Obiter*
Du Toit P "The Search Warrant Provisions of the Cybercrimes Act and Their Relationship with the Criminal Procedure Act" 2022 *Obiter* 764-779

Du Toit *et al Commentary on the Criminal Procedure Act*
Du Toit E *et al Commentary on the Criminal Procedure Act* (Juta Cape Town 1997-, 2024 update)

Geldenhuys 2017 *Servamus*
Geldenhuys K "Cellphone Evidence = Digital DNA" 2017 *Servamus* 16-21

Geldenhuys 2022 *Servamus*
Geldenhuys K "Cellphones: Evidence That Does Not Lie" 2022 *Servamus* 1-15

Glover *Murphy on Evidence*
Glover R *Murphy on Evidence* 14th ed (Oxford University Press Oxford 2015)

Harvie and Foster 1997 *Man LJ*
Harvie R and Foster H "Unwarranted Behaviour: The Airbus Affair, United States Law, and Searching Foreign Bank Accounts" 1997 *Man LJ* 421-448

Kruger *Hiemstra's Criminal Procedure*
Kruger A *Hiemstra's Criminal Procedure* (LexisNexis Durban 2008-, 2023 update)

Lochner and Zinn 2014 *Acta Criminologica*
Lochner H and Zinn R "Detecting Invisible Traces Generated by a Cellphone at a Crime Scene" 2014 *Acta Criminologica* 160-175

Lochner, Benson and Horne 2012 *Acta Criminologica*
Lochner H, Benson B and Horne J "Making the Invisible Visible: The Presentation of Electronic (Cell Phone) Evidence as Real Evidence in a Court of Law" 2012 *Acta Criminologica* 69-80

Schwikkard and Van der Merwe *Principles of Evidence*
Schwikkard P and Van der Merwe SE *Principles of Evidence* 4th ed (Juta Cape Town 2016)

Tapper *Cross and Tapper on Evidence*
Tapper C *Cross and Tapper on Evidence* 13th ed (Oxford University Press Oxford 2013)

Zeffert and Paizes *South African Law of Evidence*
Zeffert DT and Paizes A *The South African Law of Evidence* 3rd ed (LexisNexis Butterworths 2017)

Case law

Canada

R v Plant [1993] 3 SCR 281

Schreiber v Canada (Attorney General) [1998] 1 SCR 841

South Africa

Bernstein v Bester 1996 2 SA 751 (CC)

Commissioner for the South African Revenue Service v Bachir (87306/2014) [2016] ZAGPPHC 251 (22 April 2016)

Commissioner for the South African Revenue Service v Sunflower Distributors CC 2015 JDR 2546 (GP)

Gaertner v Minister of Finance 2014 1 SA 442 (CC)

Gcabashe v MTN Group Ltd (53/2019) [2024] ZAGPPHC 233 (6 March 2024)

Haysom v Additional Magistrate, Cape Town; S v Haysom 1979 3 SA 115 (C)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit 2000 2 SACR 349 (CC)

Magajane v Chairperson, North West Gambling Board 2006 2 SACR 447 (CC)

Matisonn v Additional Magistrate, Cape Town 1980 2 SA 619 (C)

Minister for Safety and Security v Van der Merwe 2011 2 SACR 301 (CC)

Minister of Police v Kunjana 2016 2 SACR 473 (CC)

Nel v Le Roux 1996 3 SA 562 (CC)

Panday v Minister of Police 2012 2 SACR 421 (KZD)

Powell v Van der Merwe 2005 5 SA 62 (SCA)

S v De Vries (67/2005) [2008] ZAWCHC 38 (11 June 2008)

S v De Vries 2009 1 SACR 613 (C)

S v Dos Santos 2010 2 SACR 382 (SCA)

S v Matisonn 1981 3 SA 302 (A)

S v Miller 2016 1 SACR 251 (WCC)

S v Murphy - Main Judgment (CC27/2018) [2023] ZAWCHC 186 (12 July 2023)

S v Waite 1978 3 SA 896 (O)

Stevens v Investec Bank Limited (2012/32900) [2012] ZASGHC 1 (25 October 2012)

Thint v National Director of Public Prosecution; Zuma v National Director of Public Prosecutions 2000 1 SA 1 (CC)

Wessels v General Public Service Sectoral Bargaining Council (JR2211/12) [2019] ZALCJHB 361 (19 December 2019)

United States of America

Abel v US 362 US 217 (1960)

Katz v US 389 US 347 (1967)

Legislation

Constitution of the Republic of South Africa, 1996

Criminal Procedure Act 51 of 1977

Cybercrimes Act 19 of 2020

Financial Intelligence Centre Act 38 of 2001

International Co-operation in Criminal Matters Act 75 of 1996

Prevention of Organised Crime Act 121 of 1998

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

Tax Administration Act 28 of 2011

Internet sources

FIC 2023 https://www.fic.gov.za/2023/11/08/how-accountable-institutions-can-help-fight-financial-crime-by-reporting-to-the-fic/

Financial Intelligence Centre 2023 *How Accountable Institutions Can Help Fight Financial Crime by Reporting to the FIC* https://www.fic.gov.za/2023/11/08/how-accountable-institutions-can-help-fight-financial-crime-by-reporting-to-the-fic/ accessed 9 May 2024

SAPS 2020 https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf
South African Police Service 2020 *Standard Operating Procedures in Terms of Section 26 of the Cybercrimes Act, No 19 of 2020 for the Investigation, Search, Access or Seizure of Articles* https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf accessed 15 January 2025

List of Abbreviations

CCA	Cybercrimes Act 19 of 2020
CPA	Criminal Procedure Act 51 of 1977
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act 38 of 2001
Man LJ	Manitoba Law Journal
POCA	Prevention of Organised Crime Act 121 of 1998
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
SAPS	South African Police Service
SARS	South African Revenue Service
SOPs	Standard Operating Procedures
TAA	Tax Administration Act 28 of 2011
WGA	whole-of-government approach