



SUPPLEMENTARY REPORT

REFORMING COMMUNICATION SURVEILLANCE IN SOUTH AFRICA

Understanding the section 205 'loophole'

SUPPLEMENTARY REPORT

REFORMING COMMUNICATION SURVEILLANCE IN SOUTH AFRICA

Understanding the section 205 ‘loophole’

Intelwatch

Report prepared by Heidi Swart

May 2023

Intelwatch is dedicated to research, policy work and advocacy to strengthen public oversight of state and private intelligence agencies in Southern Africa and around the world. Founded in 2022 in South Africa, Intelwatch aims to carry forward and build on the work of the Media Policy and Democracy Project.

For more information see intelwatch.org.za.

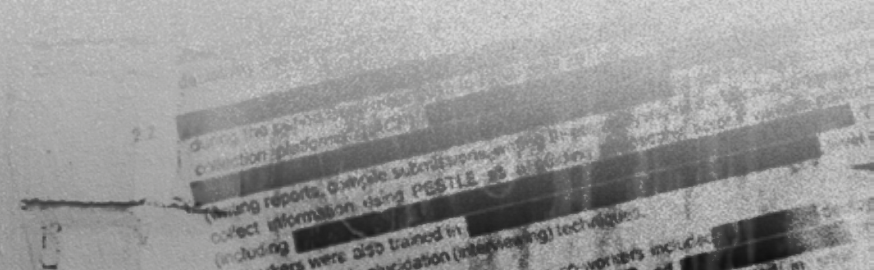


TABLE OF CONTENTS

INTRODUCTION	4
RICA AND SECTION 205 OF THE CRIMINAL PROCEDURE ACT	4
Previous recommendations	4
Separate processes	5
Record keeping	5
Number of section 205 applications and subpoenas	6
Nature, analysis and use of archived metadata in South Africa	7
Constitutionality of section 205	9
Abuse of section 205 to obtain metadata	10
CONCLUSION	12
BIBLIOGRAPHY	13
ANNEXURE A Correspondence from the Department of Justice (May 2017)	

INTRODUCTION

This is a supplementary report to *Reforming Communication Surveillance in South Africa: Recommendations in the wake of the AmaBhungane judgment and beyond*, published in May 2023.¹ The purpose of this supplementary report is to set out additional information about the implementation of RICA and the potential for the abuse of the State's communications surveillance capabilities by law enforcement and intelligence agencies, with particular relevance to section 205 ("section 205") of the Criminal Procedure Act of 1977 ("CPA"). Of particular concern, is the extensive use of section 205 to obtain metadata from telecommunications service providers ("service providers") outside of the protections envisaged by RICA, and the abuse of weaker safeguards in the section 205 process to obtain metadata illegally.

The Constitutional Court did not address the section 205 process in the *AmaBhungane* judgment, as the matter was not before the Court. However, it is vital that the current reform process in the wake of the *AmaBhungane* judgment addresses the concerns pertaining to section 205 metadata applications.

RICA AND SECTION 205 OF THE CRIMINAL PROCEDURE ACT

Section 13 of RICA makes provision for both an archived communications-related information ("archived metadata") direction and a real-time communications-related information ("real-time metadata") direction to be issued by a designated Judge in terms of RICA ("the RICA Judge"). The former refers to past records of metadata stored by the service provider, while the latter is provided "on an ongoing basis, as it becomes available".² A number of other sections in RICA deal with the application for metadata by state intelligence and law enforcement agencies. These include sections 14 to 15 and 17 to 19 of the Act. Section 30 of RICA provides for storage of metadata by the service providers, and section 50 deals with unlawful provision of metadata.

Section 15(1) of RICA makes provision for the use of "other procedures for obtaining real-time or archived communication-related information". As a result, section 205 of the CPA is used by the South African Police Service ("SAPS") to obtain metadata from service providers.

Previous recommendations

In 1999, the South African Law Commission published its report on Project 105. The project entailed a review of security legislation, including RICA's predecessor, the Interception and Monitoring Prohibition Act of 1992. The aim of the review was to produce recommendations for amendments to the Act. Among the Commission's recommendations was that legislation outside of the Interception and Monitoring Prohibition Act – including section 205 of the CPA in particular – should not be made available to the State as an avenue to obtain metadata. The Commission stated in its recommendations:³

"The Commission notes that section 205 of the Criminal Procedure Act and section 11(1)(e) of the Drugs and Drug Trafficking Act, 1992 confers powers on law enforcement agencies to obtain evidence such as call-related information. The Commission poses the question whether this situation should be sanctioned by the proposed clause 5B(4) and whether the interception Act should permit agencies to request the provision of call-related information. The question as to abuse of the provisions arises. The need for the existence of different methods of enabling law enforcement agencies to obtain call-related information seems questionable. The Commission is therefore of the view that the Interception and Monitoring Prohibition Act should be the only Act to authorise the request for call-related information and should exclude the use of any power in any other Act to obtain evidence or information in respect of a person, body or organization."

¹ Available at <https://intelwatch.org.za/research/>.

² Section 1 of RICA.

³ South African Law Commission Report on project 105: Review of Security Legislation, the Interception and Monitoring Prohibition Act 127 of 1992 (October 1999) at para 25.

Despite these opinions, section 15(1) was still included in RICA, although section 15(2) does limit the provision of metadata in that it cannot be provided on an ongoing basis (be it real-time or archived).⁴

As a result, section 205 of the CPA provides a process for obtaining metadata without the authorisation of the RICA Judge. Instead, a Judge of the High Court, a Regional Court Magistrate or a Magistrate issues subpoenas in terms of section 205. Thus, personal metadata can be obtained in the same manner as any other evidence.⁵

Separate processes

Metadata obtained through the various sections of RICA and section 205 of the CPA are effectively identical. However, different legal obligations regulate processes that concern the application for and provision of metadata, with the RICA process offering more stringent protections.

Whereas the RICA Judge submits annual statistical data to Parliament about the number of applications received (this includes applications for archived metadata, real-time metadata, as well as communications content) and related directions issued, the courts do not make similar statistics for section 205 applications and subpoenas available. RICA provides that law enforcement may only use its processes to access communications data in relation to relatively serious criminal offences, by relatively senior officials, with the authorisation of a senior Judge; section 205 processes are theoretically available even to junior officials, for any level of offence, with the authorisation of any magistrate.

This contrast between the two legislative mechanisms is perhaps the most stark when regarding section 19(1) of RICA. As with section 205 of the CPA, section 19(1) provides a mechanism for state intelligence and law enforcement agencies to obtain archived metadata by applying to a Judge of the High Court, a Regional Court Magistrate or a Magistrate. However, section 19 stipulates that the Judge must submit copies of the application as well as the archived metadata direction concerned to the RICA Judge as soon as possible after the order is granted,⁶ and the RICA Judge must in turn keep such copies for at least five years.⁷ There is no such obligation on the Judge in cases where section 205 is used to obtain archived metadata.

Record keeping

The Department of Justice stated in formal correspondence⁸ with the media in 2017 that “[t]he lower court judiciary implemented measures to keep records of proceedings in terms of section 205 as was also discussed in *Panday v Minister of Police and Others* 2012 (2) SACR 421 (KZD) at paragraphs 12 to 17”. However, the Department did not indicate whether section 205 applications for archived metadata would be placed in a separate register. It is unclear whether any such record-keeping whatsoever has materialised in practice.

The Court has, however, recognised that there is currently no obligation on Judges to ensure that records of section 205 applications and subpoenas are kept. In *Panday*, the Court referred to a previous circular issued by a Judicial Head:⁹

“In the circular the acting Judicial Head, S F van Niekerk, refers to a lack of uniformity of practice relating to the keeping of records of search warrants and subpoenas in terms of section 205. After pointing out the obligation on judicial officers to exercise their discretion judicially in authorising warrants or subpoenas, Van Niekerk also warns of the potential for constitutional challenges which occur after the lapse of a period of time after the authorisation and will therefore entail sight of the application in order for the judicial officer to furnish reasons and to demonstrate that his discretion was exercised judicially.”

4 Section 15(2) of RICA.

5 Section 205 of the CPA and Section 15(1) of RICA.

6 Section 19 (7) of RICA.

7 Section 19 (8) of RICA.

8 See annexure A: Correspondence from the Department of Justice (May 2017).

9 *Panday v Minister of Police and Others* (12044/10) [2012] ZAKZDHC 20; 2012 (2) SACR 421 (KZD) (18 April 2012) at para 12 and 13.

“Van Niekerk therefore suggests in the circular that a register of the details of such applications are maintained at each office, and a copy of each application be kept in a file.

The circular, firstly, confirms that there is no peremptory requirement relating to the keeping of records of section 205 applications or the recording of reasons therefor.”

Number of section 205 applications and subpoenas

Publicly available records provided by the four largest telecommunications service providers in South Africa show that section 205 applications for archived metadata far outnumber such applications to the RICA Judge. In 2017, the Department of Justice stated in formal correspondence with the media that “[i]t is probable that most call-related information is obtained in terms of section 205 of the Criminal Procedure Act. It is mainly in instances where archived communication-related information is required on an ongoing basis, as it becomes available, that section 19 of the RICA is used (see section 15(2) of the RICA).”¹⁰

In 2017, the non-profit organisation Right2Know utilised the Promotion of Access to Information Act (“PAIA”) to request from South Africa’s four largest telecommunications service providers information regarding the number of section 205 subpoenas for archived metadata they were served annually. The providers included Vodacom, MTN, Cell C, and Telkom.¹¹ All four providers furnished information.

For the three consecutive financial years of 2014/2015, 2015/2016 and 2016/2017 the country’s largest service provider, Vodacom, was served subpoenas for the archived metadata related to 70 315, 69 286 and 71 731 cellular phone numbers, respectively. The corresponding number of section 205 subpoenas (one application can pertain to more than one cellular phone number) for those financial years were 19 614, 18 594 and 19 580, respectively. During those three years, only one subpoena for archived metadata did not result in Vodacom furnishing information.¹² Right2Know’s PAIA applications saw the first such public release by South African providers of statistical information about section 205 subpoenas for metadata:

	2015	2016	2017	2018
Vodacom	19 614	18 594	19 580	22 690
MTN	25 808	23 762	29 749	Not provided
Cell C	5 786	6 455	5 733	Not provided
Telkom	1 189	1 450	1 611	Not provided

Table: Total number of section 205 requests received¹³

By comparison, far fewer applications for directions are considered by the RICA Judge. For instance, for the 2014/2015 financial year, the RICA Judge received a total of 760 applications (of which 11 were refused). This total includes applications for archived and real-time metadata and communications content, as well as entry warrants to plant interception devices in physical spaces.¹⁴

¹⁰ Correspondence from the Department of Justice (May 2017).

¹¹ Right2Know “MTN, Vodacom, Telkom and Cell C: 30 days to provide surveillance stats” (May 2017), available at <https://www.r2k.org.za/2017/05/30/mtn-vodacom-telkom-and-cell-c-30-days-to-provide-surveillance-stats/>.

¹² Letter from Vodacom to Right2Know (June 2017).

¹³ Hunter “Cops and Call Records: Policing and Metadata Privacy in South Africa” *Media Policy and Democracy Project* (27 March 2020) at 5, available at <https://archive.org/details/2003-cops-and-call-records-metadata-and-policing>.

¹⁴ Annual Report by the designated RICA Judge on Interception of Private Communications for the Period 2014/2015 to the Joint Standing Committee on Intelligence (October 2015).

Nature, analysis and use of archived metadata in South Africa

Since cases where section 205 is utilised to obtain metadata are heard in magistrates' courts and High Courts, there are public records of the practicalities involved in obtaining such data through section 205, as well as records of how such data is analysed and utilised by law enforcement in practice.

In South Africa, the specific categories of archived metadata are presented to the court by expert witnesses (either employed by the service provider or a police officer with special qualifications in analysing such evidence) following a successful execution of a section 205 subpoena for metadata. The metadata is presented to law enforcement by the service provider in tabular form, with each column containing a specific type of metadata. Below are the column headings and their related technical explanations:¹⁵

- The 'MSISDN' (Mobile Subscriber Integrated Services Digital Number) column contains the cell phone number of the surveillance target.
- The 'IMEI' (International Mobile Equipment Identity) number column contains the unique number identifying the mobile handset of the surveillance target.
- The 'date and time' column refers to the time and the date when the communication was initiated or received by the surveillance target.
- The 'other party' column shows the number of the other party involved in a communication session with the surveillance target.
- The 'third party' column refers to when the phone of the surveillance target was not in use, and when the call forwarding function was activated to allow an incoming call to be handled by the voice mail function; if the call is diverted to an alternative number, that number will appear in the 'third party' column.
- The 'call type' column contains the type of communication that occurred through the handset of the surveillance target, be it an internet or data connection, an incoming or outgoing call, or an incoming or outgoing SMS.
- The 'duration' column is the length of time that the communication lasted. An incoming or an outgoing SMS will display a duration of milliseconds.
- The 'cell number' column is the identification code for the cell tower (base station) to which the mobile device was connected.
- The 'handset name and type' column contains the name, model and type of handset used by the surveillance target during the communication.
- The 'MTC' column indicates the Mobile Terminating Call which refers to an incoming communication.

Since RICA came into effect, communications technology has developed considerably; second generation (2G) cellular phones, for instance, have largely been replaced by fourth and fifth generation (4G and 5G) 'smartphones'. The latter generates a tremendous amount of metadata when compared to its earlier iteration. Accordingly, metadata available to law enforcement and intelligence agencies globally has diversified and increased substantially as more devices (other than smartphones and computers) become connected to and dependent on the internet in order simply to function. However, due to international legal restrictions, it appears that, in South Africa, archived metadata in the form of cellular phone billing records are still the primary form of metadata evidence presented in the ordinary courts.¹⁶

¹⁵ *S v Hasane and Others* (K/S 01/2017) [2020] ZANHC 28 (12 May 2020) at para 322, available at <http://www.saflii.org/cgi-bin/disp.pl?file=za/cases/ZANHC/2020/28.html&query=%22cell%20phone%22>.

¹⁶ Swart "Special report: 5G opens the gates for surveillance on steroids" *Media Policy and Democracy Project* (6 April 2021) published in *The Daily Maverick*, available at <https://www.dailymaverick.co.za/article/2021-04-06-5g-opens-the-gates-for-surveillance-on-steroids/>.

Archived metadata obtained through section 205 applications can be extensive. For instance, in *S v Matsitela*,¹⁷ cell phone metadata evidence filled four lever arch files. In *S v Agliotti*, the expert witness for Vodacom testified that “50 lever arch files full of cellphone records in respect of various people” were provided to the police.¹⁸

Such large volumes of metadata can be analysed utilising computer software. This allows law enforcement to derive intelligence from the data in a far more accurate and efficient manner when compared to manual analysis by a person. This software is available to law enforcement and state intelligence agencies in South Africa. This analysis is described as follows in *S v Miller*:¹⁹

“This information, once supplied by the SP’s [service providers], was fed into a laptop computer equipped with a software program called ‘Analyst Notebook’. The latter is evidently a software tool that is used to collate data and to provide a visual link where similarities are found. So, for example, when supplied with the requisite data from the SP’s it will show when particular cell phone numbers have been in contact with each other. If one then establishes the identity of the subscribers to these numbers, one can establish who called who, for how long they spoke, what handsets were used during the conversations and where each handset was geographically located during the call. Identification of the subscriber to a particular cellular number can be established through various channels. Firstly the subscriber can furnish the number personally. Secondly, the SP can be asked to identify the subscriber, and thirdly, one can access a particular subscriber’s handset and establish from the address book what name the subscriber has allocated to a particular number.

Having applied “Analyst Notebook” Capt Brink produced several diagrams which depicted cell phone traffic between various numbers. These diagrams, which were colloquially referred to as “spiders”, were placed before the court in documentary form. Such a spider would generally depict the principal cell phone in the middle of the diagram and the various other numbers with which contact had been made around the periphery of the diagram. By way of lines connecting the number in the middle with those around the periphery one can establish the frequency of cell phone contact. It is important to observe, at this stage, that Analyst Notebook does not in any way interfere with the data which it is required to analyse. As I understand it, it is simply an organisational tool which saves the individual the arduous task of doing the exercise manually.”

In 2014, the United Nations High Commissioner for Human Rights stated that archived metadata, when viewed in aggregate, may in fact convey more than what is said in an actual conversation:²⁰

“The aggregation of information commonly referred to as ‘metadata’ may give an insight into an individual’s behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.”

Similarly, the American Civil Liberties Union of California has stated: ²¹

“Metadata can reveal who we are, who we know, what we do and care about and plan to do next – essentially the same spectrum of sensitive information that could also be contained in the contents of a communication.”

The European Court of Human Rights drew similar conclusions in a case about metadata retention in the European Union:²²

17 *S v Matsitela and Others* (78/2017) [2018] ZAFSHC 135 (13 September 2018) at para 34.

18 *S v Agliotti* (SS 154/2009) [2010] ZAGPJHC 129; 2011 (2) SACR 437 (GSJ) (25 November 2010) at para 137.

19 *S v Miller and Others* (SS13/2012) [2015] ZAWCHC 118; [2015] 4 All SA 503 (WCC); 2016 (1) SACR 251 (WCC) (2 September 2015) at para 17 and 18.

20 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014) at para 19.

21 American Civil Liberties Union of California ‘Metadata: Piecing Together a Privacy Solution’ at 5.

22 *Big Brother Watch and Others v The United Kingdom* [2018] ECHR 722 at para 356.

“In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with ...”

Hunter sets out the implications of metadata collection for personal privacy even when no analysis of aggregated data has occurred:²³

“With no further analysis, for example, locational information from a person’s cell phone data would reveal where they sleep at night and who they visit during the day; whether they stop in at a temple or a clinic or a political meeting and for how long. Their call records would reveal much about their associations and activities: who they communicate with and for how long, and how regularly they speak with a labour lawyer or a debt counsellor or make late-night calls to someone who is not their spouse.”

Despite the sensitivity of metadata obtained through a section 205 subpoena, it is not afforded the same treatment and protections as metadata (archived and real-time) and communications content obtained through RICA.²⁴ In addition, while the RICA Judge must report to Parliament regarding directions issued, there is no such reporting mechanism for section 205 applications and subpoenas.

Finally, archived metadata in South Africa must, in terms of section 30(2)(a)(iii) of RICA, be retained by service providers for a minimum of three years and a maximum of five years.²⁵ The result is that the South African State has even larger data sets that could be analysed than if data were stored for shorter periods, as is the practice in other democracies. (For instance, in Australia, the retention period is two years,²⁶ and in Ireland legislation was recently amended to set the default retention period to one year.²⁷) Privacy International has argued that section 30(1)(b) of RICA allows for “blanket, mandatory data retention” with an “untargeted and indiscriminate scope”, and resultantly does not meet the requirements of necessity and proportionality, possibly putting it in breach of domestic and international law.²⁸

Constitutionality of section 205

In 1996, the Constitutional Court found that section 205 does not infringe on a number of constitutional rights placed before the Court. In 2017, the Department of Justice stated its position on section 205’s constitutionality as follows:²⁹

“In NEL v LE ROUX NO AND OTHERS 1996 (1) SACR 572 (CC), at paragraph 20, the Constitutional Court rejected the contention that section 205 of the Criminal Procedure Act infringes a number of fundamental constitutional rights and held that section 205 was as ‘narrowly tailored as possible to meet the legitimate State interest of investigating and prosecuting crime’. The Constitutional Court did not find it necessary to interfere with the procedure envisaged by the section 205 or to prescribe any procedural formality to preserve its constitutionality. The court was mindful of the fact that applications in terms of section 205 demand ‘the exercise of invasive and compulsive powers’, and are subject only to the exercise of judicial discretion by the presiding officers after

23 Hunter “Cops and Call Records: Policing and Metadata Privacy in South Africa” *Media Policy and Democracy Project* (27 March 2020) at 8, available at <https://archive.org/details/2003-cops-and-call-records-metadata-and-policing>.

24 Ibid at 9.

25 Privacy International “Stakeholder Report; Universal Periodic Review 27th Session, South Africa: The Right to Privacy in South Africa” (2016) at para 28 and 29, available at https://privacyinternational.org/sites/default/files/2018-04/South%20Africa_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf.

26 Australian Government Department of Home Affairs, “Data retention obligations”, available at <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations>.

27 Madden “New data retention laws for Ireland” *The Irish Legal News* (14 September 2022), available at <https://www.irishlegal.com/articles/michael-madden-new-data-retention-laws-for-ireland>.

28 Privacy International “Stakeholder Report; Universal Periodic Review 27th Session, South Africa: The Right to Privacy in South Africa” (2016) at para 28 and 29, available at https://privacyinternational.org/sites/default/files/2018-04/South%20Africa_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf.

29 Correspondence from the Department of Justice (May 2017).

due consideration of the facts disclosed in the application. This judgment, however, preceded the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002) (the RICA), and was not decided on the basis of the applicability of section 205 in relation to call-related information.”

As acknowledged by the Department of Justice, the 1996 *Nel v Le Roux* NO ruling predates RICA. In a 2005 case concerning the admissibility of archived metadata obtained through section 205, Judge Bozalek reasoned that metadata could be considered personal information protected by the right to privacy:³⁰

“The State contended in the first place that the accused had no standing to challenge the admissibility of the evidence obtained pursuant to the subpoenas because their right to privacy was not infringed. As I understood this argument the contention was that because the records or data were not in the accused’s possession, only the witness i.e. the cell phone company, could challenge the validity of the subpoena. Another leg to the State’s argument in this regard was that no accused’s right to privacy was involved since the content of telephone conversations or text messages was not involved. I disagree. The simple fact that the cell phone company’s records relate to the use of cell phone numbers allegedly used by the accused gives them a sufficient interest in the subject matter to object to its admissibility. The fact that the records do not reveal the content of telephone calls or text messages does not mean that the accused’s right to privacy is unaffected. Information regarding to whom cell phone calls are made or from whom they are received, is, in the normal course, personal information which may be protected under one’s right to privacy. Although a suspect or an accused person may, in practice, have no initial right to object to such information being disclosed by a third party under a s 205 subpoena to a court or the prosecuting authorities, there can be no reason in principle why, as and when such evidence is tendered at trial, such person cannot raise an objection to the admissibility thereof.”

Abuse of section 205 to obtain metadata

There is a pattern of evidence showing how the weak safeguards in section 205 procedures have led to these procedures being abused. In 2017, the Department of Justice set out the safeguards built into section 205 applications for metadata as follows:³¹

“Obviously, an application for an order in terms of section 205 can only be considered and issued if the objective of the order is to obtain information in the course of, or to assist in, an investigation of an offence. Section 205 of the Criminal Procedure Act provides for the following safeguards to ensure that this objective is met:

(a) The first safeguard relates to the police official who furnishes the information that forms the basis of the application. If the police official wilfully states information in the application which is false he or she commits an offence.

*(b) The second safeguard which is built into the section 205 procedure is that only a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the Director of Public Prosecutions can request a judicial officer to authorise an order in terms of section 205. This in effect means that very senior prosecutors are involved in these applications. In *S v MALIGA* 2015 (2) SACR 202 (SCA) at paragraph 20, the court found that “a prosecutor stands in a special position in relation to the court. The paramount duty of a prosecutor is not to procure a conviction but to assist the court in ascertaining the truth. (*S v Jija and Others* 1991 (2) SA 52 (E) at 67J – 68A.) Implicit herein is the prosecutor’s role in assisting a court to ascertain the truth and dispense justice. This, not surprisingly, gels with the stringent ethical rules by which all legal representatives have to conduct themselves in their professional lives”. It is therefore the duty of the prosecutor in question to ensure that the application for an order in terms of section 205 is regular.*

³⁰ *S v De Vries and Others* (67/2005) [2008] ZAWCHC 38; 2009 (1) SACR 613 (C) (11 June 2008) at para 12.

³¹ Correspondence from the Department of Justice (May 2017).

(c) The third safeguard is that an independent judicial officer must consider the request. The failure of judicial officers to exercise their discretion judicially is the main ground in the few reported cases on which section 205 orders were challenged. In *PANDAY v MINISTER OF POLICE AND OTHERS* 2012 (2) SACR 421 (KZD), at paragraph 28, the court had the following to say about section 205 orders:

‘In R v Parker 1966 (2) SA 56 (RA) at 58, although the decision is pre-constitutional, the court recognised that the interest of an individual to privacy is unequal when weighed against the competing interest of justice. It accordingly held that it would not be a proper exercise of discretion if the available facts indicate that the enquiry is to be based on vague supposition and that the magistrate had a duty ‘to ensure that the members of the public are not unduly harassed by inquisitions’ (my emphasis). Therefore, although the key word ‘unduly’ emphasises the obligation on the magistrate to apply his mind to the application and not act as ‘a rubber stamp’ in authorising an invasive enquiry into the affairs of an individual, the court also recognised that such invasion may be necessary and justified in the interests of justice, provided that it is properly grounded.’

“The duties of a judicial officer when considering and issuing an order in terms of section 205, have been clearly interpreted in, among others, HAYSOM v ADDITIONAL MAGISTRATE, CAPE TOWN AND ANOTHER; S v HAYSOM 1979 (3) SA 155 (C), *S v MATISONN* 1981 (3) SA 302 (A), *S v DE VRIES AND OTHERS* 2009 (1) SACR 613 (C), *PANDAY v MINISTER OF POLICE AND OTHERS* 2012 (2) SACR 421 (KZD) and *S v MILLER AND OTHERS* 2016 (1) SACR 251 (WCC), where it was decided that the function of the judicial officer is not merely that of a ‘rubber stamp’, and that the subpoena must be drawn in such a fashion that it is ‘as narrowly tailored as possible to meet the legitimate State interest of investigating and prosecuting crime.’”

Despite the safeguards built into section 205 as set out above by the Department of Justice, there have been cases detailing the failure of such safeguards. For instance, in *S v Agliotti*,³² the South African Police Service had obtained archived metadata from cellular phones belonging to persons not related to the case. In total, there were 50 lever arch files filled with archived metadata subpoenaed from Vodacom alone. (Vodacom was not the only service provider served with section 205 subpoenas in the case.) Judge Kgomo described the abuse as follows:

“Abuse of the system by the police was demonstrated by Hodes SC during cross-examination of these cellphone ‘experts’. For example, he elicited evidence to the effect that cellphone records of the accused’s attorney; himself, Hodes SC, accused’s counsel herein; his (Hodes’) father’s, also an advocate who has nothing to do with this case; other clients of accused’s counsel, Hodes SC like one Peter Skeet; phones of private attorneys’ firms and private investigator Warren Goldblatt; among many others, were subpoenaed and obtained by the police from the cellphone companies.

This elicited a question from me at one stage to the effect whether if and when this country’s State President’s phone records were subpoenaed, whether they (the cellphone companies) would issue them out without much ado. The answer was that those records would be extracted and handed over without asking another question.

It is my considered view that if this state of affairs did occur or does occur and is allowed to persist, WE SHOULD ALL BE AFRAID, VERY AFRAID!!!”

In *S v De Vries*³³ Judge Bozalek found that the magistrate had granted a section 205 subpoena for archived metadata “largely on the strength of the reputation of the applicant and not considering the merits of the application”, and declared this approach “impermissible”, stating that “[t]he issuing magistrate’s function is decidedly not that of a “rubber stamp”.

³² *S v Agliotti* (SS 154/2009) [2010] ZAGPJHC 129; 2011 (2) SACR 437 (GSJ) (25 November 2010) at paras 138 - 140.

³³ *S v De Vries and Others* (67/2005) [2008] ZAWCHC 38; 2009 (1) SACR 613 (C) (11 June 2008) at paras 14 to 15.

Judge Bozalek also commented on potential shortcomings of the section 205 application placed before the magistrate, which points to a lack in uniformity in applications for section 205 subpoenas:

“Whilst it would not be irregular, in my view, to consider such an application by having regard to no more than the contents of witness statements in the docket, 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.”

Investigative research has documented other instances where section 205 procedures appear to have been blatantly misused to acquire the phone records of high-profile individuals for apparently nefarious purposes. In 2018, investigative journalist Athandiwe Saba learned that a police officer had used a section 205 request to acquire her phone records alleging they related to a suspect in a housebreaking investigation. These phone records later came into the possession of a private investigator.³⁴ In another incident in 2017, a SAPS Captain in the Western Cape faced criminal charges for, among other things, allegedly using section 205 procedures to fraudulently seize the phone records of lawyers, senior police officials, and various private citizens.³⁵

CONCLUSION

The extent to which the misuses seen in *S v De Vries* and *S v Agliotti* occurs is impossible to assess since such abuses appear only to come to light when a surveillance target institutes litigation to contest the use of the relevant metadata as evidence, or when such metadata is presented as evidence in court. Without additional safeguards applied to the section 205 process, the risk for the type of abuse as seen in *S v De Vries* and *S v Agliotti* will likely remain.

Rather, unless the lack of appropriate safeguards in the section 205 processes are addressed as part of the ongoing RICA reform process, it seems likely any resulting reforms will fall short of providing the necessary protections to constitutional rights envisaged by the Court in the *AmaBhungane* judgment.

³⁴ Hunter, at 4.

³⁵ Ibid.

BIBLIOGRAPHY

South African legislation

1. Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002.
2. Criminal Procedure Act 51 of 1977.

South African cases

1. *Panday v Minister of Police and Others* (12044/10) [2012] ZAKZDHC 20; 2012 (2) SACR 421 (KZD)
2. *S v Agliotti* (SS 154/2009) [2010] ZAGPJHC 129; 2011 (2) SACR 437 (GSJ).
3. *S v De Vries and Others* (67/2005) [2008] ZAWCHC 38; 2009 (1) SACR 613 (C).
4. *S v Hasane and Others* (K/S 01/2017) [2020] ZANCHC 28.
5. *S v Matsitela and Others* (78/2017) [2018] ZAFSHC 135.
6. *S v Miller and Others* (SS13/2012) [2015] ZAWCHC 118; [2015] 4 All SA 503 (WCC); 2016 (1) SACR 251 (WCC)

Decisions of regional and foreign courts

1. *Big Brother Watch and Others v The United Kingdom* [2018] ECHR 722 (n.d.)

United Nations reports and resolutions

1. Report of the Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (30 June 2014).

Further reports

1. Annual Report by the designated RICA Judge on the Interception of Private Communications for the Period 2014/2015 to the Joint Standing Committee on Intelligence (October 2015).
2. American Civil Liberties Union of California “Metadata: Piecing Together a Privacy Solution” (February 2014).
3. Report on project 105: Review of Security Legislation, the Interception and Monitoring Prohibition Act 127 of 1992 *South African Law Commission* (October 1999).

Internet sources

1. Australian Government Department of Home Affairs “Data retention obligations”, available at <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations>
2. Hunter “Cops and Call Records: Policing and Metadata Privacy in South Africa” *Media Policy and Democracy Project* (27 March 2020), available at <https://archive.org/details/2003-cops-and-call-records-metadata-and-policing>.
3. Madden “New data retention laws for Ireland” *The Irish Legal News* (14 September 2022), available at <https://www.irishlegal.com/articles/michael-madden-new-data-retention-laws-for-ireland>
4. Privacy International “Stakeholder Report; Universal Periodic Review 27th Session, South Africa: The Right to Privacy in South Africa” (2016), available at https://privacyinternational.org/sites/default/files/2018-04/South%20Africa_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf
5. Right2Know, “MTN, Vodacom, Telkom and Cell C: 30 days to provide surveillance stats” (May 2017) available at <https://www.r2k.org.za/2017/05/30/mtn-vodacom-telkom-and-cell-c-30-days-to-provide-surveillance-stats/>
6. Swart, “Special report: 5G opens the gates for surveillance on steroids” *Media Policy and Democracy Project* (6 April 2021) published in *The Daily Maverick*, available at <https://www.dailymaverick.co.za/article/2021-04-06-5g-opens-the-gates-for-surveillance-on-steroids/>


Media Statements

1. Correspondence to the Daily Maverick from the Department of Justice (May 2017)
2. Portfolio Committee on Police, official media statement (23 March 2023), available at <https://www.parliament.gov.za/press-releases/media-statement-committee-police-says-success-rural-safety-strategy-depends-community-mobilisation>

Annexure A

Gmail - Media Response

2023/04/06, 17:12



Heidi Swart <swart.heidi@gmail.com>

Media Response
1 message

Mahlangu Solomon <SoMahlangu@justice.gov.za>
To: "swart.heidi@gmail.com" <swart.heidi@gmail.com>
Cc: Mahlangu Stephans <StMahlangu@justice.gov.za>, Mathebula Mandla <ManMathebula@justice.gov.za>

Fri, May 5, 2017 at 2:40 PM

Afternoon Mr. Swart Heidi!

Below is a media response to your set of questions.

I hope is on order.

Kind regards

Solomon B Mahlangu

Media Research and Liaison


012 315 8721

072 520 5530

SoMahlangu@justice.gov.za

.....

.....



the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

<https://mail.google.com/mail/u/0/?ik=48d5d20fe9&view=pt&search-f:1566559993352223369&simpl=msg-f:1566559993352223369&mb=1>

Page 1 of 7

MEDIA RESPONSE**ATT: Daily Maverick (Heidi Swart)****05 May 2017****MEDIA ENQUIRY: DAILY MAVERICK: ILLEGAL SECTION 205 CALL RECORD SUBPOENAS****Questions and Response****1. Question 1****1.1 Is the Department aware of flaws relating to the issuing of subpoenas in terms of section 205 of the Criminal Procedure Act in respect of call data?**

The Department is aware of the few judgments where proceedings in terms of section 205 of the Criminal Procedure Act, 1977 (Act 51 of 1977) (the Criminal Procedure Act), were held to be irregular.

1.2 Has the Department attempted to address shortcomings or judicial oversight mechanisms in section 205 proceedings in so far as it relates to call data.

In *NEL v LE ROUX NO AND OTHERS* 1996 (1) SACR 572 (CC), at paragraph 20, the Constitutional Court rejected the contention that section 205 of the Criminal Procedure Act infringes a number of fundamental constitutional rights and held that section 205 was as 'narrowly tailored as possible to meet the legitimate state interest of investigating and prosecuting crime'. The Constitutional Court did not find it necessary to interfere with the procedure envisaged by the section 205 or to prescribe any procedural formality to preserve its constitutionality. The court was mindful of the fact that applications in terms of section 205 demand 'the exercise of invasive and compulsive powers', and are subject only to the

exercise of judicial discretion by the presiding officers after due consideration of the facts disclosed in the application. This judgment, however, preceded the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002) (the RICA), and was not decided on the basis of the applicability of section 205 in relation to call-related information.

Obviously, an application for an order in terms of section 205 can only be considered and issued if the objective of the order is to obtain information in the course of, or to assist in, an investigation of an offence. Section 205 of the Criminal Procedure Act provides for the following safeguards to ensure that this objective is met:

(a) The first safeguard relates to the police official who furnishes the information that forms the basis of the application. If the police official wilfully states information in the application which is false he or she commits an offence.

(b) The second safeguard which is built into the section 205 procedure is that only a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the Director of Public Prosecutions can request a judicial officer to authorise an order in terms of section 205. This in effect means that very senior prosecutors are involved in these applications. In *S v MALIGA* 2015 (2) SACR 202 (SCA) at paragraph 20, the court found that "a prosecutor stands in a special position in relation to the court. The paramount duty of a prosecutor is not to procure a conviction but to assist the court in ascertaining the truth. (*S v Jija and Others* 1991 (2) SA 52 (E) at 67J – 68A.) Implicit herein is the prosecutor's role in assisting a court to ascertain the truth and dispense justice. This, not surprisingly, gels with the stringent ethical rules by which all legal representatives have to conduct themselves in their professional lives". It is therefore the duty of the prosecutor in question to ensure that the application for an order in terms of section 205 is regular.

(c) The third safeguard is that an independent judicial officer must consider the request. The failure of judicial officers to exercise their discretion judicially is the main ground in the few reported cases on which section 205 orders were challenged. In *PANDAY v MINISTER OF POLICE AND OTHERS* 2012 (2) SACR 421 (KZD), at

paragraph 28, the court had the following to say about section 205 orders:

"In *R v Parker* 1966 (2) SA 56 (RA) at 58, although the decision is pre-constitutional, the court recognised that the interest of an individual to privacy is unequal when weighed against the competing interest of justice. It accordingly held that it would not be a proper exercise of discretion if the available facts indicate that the enquiry is to be based on vague supposition and that the magistrate had a duty 'to ensure that the members of the public are not unduly harassed by inquisitions' (my emphasis). Therefore, although the key word 'unduly' emphasises the obligation on the magistrate to apply his mind to the application and not act as 'a rubber stamp' in authorising an invasive enquiry into the affairs of an individual, the court also recognised that such invasion may be necessary and justified in the interests of justice, provided that it is properly grounded."

The duties of a judicial officer when considering and issuing an order in terms of section 205, have been clearly interpreted in, among others, *HAYSOM v ADDITIONAL MAGISTRATE, CAPE TOWN AND ANOTHER*; *S v HAYSOM* 1979 (3) SA 155 (C), *S v MATISONN* 1981 (3) SA 302 (A), *S v DE VRIES AND OTHERS* 2009 (1) SACR 613 (C), *PANDAY v MINISTER OF POLICE AND OTHERS* 2012 (2) SACR 421 (KZD) and *S v MILLER AND OTHERS* 2016 (1) SACR 251 (WCC), where it was decided that the function of the judicial officer is not merely that of a 'rubberstamp', and that the subpoena must be drawn in such a fashion that it is 'as narrowly tailored as possible to meet the legitimate State interest of investigating and prosecuting crime'.

Also see the general comments below under paragraph 3.

2. Question 2

2.1 The Department is not in possession of statistics of the number of section 205 orders which were issued. The lower court judiciary implemented measures to keep records of proceedings in terms of section 205 as was also discussed in *PANDAY v MINISTER OF POLICE AND OTHERS* 2012 (2) SACR 421 (KZD) at paragraphs 12 to 17.

2.2 The Department cannot confirm or deny allegations that the South African Police

Service utilises i2 Analyst's Note Book or the number of police officials which are trained to use the software in question.

2.3 (a) In terms of section 205 of the Criminal Procedure Act, an order may be issued by a judge of a High Court, a regional court magistrate or a magistrate. The designated judge is not involved in proceedings in terms of section 205 of the Criminal Procedure Act and no statutory duty exists which requires the designated judge 'to keep track of or review' proceedings in terms of section 205 of the Criminal Procedure Act.

(b) Section 19(1) of the RICA can be used to apply for archived communication-related information. A judge of a High Court, regional court magistrate or magistrate who issues an archive communication-related direction, must, as soon as practicable thereafter, submit a copy of the application and archived communication-related direction concerned to a designated judge (section 19(7) of the RICA). In terms of section 19(8) of the RICA, the designated judge must keep all copies of applications and archived communication-related directions submitted to him or her in terms of section 19(7) of the RICA, or cause it to be kept, for a period of at least five years. The process provided for in terms of section 205 of the Criminal Procedure Act, in so far as it relates to call-related information, does not provide for a similar process. In terms of section 19 of the RICA, there is no obligation on a designated judge to examine applications for or archived communication-related directions issued in terms of section 19(3) of the RICA.

(c) It is probable that most call-related information is obtained in terms of section 205 of the Criminal Procedure Act. It is mainly in instances where archived communication-related information is required on an ongoing basis, as it becomes available, that section 19 of the RICA is used (see section 15(2) of the RICA).

(d) Only a judge of a High Court, a regional court magistrate or a magistrate may issue an order in terms of section 205 of the Criminal Procedure Act. The designated judge cannot be approach to issue an order in terms of section 205 of the Criminal Procedure Act. This explains the reason why the designated judge does not refer to orders in terms of section 205 of the Criminal Procedure Act in his or her annual report. To our knowledge, it is correct that the categories of directions which are issued by the designated judge in terms of

Chapter 3 of the RICA are not specified in the annual report of the designated judge.

3. General comments

The Department is currently in a process to revise the RICA. Most other countries have also revised their interception legislation to ensure a more open and transparent process which is aimed at protecting the privacy of the communications of persons relative to the legitimate needs of the State to protect its subjects against crime. International developments will be taken into account during this revision process. Section 205 of the Criminal Procedure Act, which was amended by the RICA to provide for the provision of archived communication-related information, will also be considered during the revision process.

Ends

Enquiries: Advocate Mthunzi Mhaga
Spokesperson for the Ministry of Justice and Correctional Services
0836418141
Mediaenquiries@justice.gov.za

Privileged/Confidential information may be contained in this message. If you are not the addressee indicated in this message (or responsible for delivery of the message to such person) you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply E-Mail. Please advise immediately if you or your employer do not consent to e-mail messages of this kind. Opinions, conclusions and other information in this message that do not relate to the official business of the Department of Justice and Constitutional Development shall be understood as neither given nor endorsed by it. All views expressed herein are the views of the author and do not reflect the views of the Department of Justice unless specifically stated otherwise.

Privileged/Confidential information may be contained in this message. If you are not the addressee indicated in this message (or responsible for delivery of the message to such person) you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply E-Mail. Please advise immediately if you or your employer do not consent to e-mail messages of this kind. Opinions, conclusions and other information in this message that do not relate to the official business of the Department of Justice and Constitutional Development shall be understood as neither given nor endorsed by it. All views expressed herein are the views of the author and do not reflect the views of the Department of Justice unless specifically stated otherwise.



image001.jpg
43K