# S v MILLER

## Ruling re Admissibility of Captain Lodewyk Brink's Evidence
## 2 September 2015

**GAMBLE, J**

**INTRODUCTION**

[1] The eight accused are charged with a number of offences under the Prevention of Organised Crime Act, 121 of 1998 ("*POCA*") , and the Marine Living Resources Act,18 of 1998, the core of the State's case being that they collectively ran an enterprise involving the unlawful processing, packaging and export of abalone .

[2] The accused were arrested over a period of 8 months in 2006 (February – October) along with several others. In October 2008 their trial commenced in this Division and at that stage there were some 18 accused before Erasmus J. A number of procedural objections were raised at the commencement of the hearing, all of which were unsuccessful (See S v Chao and others 2009(1) SACR 479 (C))

[3] Certain of the accused then offered pleas of guilty in terms of section 112 of the Criminal Procedure Act, 51 of 1977 ("*the CPA*") and were duly convicted and sentenced. Thereafter the trials were separated and the case continued in regard to the remainder of the accused. The matter was removed from the trial roll and sent back for pre-trial management. During this period certain of the accused skipped bail leading to further delays in the matter. Finalisation of the pre-trial procedures was also delayed

while the parties awaited the outcome of the Constitutional Court decision in the case of Savoi and others v National Director of Public Prosecutions and others 2014(5) SA 317 (CC). That judgment, delivered on 20 March 2014, dealt extensively with the constitutionality of POCA.

[4] Eventually, the matter was sent to trial on 11 August 2014 before this court sitting with assessors. At the commencement of the trial one of the accused, Stanley Dlamini, absconded and after a warrant for his arrest had been issued, the trial continued against the remaining eight accused.

[5] The trial has run in fits and starts for a number of reasons. During the fourth term of 2014 accused number one required neck surgery and counsel for accused number three, seven and eight, Mr Theunissen, was permitted to withdraw due to apparent differences with his clients. These events led to the matter standing down. The matter ran fairly regularly during the first term of 2015 and on 16 March 2015 (the 38th day of the trial) the State called Capt Lodewyk Brink to the witness box to testify regarding, inter alia, his analysis of cellular phone communications between the accused *inter se* as well as with various of the State witnesses and other parties.

[6] It seems that the accused were taken by surprise by this turn of events since no witness statement from Capt Brink was contained in the police docket. After

expressing their frustration at the absence of such a statement to work off counsel were assured that they would be given ample opportunity to digest the evidence and to take instructions thereon before cross-examining. I should mention that the prosecution too was frustrated by this latest development: as lead counsel for the State, Ms Greyling, later put it "both the State and the defence were required to play catch up."

[7] The day before the Easter recess commenced on 26 March 2015 Capt Brink had been in the witness box for six days in examination-in-chief. The court ordered that the matter stand down for three weeks (a week longer than the recess) and defence counsel were thereby offered the opportunity to prepare cross-examination. The evidence-in-chief of Capt Brink then stood down to 20 April 2015 to enable him to consider further documentation and to prepare further documentary exhibits. By agreement with the defence certain other witnesses were interposed while this took place.

[8] When the sitting of the court in the second term recommenced on 20 April 2015 the State completed the evidence-in-chief of Capt Brink. He was then fully cross-examined by counsel for accused number one, Ms Joubert.

[9] At the commencement of the cross-examination for accused numbers 2, 4 and 5, Mr Uijs SC reiterated his earlier frustrations at being unable to manage and understand the evidence and prepare cross-examination of Capt Brink. Mr Uijs then

cross examined the witness for several hours before the court adjourned at its usual time. At that stage the witness was requested by several counsel to conduct certain further enquiries regarding the location of certain cell phone handsets in relation to transmitter base stations and to revert to the court with his conclusions in tabular form. The witness stood down to this end for a week.

[10] When the court then resumed sitting we were informed that Capt Brink had not finished his follow-up work and his evidence stood down further for another week, to 4 May 2015. In the interim further witnesses were interposed.

[11] When the matter recommenced on 4 May 2015 counsel for accused number six , Mr Banderker, informed the court that his client was suspected of having suffered a minor heart attack and upon admission to hospital had been diagnosed with TB. When this was confirmed two days later, the matter was postponed to 3 August 2015, the first day of the third term on which criminal courts sat.

**THE CHALLENGE TO THE EVIDENCE**

[12] A couple of days before the court recommenced sitting on 3 August 2015 Mr Uijs filed a notice of motion on behalf of each of his clients in which it was sought to strike out all of the evidence of Capt Brink relating to cell phone traffic and usage. The notice of motion was supported, not by any affidavit, but by Mr Uijs' detailed heads of argument with annexures. At the start of proceedings the State asked for time to deal

with the notice of motion and the matter stood down yet again. In response to the defence application the State filed a notice of opposition as well as affidavits by the investigating officer, Inspector Potgieter, and Capt Brink. Eventually, on Monday, 24 August 2015 the notice of motion was argued in open court.

[13] The parties agreed that the belated challenge to the admissibility of Capt Brink's evidence should be dealt with by way of a trial-within-a-trial. No *viva voce* evidence was led at the trial-within-a-trial and it was agreed that all of the evidence which had been adduced in the trial so far would be imported into the trial-within-a-trial. It was also agreed that the statements filed by the State in opposition to the notice of motion would stand as written statements submitted under section 213 of the CPA.

[14] Ms Joubert indicated to the court that accused number one did not support nor oppose the application: he adopted a neutral position thereto. Counsel for the remaining accused all stated that their clients supported the application to strike out the evidence.

[15] The challenge to Capt Brink"s evidence was founded on two bases. Firstly, it was alleged that certain cell phone records procured by the State under section 205 of the CPA had been obtained unlawfully since the subpoenas presented to the issuing magistrate in terms of section 205 were allegedly fatally defective. Secondly, it was said that the accuseds' rights to privacy protected under section 14 of

the Constitution of the Republic of South Africa, 1996, had been unlawfully invaded when Capt Brink had accessed the data contained on the accuseds' various cell phones which had been lawfully seized by the police during their arrests. It was contended that this conduct was unlawful because it breached certain statutory provisions to which I shall refer later. Counsel argued that in terms of section 35(5) of the Constitution the evidence therefore fell to be excluded. The section reads as follows –

"*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."*

[16] To fully understand the extent of the objection some further background detail in respect of Capt Brink's evidence is required. After the accused's cell phones (as well as those of certain of the State witnesses) had been lawfully seized Capt Brink prepared subpoenas (hereafter referred to as "*the 205's*") to be issued by the by the magistrate, Cape Town under section 205 of the CPA. These subpoenas directed the responsible officials at Vodacom and MTN, two of South Africa's cellular network service providers ("*SP's*") to hand over to Capt Brink so-called "*itemised billing*" documents in respect of , inter alia, a number of specified cell phone numbers, including numbers of most of the accused and certain of the State witnesses

[17] This information, once supplied by the SP's, 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

[18] 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.

[19] The objection of the defence, then, is that the primary data which is loaded onto the police computer was unlawfully obtained in breach of section 205. In addition, it is said that Capt Brink breached the accused's rights of privacy by interpreting the data furnished to him, and in particular that he should not have had access to any data on any cell phone lawfully seized by the police without prior authorisation. I turn then to the 205 issue.

**SECTION 205**

[20] The relevant provisions of section 205 read as follows –

> "*(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 authorised 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 authorised 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."*

[21] Section 205 was extensively used in the pre-constitutional era for the examination of persons (often members of the media) to obtain information regarding the sources of their reports , or generally to glean information about the commission of an offence. The leading cases dealing with section 205 from that era emanate from this Division and include Haysom v Additional Magistrate, Cape Town and another 1979(3) SA 155 (C) and S v Matisonn 1981(3) SA 302 (A). In the democratic era the Constitutional Court has confirmed that the section is constitutional (See Nel v Le Roux NO and others 1996(3) SA 562 (CC). In deciding the case that Court, fully conscious of the invasions of the various protected rights in the Bill of Rights which the section caused, found that, if properly applied, section 205 was an important evidence gathering mechanism in the preparation of criminal prosecutions.

[22] In Haysom the court held that, once the subpoena had been authorised it could be assumed, in the absence of evidence to the contrary, that the magistrate authorising issue had done so after the exercise of a proper judgment. In the present matter the magistrate had before him the documents placed before this court in terms of section 213. Once he was satisfied, upon perusal of those documents, that the

person subpoenaed was likely to give the material evidence referred to in the subpoena, the magistrate was under a duty to authorise the subpoena. In the event that the person so subpoenaed wished to attack the validity of the subpoena it would be up to that person to produce countervailing evidence to persuade the magistrate that the subpoena was not validly authorised. I do not understand Matisonn to have overruled these principles.

[23] Counsel for the defence relied heavily on one of the judgements of Bozalek J in S v de Vries and others in this Division in regard to a ruling on a 205 subpoena. The judgment is reported at 2009(1) SACR 613 (C). In that matter the court set aside a 205 subpoena after hearing oral evidence from the magistrate. That evidence unequivocally established that the magistrate had not applied his mind properly to the application for the subpoena but seems rather to have granted it because he held the petitioning prosecutor in high regard. I agree with the approach of the learned judge, based as it is on the judgments in Haysom, Matisonn and Nel that the function of the magistrate 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."*

[24] In this matter the magistrate had before him the affidavits furnished by the police in which the alleged offences are described in significant detail. In addition, the magistrate had before him the affidavit of a potential accomplice witness (Salvin Africa). The argument for the defence is premised on the wording of the completed subpoena.

It is said that the "*finished product*" suggests that the magistrate failed to apply his mind properly to the document before him. That submission is based on a number of factors. Firstly it was said that the description of the alleged offences in respect whereof material was sought was not accurate. Counsel accepted that the detail furnished was comprehensible and that this factor on its own was not sufficient to render the subpoena invalid. Then it was said that the language of the subpoena (which was to be served on a female) was inappropriate in that it vacillated between the masculine and feminine. The document contains the word "*responsible person*" as the person sought to be subpoenaed. However, the person's name is thereafter spelt out in full in brackets.

[25] But the thrust of Mr Uijs' attack on the subpoena relates to the date upon which the person subpoenaed may appear before the magistrate if the subpoena is to be attacked or resisted. That date is given as 31 November 2006 - a non-existent date on our calendar. It was said that this was the clearest indication that the magistrate had not applied his mind to the subpoena. In my view the error is an understandable one. Common experience in the preparation of court documents and judgments, remind one how easy it is to overlook a typographical error, notwithstanding that the document has repeatedly been perused or edited. Indeed Mr Uys candidly conceded when the application was initially brought that he himself had overlooked the mistake in the subpoena several times before he picked it up.

[26] In considering whether a non-existent date should necessarily render the subpoena invalid, one must have regard to the purpose of such date. The 205 does not

require the person subpoenaed to appear on a particular date without more. If the person is willing to provide the documentation sought to the police that is the end of the matter and the date becomes irrelevant. It is only if the person wishes to oppose the subpoena that the date becomes relevant. Then the person may appear, legally represented if she so wishes, and attempt to persuade the magistrate why she should not be ordered to hand over what was sought. And, were that to happen, common sense tells one that a responsible person would approach the magistrate on either 30 November or 1 December and ask for an opportunity to be heard. An incorrect date would not in my view permit the person subpoenaed to simply ignore the request contained therein.

[27] Mr Uijs asked the court to have regard to the cumulative effect of these shortcomings in the subpoena and to conclude beyond reasonable doubt that the subpoena was invalid. In my considered view this is not the only reasonable inference to be drawn in the circumstances and I am not satisfied that the defence has established that the magistrate failed to properly consider the documents or to exercise his discretion properly. The objection must be determined on the evidence before the court and what that evidence shows is that a number of documents detailing the alleged offences were placed before the magistrate. Those documents were placed before this court by agreement in terms of section 213 and the court is entitled to accept the contents thereof accordingly. Neither the State nor the defence sought to rely on the provisions of section 213(4) to enable the magistrate in question to be cross-examined in regard to the subpoena. Accordingly, there is no direct evidence before this court that the magistrate failed to apply his mind to the document placed before him by the public

prosecutor and to that extent this case is entirely distinguishable from de Vries.

[28] In his argument in reply Mr Uijs raised one further point. He observed that the information contained in the documentation specified in the subpoenas, in some instances, went beyond the detail of the subpoena. So, for example, the SP's provided the so-called IMEI number which is the unique identification number of every cell phone, much like an individual's identity number. Mr Uijs pointed out that this number was not requested in the majority of the subpoenas issued and that the SP's had provided the information of their own volition. Ms Greyling pointed out that the SP's had collated the information sought in tabular form printed on ordinary A4 pages. This she observed was the customary way in which itemised billing was presented to the police and the way in which it was normally placed before the court. In that regard Ms Greyling is clearly correct - this court has customarily encountered the documents in that form.

[29] To the extent that information not specifically sought in the 205 has been placed before the court it is arguable that such information falls outside the ambit of the subpoena and may therefore be unlawfully before the court. In such circumstances Ms Greyling requested the court to receive the evidence under the exception contained in section 35 (5) of the Constitution. I am prepared to assume, without deciding, that the information referred to has found its way into the court record unlawfully. I am unable to say at this stage that the admission of this evidence has, or will, render the trial unfair. I am however persuaded that it would be detrimental to the administration of justice to exclude such evidence from the record. In the first place, a case such as this should be

decided on all the available evidence. Furthermore, there is no particular secret in an IMEI number. Counsel were agreed that many cell phones contained that number on the back of the handset's casing. It can also be obtained from the cell phone itself by pressing in a code which is widely known.

[30] Having regard to the foregoing I am not persuaded that the defence has established that the subpoena was wrongly issued or that it falls to be declared invalid. The first attack by the defence on the admissibility of Capt Brink's evidence, that the subpoenas were unlawfully issued, must therefore fail.

**THE COMMUNICATIONS RELATED STATUTES – ECTA & RICA**

[31] For the second leg of the defence argument , Mr Uijs referred the court to 2 statutes – the Electronic Communications and Transactions Act 25 of 2002 ("*ECTA*") , which came into operation on 30 August 2002 , and the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ("*RICA"*) , which came into operation on 30 September 2005. I shall commence with the latter.

[32] Section 12 of RICA provides as follows –

***"12 Prohibition of provision of real-time or archived communication-related***

***information***

*Subject to this Act, no telecommunications service provider or employee of a telecommunication service provider may intentionally provide or attempt to provide any real-time or archived communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such real-time or archived communication-related information relates."*

[33] It will be observed that section 205(1) which has been set out above contains a cross-reference to section 15 of RICA. The latter section reads as follows –

> ***"15 Availability of other procedures for obtaining real-time or archived communication-related information***
>
> *Subject to subsection (2), the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in sections 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act.*
>
> *Any real-time or archived communication-related information which is obtained in terms of such other Act may not be obtained on an on going*

*basis."*

[34] Counsel were in agreement that the prohibition contained in section 12 of RICA was ameliorated by section 15 thereof. In other words if the police wish to obtain cell phone records from MTN or Vodacom they may do so provided they make use of a 205, and provided further that a separate subpoena is issued in respect of each individual request. In light of my finding regarding the validity of the 205's, and subject to the aforementioned qualification under section 35(5) of the Constitution, there can be no debate about the lawful possession by the police of such records in this case. The crux of the objection raised by Mr Uijs on behalf of the defence was what could be done with such records once they had been handed over by the SP's. I shall revert to this question later once I have dealt with the seizure of cell phone handsets and other items by the police.

**SEARCH AND SEIZURE**

[35] During the various arrests which gave rise to the initial prosecution, and later this prosecution, the police seized a number of cell phones from persons present on the respective scenes. They also seized on occasion unused SIM cards for cell phones contained in what were referred to as "*starter packs*", and the remainders of used starter packs from which details of SIM cards and cell phone numbers could be established. Some of these arrested persons were subsequently prosecuted, some became State witnesses in terms of sec 204 of the CPA ("*204's*") and others were left

to continue life as before.

[36] In conducting the various raids the police acted generally in terms of Sec 20 of the CPA which is to the following effect –

> ***"20. State may seize certain articles***
>
> *The State may, in accordance with the provisions of this Chapter, seize anything (in this Chapter referred to as an article) –*
>
> *(a) which is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the Republic or elsewhere;*
>
> *(b) which may afford evidence of the commission or suspected commission of an offence, whether within the Republic elsewhere; or*
>
> *(c) which is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence."*

[37] Sec 20 sets out the general powers of the State to seize articles in order

to obtain evidence for the institution of a prosecution or the consideration of instituting such a prosecution. Those general powers are exercised under the specific powers granted under sections 21, 22, 23 and 24 of the CPA which empower the seizure of articles in terms of a search warrant, without a search warrant, from an arrested person and during the search of premises respectively. As I have said it is common cause between the defence and the State that the police obtained possession of the cell phones, SIM cards and starter packs lawfully and it is not necessary to consider the provisions of sections 21 to 24 further.

[38] Ms Greyling argued that the general power conferred under section 20 to seize "*anything*" entitled the police to have access to the contents of any such article seized without further ado. So, for example, she submitted that if a diary or photo album had been seized , the police could page through them and if a locked safe had been seized the police could call in a locksmith to open it in order that they could see what was inside. I did not understand Mr Uijs to take issue with this approach. He accepted that this was the sensible interpretation to be placed on the search and seizure provisions of the CPA. However, he argued, that the specific provisions of ECTA required the police to take further steps in regard to cell phones given the fact that they are in essence these days mini computers, containing as they do facilities such as word processing software with which to send emails, search programs using search-engines and generally storing information, music and photographs. It is therefore necessary to

have regard to the relevant provisions of ECTA upon which Mr Uijs relies.

[39] The genesis of the argument is to be found in section 86 of ECTA. It is contained in the penultimate chapter of the Act (Chapter XIII) which bears the heading "*CYBER CRIME"*. That chapter has its own definition provision contained in section 85 which reads as follows –

> ***"85 Definition***
>
> *In this Chapter, unless the context indicates otherwise –*
> *"access" includes the action of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data."*

[40] Then follows section 86(1) which is to the following effect –

> ***"86 Unauthorised access to, interception of or interference with data***
>
> *(1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any*

*data without authority or permission to do so, is guilty of an offence."*

[41] Mr Uijs argued that the "*authority"* contemplated under section 86(1) rested solely with the *"cyber inspector"* contemplated for appointment in section 80 of ECTA. The immediate problem with that approach is that notwithstanding the operation of ECTA for some 13 years no cyber inspector has yet been appointed. The anomaly which then arises, so it is argued, is that the police may simply not access any data on a lawfully seized cell phone. If one poses the question why the police would wish to seize a cell phone from a suspect, if not to access the names and addresses stored thereon , or to view the in-coming or out-going call logs , counsel's submission has far-reaching consequences for the police in the investigation of crime. It is therefore necessary to analyse ECTA to establish whether counsel's interpretation is in fact what the Legislature intended.

**THE APPROACH TO STATUTORY INTERPRETATION**

[42] The so-called "*golden rule"* of statutory interpretation has traditionally been to ascertain the intention of the legislature, primarily by giving the words of the provision under consideration their ordinary grammatical meaning.(Manyashe v Minister of Law and Order 1999(2) SA 179 (SCA) at 185 B-C) However as Van Heerden JA points out , with reference to all the leading appellate cases , in Bastian Financial Services (Pty) Ltd v General Hendrik Schoeman Primary School 2008(5) SA 1 (SCA) at para's 17 – 20 , the contemporary approach is to promote a "*purposive construction*"

of a statutory provision. Accordingly, where the words of a statute are not linguistically limited to a single ordinary grammatical meaning, one must have regard to the context in which these words are used in the Act in question, seen against the background of the purpose of the legislation. (See also LAWSA Vol 25 Part 1 2nd ed at p290 *et seq*). Moreover, sec 39(2) of the Constitution enjoins a court to promote the spirit, purport and objects of the Bill of Rights in interpreting any legislation.

[43] In my view, it is impermissible to peer at section 86 through blinkers as the defence sought to do. The entire Act must be examined contextually , and the interrelationship of the parts making up the whole must be considered.

[44] A purposive approach requires the court to consider the primary purpose of ECTA. That purpose is established by first having regard to the long title of ECTA which reads as follows –

*"To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith."*

[45] One then turns to the definitions section where the word "*data"* is defined as "*electronic representations of information in any form".* I am prepared to accept , as suggested Mr Uijs that, broadly speaking, this definition could include the information stored on a cell phone's list of contacts, any notes saved thereon or photographs taken with a cell phone and stored in its memory bank.

[46] The next section of relevance is section 2 of ECTA which details the objects of the Act. There are some eighteen of them set forth as follows –

***"2 Objects of Act***

*The objects of this Act are to enable and facilitate electronic communications and transactions in the public interest, and for that purpose to-*

*(a) recognise the importance of the information economy for the economic and social prosperity of the Republic;*

*(b) promote universal access primarily in underserviced areas;*

*(c) promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic;*

*(d) remove and prevent barriers to electronic communications and transactions*

*in the Republic;*

*(e) promote legal certainty and confidence in respect of electronic communications and transactions;*

*(f) promote technology neutrality in the application of legislation to electronic communications and transactions;*

*(g) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;*

*(h) ensure that electronic transactions in the Republic, conform to the highest international standards;*

*(i) encourage investment and innovation in respect of electronic transactions in the Republic;*

*(j) develop a safe, secure and effective environment for the consumer, business and the government to conduct and use electronic transactions;*

*(k) promote the development of electronic transactions services which are responsive to the needs of users and consumers;*

*(l) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities and, areas and the disabled are duly*

*taken into account;*

*(m) ensure the compliance with accepted international technical standards in the provision and development of electronic communications and transactions;*

*(n) promote the stability of electronic transactions in the Republic;*

*(o) promote the development of human resources in the electronic transactions environment;*

*(p) promote SMMEs within the electronic transactions environment;*

*(q) ensure the efficient use and management of the .za domain name space; and*

*(r) ensure the national interest of the Republic is not compromised through the use of electronic communications.'*

[47] Section 3 of the Act is a particularly important provision since it deals expressly with interpretation –

"*This Act must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act.*"

[48] Chapter VIII of ECTA deals with the protection of "*personal information".* The latter phrase is extensively defined in the definitions clause (which I shall not recite to avoid prolixity) but that definition does not expressly include names, addresses and cell phone numbers of other persons. In addition the protection of personal information afforded by this Chapter only applies to such personal information as has been obtained through an electronic transaction.

[49] Ms Greyling drew the court's attention to section 15 of ECTA which deals with the admissibility and evidential weight of data messages. The following provisions are of relevance here –

> *"15(1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-*
>
> *(a) on the mere grounds that it is constituted by a data message;"*

[50] Finally, I must deal with the argument presented by Mr Uijs in regard to section 81(2) of the Act. Under the general heading *"81* Powers of cyber inspectors*"* there is the following –

> *"(2) Any statutory body , including the South African Police Services, with*

*power of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector to assist it in an investigation: Provided that –*

*(a) the requesting body must apply to the Department [of Communications] for assistance in the prescribed manner; and*

*(b) the Department may authorise such assistance on certain conditions."*

[51] Mr Uijs submitted that this section supported the argument that the police could only access cell phone data upon the authority of the non-existent cyber inspector after following the necessary procedure prescribed by the Department of Communications. I do not agree. Section 81(2) contains the important word *'may'* which is indicative of a permissive power to ask for assistance (with the correlative power of the Department to offer assistance conditionally), rather than a peremptory directive that that the police "*shall*" apply for such assistance in all instances where they wish to access cell phone data. In any event, given the importance of speedy investigatory steps in the fight against crime it seems counter-productive to require the police to follow a bureaucratic procedure to access digital information, a procedure which would not be required in respect of non-digital evidential material.

[52] Having regard then to the Act in its entirety, and in particular the sections to which I have referred above, I am driven to conclude that the main purpose of ECTA is to regulate electronic commercial transactions and communications related thereto. In this regard the State referred the court to a journal article written by Associate

Professor Julien Hofman of the University of Cape Town in 2006 SACJ 257. The author explains the background to ECTA , pointing out that it is based on the United Nations Commission on International Trade Law Model Law on Electronic Commerce (the so-called "*Model Law*").

> *"The Model Law was drafted to promote electronic commerce by providing an electronic equivalent for written, signed and original documents. It does this by adopting what it calls a functional equivalent approach. Functional equivalence recognises the differences between written and electronic communication. Rather than using a legal fiction to create an artificial identity between the two, the functional equivalent approach regulates electronic documents so they can perform the same commercial functions as non-electronic documents.*
>
> *…..(The) functional equivalence of data messages as evidence is clearly necessary to make the functional equivalence of data messages as documents effective. This will ensure a "media-neutral environment" for anyone relying on electronic evidence. It will neither discriminate against those transacting electronically nor give them an unfair advantage. This approach not only respects international law and encourages electronic commerce. It also does away with the incentive to engage in "format shopping".*

It is most instructive in my view to note the author's repeated references to "electronic commerce".

[53] Prof Hofman deals extensively in this article with the import of section 15

of ECTA in relation to the admissibility of data messages in civil and criminal proceedings and, in particular, to problems occasioned by the rule against the admission of hearsay. It is not necessary for the purposes of this ruling to go into any detail of the discussion on that score other than to say that the basis for the discussion is the relevance of such evidence in documents dealing with electronic commerce. However, there is some interesting discussion in relation to search warrants.

"*Data messages not transmitted but stored on a computer will not fall under the interception directions in RICA. Anyone who needs such information as part of a criminal investigation will have to apply for a search warrant in terms of chapter 2 of the Criminal Procedure Act or other legislation that provides for search warrants.*

*Section 20(b) of the Criminal Procedure Act allows the State to seize 'anything (in this Chapter referred to as an article) that may afford evidence of the commission or suspected commission of an offence whether within the Republic or elsewhere". "Anything" has been held to extend to documents and money and will certainly extend to a computer or hard drive in which messages are stored"*

The last sentence in this extract from the article seems to suggest that there is authority ("*has been held*") for the submission. However in footnote 82, which is the basis for the submission, the author points out that *"there have been high profile cases where search warrants have been used to seize computers and the data on computers but none seem to have found their way into the law reports".*

[54] The 2004 judgment of Thring J in this Division, which traversed this point

in part, was only reported in 2007 and would not have been readily available to the author in 2006 (See Beheersmaatskappy Helling I NV and Others v Magistrate , Cape Town and Others 2007(1) SACR 99 (C)). That matter involved a request by a foreign government for the seizure of electronic information stored in computers in Cape Town for purposes of litigation in the Netherlands. The police had removed a number of computers at the premises of the applicant company in Mowbray and its employees in Clovelly and Table View. The computers were subjected to what was called an "*off-site search*" and data stored thereon was copied for onward transmission to the Netherlands. The searches had been conducted under warrants issued by magistrates in terms of sections 20 and 21 of the CPA read in conjunction with the provisions of the International Co-operation in Criminal Matters Act 75 of 1996. The applicants applied to set aside the warrants on the basis that the police had exceeded the powers given to them in terms of the warrants. In upholding the application Thring J found that it was unnecessary to remove the computer central processing units from the office premises in Mowbray to copy them and that in so doing the police had unnecessarily disrupted the business of the applicant. It was held that an off-site search was not necessary and that the relevant data could have been retrieved by the police at the applicant's premises. The warrants were therefore set aside on that basis , but it is important to note that neither the applicant nor the court were in any way concerned with the fact that data was ultimately downloaded off the computers.

[55] While the case is not entirely in point, I consider it useful authority for the principal submission made by Ms Greyling – that the reason that a cell phone is seized in a case such as this is to enable the police to access and examine its contents, be

they phone numbers and addresses, SMS messages, emails or photographs. Possession of the instrument *per se* would be of no assistance to an organised crime investigation such as was undertaken here. Similarly in Beheermaatschappij Helling , the court did not question the lawfulness of the accessing and downloading of data on the computers as such but rather the manner in which it was done.

**CONCLUSIONS REGARDING THE APPLICATION OF ECTA**

[56] Reverting to the provisions of ECTA, I am not persuaded that it was the intention of the Legislature when passing that Act to criminalise or proscribe the accessing of cell phone data by the police in circumstances where the instrument had been lawfully taken into possession during the course of a criminal investigation. I say so for the following reasons.

- Firstly, the provisions of section 86 relied on by Mr Uijs are contained in a chapter of ECTA called "*Cyber Crime"*. The section when read in context is aimed at criminalising the interference (in a number of defined ways) with data on computers that have been used either in the course of electronic commerce or specifically for computer-based crime, such as fraud, forgery or extortion, to which reference is made in section 87. The recent press reports of a sophisticated mobile electronic bugging and interception device dubbed "*The Grabber*" which is used to gain access to bank accounts , cell phone messages and the like, and which was evidently seized by the police, would fit the ordinary description of the term "*cyber crime"'*.

I should mention, too, that the Government has very recently published for comment by 30 November 2015 the Cybercrimes and Cybersecurity Bill. This is a very comprehensive piece of draft legislation running to some 68 sections which details the nature and extent of what is considered to be cybercrime, associated criminal contraventions and penal sanctions. If passed in its present form it will repeal and replace, *inter alia,* sections 85 – 90 of ECTA. While it is still early days in the preparation and passage of this Bill , it must be said that in its present guise it is certainly arguable that the Bill would not seek to penalise the police conduct complained of in this matter.

- Secondly, there is the proviso in section 3 (the interpretation clause) of ECTA which specifically preserves the statutory and common law powers of search and seizure available to the police. If the purpose of the seizure of a cell phone is to access the data stored on it, and the police have complied with the search and seizure provisions of the CPA, they are, in my view, entitled to do the obvious thing that any police officer in possession of a seized object would do – examine it for purposes of establishing its potential use in an offence and the subsequent criminal prosecution of such offence. The situation is no different to the seizure of a bloodied knife being sent for finger print and DNA analysis, a photo album being viewed for identification of potential suspects depicted therein, or a telephone/address book being studied to view the handwritten entries therein. The preservation of the existing search and seizure powers in favour of the police contemplated in this section clearly remove conduct in accordance with such powers from the ambit of cybercrime contemplated by ECTA.

- Thirdly, and in any event, there is the very wording of section 86(1) which criminalises the accessing or interception of data, only in circumstances where this occurs "*without authority*". (The subsection is to be read in conjunction with the definition of "*access*" in section 85 which covers the innocent accessing of data and the continued use once thereof the accessor has gained knowledge of the fact that access was prohibited.) The section in question does not seek to criminalise a person accessing data under "*authority*". Given the provisions of section 3 to which I have just referred , such authority would of necessity include a search sanctioned by section 20 of the CPA , and not be limited to the powers of search and seizure available under section 82 of ECTA to a non-existent cyber inspector.

- Fourthly, and in any event, there is the further provision in section 86(1) of ECTA which, in my view, legitimises access to data pursuant to the granting of 'permission' to the police to access such data in a cell phone as they may require.

- Fifthly, and in any event, there are the provisions of section 84 of ECTA which permit any person who has obtained access to information under Chapter XII of ECTA (which is titled "*Cyber Inspectors*") to disclose such information to another for purposes of the prosecution of an offence.

**PERMISSION GRANTED BY ACCUSED 2 & 4**

[57] I referred above to the furnishing of permission to a person to access data. The facts of the present case are that accused number two, Mr van Rensburg , was aware of the fact that the police were intent on arresting him. Accordingly, he surrendered himself to the police at a police station in the presence of his attorney. He willingly handed over to the arresting officer his cell phone which he had taken along with him. Given what I have said above in regard to the purpose of the seizure of a cell phone in a matter such as this , there could have been no doubt in the mind of Mr van Rensburg why the police wanted his phone. Capt Brink recorded that this cell phone had no PIN ("*Personal Identification Number"*) thereby removing any restriction on the police obtaining access to the instrument. In such circumstances , by handing over a phone *sans* PIN without protest or objection, I am satisfied that on the evidence now before the court, accused number 2 tacitly gave "*permission*" as contemplated by section 86(1) of ECTA for the police to access the data.

[58] A similar situation applies to accused number 4, Mr du Toit. He was arrested at his house in Bellville by the police after a raid at a house in Durbanville. During the arrest (the legality whereof is not in issue) Mr du Toit handed 2 cell phones to the arresting officer – one in working condition and the other broken. In respect of the working phone Capt Brink's documents contained in Exhibit 3 (and in particular Exh 3.49) indicate that the phone's PIN number was furnished to the police by Mr du Toit. Given that the PIN number has to be entered into the phone to afford access to the data thereon , I consider that on the evidence now before court Mr du Toit also furnished the necessary permission contemplated by section 86(1).

***" FORBIDDEN FRUIT "***

[59] Mr Uijs drew the court's attention to a recent decision of the United States Supreme Court which dealt with the seizure of cell phones and the subsequent accessing of data thereon by the law enforcement authorities. (See Riley v California 573 US (2014). This case was, very properly, drawn to the defence's attention by the State. Mr Uijs reminded the court of section 39(1)(c) of the Constitution which enjoins a court to have regard to foreign jurisprudence where appropriate, and urged the court to apply the majority decision of that court which excluded the data so accessed. Mr Uijs was unable to assist the court with the applicable rules of evidence which obtained in California where this matter originated. However, he asked the court to consider that it was now required to apply the doctrine commonly referred to as the "*fruits of the poisoned tree*" and exclude the evidence on that basis. The doctrine is to the effect that once the procurement of evidence is in any way tainted by illegality , such evidence must be excluded without more.

[60] In de Vries at para 28, Bozalek J was similarly urged to apply the doctrine. His Lordship refused to do so pointing out that the doctrine does not form part of our law. (See S v Melani and others 1996 (1) SACR 335 (E), S v Marx and another 1996 (2) SACR 140 (W) and S v Malefo en andere 1998(1) SACR 127 (W)). Indeed in Malefo , after a detailed consideration of both local and foreign authorities, the court observed that not only was the doctrine a rigid exclusionary rule that was at odds with our law (and in particular the provisions of section 35(5) of the Constitution), but that it had been

roundly criticised in America whence it came. In the circumstances I decline to follow the majority opinion in Riley .

[61] That having been said , Ms Greyling drew the Court's attention to the minority concurring opinion of Justice Alito in Riley in which he bemoaned the natural consequences of the majority opinion, while noting the following anomaly which is the hallmark of the "*'poisoned fruit* ' doctrine .

> *"I agree that we should not mechanically apply the rule used in the pre-digital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests.*
>
> *The Court strikes this balance in favour of privacy interests with respect to all cell phones and all information found in them, and this approach leads to anomalies. For example, the Court's broad holding favours information in digital form over information in hard-copy form. Suppose that two suspects are arrested. Suspect number one has in his pocket a monthly bill for his land-line phone, and the bill lists an incriminating call to a long-distance number. He also has in his wallet a few snapshots, and one of these is incriminating. Suspect number two has in his pocket a cell phone, the call log of which shows a call to the same incriminating number. In addition, a number of photos are stored in the*

*memory of the cell phone, and one of these is incriminating. Under established law, the police may seize and examine the phone bill and the snapshots in the wallet without obtaining a warrant, but under the Court's holding today, the information stored in the cell phone is out.*

*While the Court's approach leads to anomalies, I do not see a workable alternative. Law enforcement officers need clear rules regarding searches incident to arrest, and it would take many cases and many years for the courts to develop more nuanced rules. And during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change. "*

[62] Fortunately our law is not hit by these sorts of anomalies because of the provisions of section 35(5) of the Constitution. Through the considered application of that section, our courts are indeed able to address the issue of privacy which is invaded through access to data on seized cell phones, and the investigation of crime which is so necessary in a country like ours with its notoriously high crime rate and disregard for the rights of others, by attempting to achieve some sort of balance.

**APPLICATION OF SECTION 35(5) OF THE CONSTITUTION**

[63] And so I turn to the last aspect which falls to be considered in the defence's objection to Capt Brink's evidence, the applicability of section 35(5) of the

Constitution. The section applies at 2 levels in this case. Firstly, in the event that the evidence was seized unlawfully in violation of a right protected under the Bill of Rights, and secondly, even if it was seized lawfully, the section applies because the accessing of stored data on a cell phone is *prima facie* an invasion of the right to privacy protected under section 14 of the Bill of Rights contained in Chapter 2 of the Constitution. (See de Vries at para 65). I say, *prima facie,* because it is difficult to conceive that accused numbers 2 and 4 could continue to assert the right to privacy where they had willingly handed over their cell phones to the police and afforded them access to the contents thereof whether ECTA applied or not.

[64] The default position under section 35(5) is that such evidence falls to be excluded if it would "*render the trial unfair or otherwise be detrimental to the administration of justice."* A court is therefore required to undertake a balancing act between the competing rights in considering all the relevant circumstances and apply a value judgment which inevitably brings about considerations of the interests of the public and the administration of justice (See S v Pillay and others 2004(2) SACR 419 (SCA) para 85 *et seq.*)

[65] The task of the court in applying the predecessor of this section under the Interim Constitution of 1993 (section 25(3)) was described thus by Kriegler J in the leading decision of the Constituional Court , Key v Attorney-General,Cape Provincial Division and another 1996(2) SACR 113 (CC) at 120g –

*"[13] In any democratic criminal justice system there is a tension between, on the one hand, the public interest in bringing criminals to book and, on the other, the equally great public interest in ensuring that justice is manifestly done to all, even those suspected of conduct which would put them beyond the pale. To be sure, a prominent feature of that tension is the universal and unceasing endeavour by international human rights bodies, enlightened legislatures and courts to prevent or curtail excessive zeal by State agencies in the prevention, investigation or prosecution of crime. But none of that means sympathy for crime and its perpetrators. Nor does it mean a predilection for technical niceties and ingenious legal stratagems. What the Constitution demands is that the accused be given a fair trial. Ultimately, as was held in Ferreira v Levin [NO 1996(1) SA 984(CC)], fairness is an issue which has to be decided upon the facts of each case, and the trial judge is the person best placed to take that decision. At times fairness might require that evidence constitutionally obtained be excluded. But there will also be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted."*

[66] In arguing that the court should exclude the contested evidence , Mr Uijs laid great stress upon the late emergence of the cell phone evidence. He complained that this caused great injustice to the accused who are now required almost 10 years later to remember details of telephone calls which they were never warned to remember. Also, said Mr Uijs, the recall of State witnesses would be necessitated

thereby prolonging the matter. Finally, it was said that the accused were not in possession of the necessary software to verify the correctness of Capt Brink's conclusions and that the defence had been confronted with piles of documentation.

[67] While the protraction of the case has on occasion been due to systemic problems which are part of long trials involving multiple accused (illness and disagreement with legal representatives) I cannot lose sight of the fact that the accused too have adopted positions , perhaps strategies, which have led to the case taking long to conclude. There are ways to avoid the leading of *viva voce* evidence – for example admissions can be made. The accused all pleaded not guilty and offered no plea explanations. That is their right under the CPA, but this of necessity means that the State is obliged to take the long route to establish their guilt. We have all (I think) come to accept in this matter that this is going to be a very long trial. When the accused have needed time to consult their legal representatives, or the latter have needed time to prepare, they have been accommodated accordingly. I see nothing unfair in the further protraction of this case – it is a complex and detailed matter which will take long to complete.

[68] It is apposite also to mention that the application to strike out the evidence comes at a very advanced stage of the proceedings. The witness has completed his evidence-in-chief and has been cross-examined in part. The application was launched, not at the beginning of his evidence, nor when he stood down to do further investigation at the request of the defence, but only when the court was ready to recommence sitting after yet another lengthy "*systemic delay*". To his credit, Mr Uijs informed the court with

his customary frankness, that consideration of the 205 and ECTA points had only occurred to him sometime in mid-June, almost as if by way of late afterthought.

[69] As to the objection regarding the late entry of the evidence and the bulky nature thereof, this is undoubtedly a factor to be considered. The court does not know why it comes so late – perhaps it has something to do with the defences put up by the accused during cross examination of State witnesses which has alerted the State to evidence to disprove the allegations? What the court does know is that both sides have had to play catch-up, as it were. That is also very much a systemic problem in a long and complex trial involving multiple scenes of crime and the linking up of the various role players. The thrust of the cell phone records has been, it seems (and I must hasten to add that I do not wish to be heard to be evaluating it at this stage) to demonstrate which role players were in contact with each other. It does not seem to me to be particularly relevant (save for a few incidents) when such calls were made. Rather, it seems that the volume of calls may be of importance to the State. If that is so, then Mr X will know if he ever phoned Mr Z or not, and will be able to instruct his counsel accordingly. And, if there be doubt, the hard copies of the itemised billings can be consulted for purposes of verification. Having considered all the relevant circumstances, I am not persuaded that the accused's fair trial rights have been, nor will be, affected by the introduction of Capt Brink's evidence.

[70] Section 35(5) also enjoins the court to consider the administration of justice and the possible detrimental effect thereon should the evidence be excluded.

The unchallenged evidence thus far shows that huge quantities of abalone have been stripped from our coastline and have found their way to the Orient where abalone is a prized delicacy. The resource has been shown to be sorely depleted and there can be little debate that the law abiding public would expect those responsible therefor to be brought to book. The accused are charged under POCA which predicates that they have been involved in a criminal enterprise. The cell phone is an integral part of modern day life, and there are very few people who do not make use thereof. It provides instant, mobile and private communication to the users. The cell phone is ideally suited to the commission of crime, whether for common law offences or under the more complex regime of POCA. Indeed, hardly a day goes by in this court that we do not read or hear of the involvement of cellular communication in the commission of crime.

[71] As Kriegler J suggested in Key , the ordinary law-abiding members of the public expect the criminal courts to do their work properly – to acquit where there is reasonable doubt and to convict where there is not. If in the process of the commission of a string of offences the State alleges that the suspects before court have made extensive use of cellular communication in furtherance of their illegal enterprise (and of course I make no finding in that regard at this stage) then the interests of justice, in my considered view, demand that it should be afforded the reasonable opportunity to present that evidence. After all, nobody has obliged anyone to make use of cellular communication in a case such as this. If any of the accused elected to do so, they willingly ran the risk that those communications may later be detected by the authorities.

[72] I further have regard to the fact that the conduct of the police throughout

in regard to the cell phone evidence has been *bona fide.* The requisite warrants were applied for and obtained prior to the search and seizure operations , save (as I recall) for the raid in Bellville South where the police had probable cause. In assessing the cell phone data Capt Brink appears, at all material times, to have genuinely believed that he was entitled to do so. Indeed, conscious of the fact that he was dealing with evidence that could be considered to be infringing on privacy rights, he took specific steps to ensure that the evidence that he obtained was used restrictively and not made available to all and sundry.

**CONCLUSION**

[73] In the result, I am not persuaded that the evidence of Capt. Brink is inadmissible as alleged by the defence and I am satisfied that it is properly before this court. Accordingly, the application for the relief contained in the notice of motion dated 29 July 2015 is dismissed. It is further directed that the cross examination of Capt Brink should continue.

---

**GAMBLE J**