REPORTABLE

THE REPUBLIC OF SOUTH AFRICA

IN THE HIGH COURT OF SOUTH AFRICA
WESTERN CAPE HIGH COURT, CAPE TOWN

CASE NO: CC 54/2014

In the matter between:

THE STATE

Versus

TERRANCE STEPHAN BROWN **Accused**

REASONS FOR RULING IN TRIAL WITHIN A TRIAL MADE ON 17 AUGUST 2015

BOZALEK, J:

[1] On 17 August 2015, at the conclusion of a trial within a trial, I ruled that certain images found on a mobile phone, ***Exhibit 1*** in the trial ('the phone'), were admissible in evidence and these are the reasons for that ruling.

[2] The accused stood trial on two counts of attempted murder, one count of murder and certain ancillary charges, all of which arose out of an incident in 16th Street, Bishop Lavis on the evening of 9 March 2014 when an unsuccessful attempt was made on the life of a gang member. Tragically, a young child was fatally wounded and another bystander shot in the leg in the incident. The State's principal witness identified the accused as the gunman

and testified that she observed something drop from his pocket during the shooting. Immediately after the gunman left she returned to the scene and found that it was a phone which she identified as ***Exhibit 1***. Shortly thereafter she gave the phone to Dylan Botha, a member of the criminal gang to which her partner, one Reagan Baptiste, and who had been the target of the original shooting, also belonged. This witness, Ms Joy Cronje ('Cronje'), was unable to state what Botha had done with the mobile phone. In later testimony it emerged that Botha had been shot dead in 2015.

[3] The accused pleaded not guilty to the charges and raised an alibi. In the course of his written plea explanation he stated that he had lost his mobile phone on the day prior to the shooting incident. In addition his counsel, Mr Mohamed, put to the various witnesses that the phone placed before Court, ***Exhibit 1****,* was not the accused's. When the prosecutor gave notice that she proposed to lead evidence concerning material which had been downloaded from the phone, Mr Mohamed stated that he objected to the admissibility of the evidence on the following grounds:

1. that the integrity of the *'chain'* i.e. the evidence of safekeeping of the phone from the time that it was allegedly picked up by Cronje to the time that material was downloaded therefrom, had not been, and could not be, proved;
2. that the evidence sought to be admitted was both hearsay and irrelevant;
3. that such evidence was not covered by the terms of a subpoena issued by a magistrate in relation to the phone in terms of sec 205 of the Criminal Procedure Act, 51 of 1977;

4. in any event, any material downloaded from the phone without the authorisation of a magistrate was unlawful and an invasion of privacy.

[4] A trial within a trial was held to determine the admissibility of the material sought to be introduced by the State which, at that stage, comprised 5 images or photographs found amongst those stored on the phone. During the course of the enquiry counsel for the State indicated that it sought only to rely on three of the five images and advised that the material was tendered simply with a view to proving that the phone in question was that of the accused or, more accurately, had been in his possession at the time of the shooting.

SUMMARY OF THE EVIDENCE IN THE TRIAL WITHIN A TRIAL

[5] The state led the evidence of four witnesses, the first of which was Lieutenant Colonel Linnen, the commander of the Co-ordination Centre (also known as the *'War Room'*), a newly created technical division of the SAPS. He testified that his everyday duties involved downloading video surveillance material and data from mobile phones. Such data could include the lists of contacts on a phone, video and photographic images as well as the messages sent or received through the phone using various messaging formats. This he was able to do using a computer software programme available to the police since approximately 2008 and in respect of which he had received training. According to Linnen the programme emanates from Sweden and is widely used by security agencies internationally.

[6] To effect the downloading from a mobile phone it is simply connected to a laptop containing the software programme which then proceeds to read all the data on the phone and, using the same principle as Bluetooth, downloads it into a file. Linnen testified that the software programme in question did not permit any tampering with the data on a phone, either purposefully or accidentally. Linnen testified that if, for example, he used the phone in question before downloading its contents, this would reflect in the data which is downloaded. In the present case he had deleted nothing from the phone and, even if information was deleted, it could be retrieved. Questioned about the security of the phone whilst it was in the custody of his unit he explained that its integrity was ensured by careful procedures, all of which had been documented. Linnen added that the integrity of the exhibit prior to its reaching his unit was not something over which he had any control nor would he, in the ordinary course, investigate this aspect.

[7] Asked about the legal basis for his authority to download material off a mobile phone, Linnen cited the provisions of sec 20 of the Criminal Procedure Act, 51 of 1977 (‘the CPA’) and sec 15 of the Electronic Communications and Transactions Act, 25 of 2002 (the ECTA’). He explained that as far as details of the ownership or registration of a mobile phone, including its SIM card, are concerned, these so-called RICA details (an acronym for the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002) could only be obtained from the relevant service provider and not through the software programme his unit used. When, using a standardised form, a mobile phone is presented to him by an investigating

officer with a request to download material, he assumes that the device has been lawfully obtained.

[8] Regarding the phone in question Linnen testified that it was received by his unit on 25 March 2014 and that he personally received it the following day. He then effected the download in a matter of some twenty minutes, producing a 29 page file. Thereafter the file had been viewed by the investigating officer who had selected five images (stored photographs) which he wished to utilise in criminal proceedings against the accused. The data downloaded from the phone indicated that the five images had been sent to the phone within 2 or 3 minutes of each other at approximately 13:26 on 7 March 2014 from certain other mobile phones, the make and model of which he could identify. Because of the small size of the images as they appeared in the downloaded file he had them enlarged for viewing purposes. Finally, Linnen explained that he had obtained the telephone number relating to the phone's SIM card by using it to send a *'please call me'* message to his own phone and reading the telephone number off that received message.

[9] Sergeant Koki, the investigating officer, confirmed that he had booked the phone into the Command Centre with a request that photographic images, text and contacts lists be downloaded, for the purposes, initially, of a bail application brought by the accused which was to have commenced in May 2014. Koki had eventually selected the images downloaded from the phone on which the State now sought to rely. He testified that he had first become aware of the existence of the phone on the day after the shooting when he noted that it had been booked into the police station's SAP 13 register in the

early hours of that day by a colleague, Major Muller. After he had read Muller's statement regarding his handing in of the phone and discussed the matter with him he had decided to have the contents of the phone analysed. He identified the phone which had been handed in at Bishop Lavis police station by Major Muller as ***Exhibit 1*** before the Court. On that same day he had taken a statement from the witness, Cronje, wherein she made mention of a phone which she said she had picked up at the crime scene and handed to Dylan Botha very shortly after the shooting. Koki testified that he had obtained the RICA details relating to the registration/ownership of the phone and SIM card from the service provider by using the phone's number which Colonel Linnen had provided to him. He obtained the RICA information by applying to a magistrate for a subpoena in terms of sec 205 of the CPA requiring the service provider to provide such information. That information indicated that the SIM card was registered in the name of one Francois Leendertz at a certain address in Delft. When he tried to trace this person he found that no one at the address knew anything about him and various other avenues he explored were also unsuccessful.

[10] Major Muller testified that he had been on duty at the crime scene on the night of the shooting. Later that night, at Bishop Lavis police station, he had been approached by a member of the neighbourhood watch well known to him and who had handed him a red mobile phone on the basis that he did not want his name to be used at any stage for fear of possible reprisals. That person told him that another unnamed person had handed him the phone earlier that night stating that it had been picked up at the scene of the shooting by a gang member, also unnamed. These last intimations were, of

course, hearsay, but since defence counsel indicated that he had no objection thereto I allowed the evidence for the purpose of explaining why Major Muller had considered it appropriate to take possession of the phone and book it in as an exhibit through the SAP 13 register. He identified ***Exhibit 1*** as the phone which he had been handed by the neighbourhood watch member. In cross-examination Muller conceded that he could not say whether anyone had tampered with the phone between the time it was first picked up and when it was handed to him.

[11] The accused did not give evidence in the trial within a trial nor did he lead any witnesses.

[12] On behalf of the accused counsel relied on the various grounds earlier cited for the exclusion of the evidence contending that its admission would violate his client's rights to a fair trial in terms of sec 35(3) and (5) of the Constitution. On the State's part it was contended that the phone had been lawfully obtained, that the downloading of data had been lawful and did not require the authority of a magistrate and that no right to privacy had been violated. Further, it was contended, the images in question were real evidence which should be admitted since there was no proof that there had been any tampering with this data.

DISCUSSION

[13] It is useful first to set out certain of the main prescriptions relating to the admission of evidence and, in particular, evidence which constitutes electronic communication.

[14] As a starting point, sec 35(5) of the Constitution provides that 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 a trial unfair or otherwise be detrimental to the administration of justice. Generally speaking, where evidence is obtained without a warrant or direction, with an improperly obtained warrant or direction, or without following the conditions set out in the warrant or direction, a Court must decide whether to admit it or not. In *Key v Attorney-General, Cape Provincial Division, and Another*[1] Kriegler J summed up the position as follows at paragraph [13], 196 A - B:

> *'What the Constitution demands is that the accused be given a fair trial. Ultimately …, 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 unconstitutionally obtained be excluded. But there will also be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted'.*

[15] Section 20 of the CPA provides that the State may seize anything *'which is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence …'* or *'which may afford evidence of the commission or suspected commission of an offence …*'. Section 21 provides that any such articles may only be seized under a search warrant but this is subject to sec 22 which deals with the circumstances in which an article may be seized without a search warrant. These circumstances, however, do not include situations where the article in question has been lost, left or abandoned at a crime scene and, furthermore, is unlikely to be claimed by someone.

[1] 1996 (2) SACR 113 (CC) at paragraph [13]

[16] The ECTA was introduced to provide inter alia for the admissibility of evidence generated by computers since its predecessor, the Computer Evidence Act, 57 of 1983, was generally considered to have failed to achieve its purpose in this regard and, in any event, had not regulated criminal proceedings. It provides for wide definitions of data – '*electronic representations of information in any form'* - and data messages – *'data generated, sent, received or stored by electronic means and includes – (a) voice, where the voice is used in an automated transaction; and (b) a stored record;'*. An electronic communication is defined as meaning a communication by means of data messages. One of the objects of the ECTA is to '*promote legal certainty and confidence in respect of electronic communications and transactions'.* Although electronic data in the form of images such as photographs and videos are not specifically referred to in either definition, in my view, on a purposive interpretation of the ECTA's provisions, they constitute a form of information.

[17] The ECTA follows an inclusionary rather than an exclusionary approach to the admission of electronic communications as evidentiary material. This appears from sec 11 which deals with the legal recognition of data messages. It provides that information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message. Clearly, the overall scheme of the ECTA is to facilitate the admissibility of data messaging as electronic evidence. Section 15 of the ECTA deals with the admissibility and evidential weight of data messages in legal proceedings. It reads in part as follows:

'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; or

b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

2. Information in the form of a data message must be given due evidential weight.

3. In assessing the evidential weight of a data message, regard must be had to –

a) the reliability of the manner in which the data message was generated, stored or communicated;

b) the reliability of the manner in which the integrity of the data message was maintained;

c) the manner in which the originator was identified; and

d) any other relevant factor.'

[18] I agree with the observation of Gautschi AJ in *Ndlovu v Minister of Correctional Services and another* [2006] 4 All SA 165 (W) at page 172 that sec 15(1)(a) does not render a data message admissible without further ado. The provisions of sec 15 certainly do not exclude our common law of evidence. This being the case the admissibility of an electronic communication will depend, to no small extent, on whether it is treated as an object (real evidence) or as a document.

A DOCUMENT OR REAL EVIDENCE

[19] Section 221(5) of the CPA provides that a document includes any device *'by means of which information is recorded or stored'*. In *Seccombe and others v Attorney-General* 1919 TPD 270 at page 277 it was noted that the word document *'is a very wide term and includes everything that contains the written or pictorial proof of something. It does not matter of what material it is made'*. As Professor J Hofman stated, in an article, (***Electronic Evidence***

in criminal cases, in 2006 SACJ 257 at page 268), in motivating his contention that graphics, audio and video that are in a data message form should be treated in the same way as documents, the view that such material must be regarded as real evidence '*is conceptually simple and appeals to those who dislike excluding any evidence. But it does not take into account the way graphics, audio and video are, to an ever-increasing extent, recorded, stored and distributed in digital form and fall under the definition of a data message. This means that graphics, audio, and video now resemble documents more than the knife and bullet that are the traditional examples of real evidence. In data message form, graphics, audio and video are susceptible to error and falsification in the same way as data messages that embody documentary content. They cannot prove themselves to be anything other than data messages and their evidential value depends on witnesses who can both interpret them and establish their relevance'*.

[20] Given the potential mutability and transient nature of images such as the images in this matter which are generated, stored and transmitted by an electronic device I consider that they are more appropriately dealt with as documentary evidence rather than *'real evidence'*. I associate myself, furthermore, with the approach followed in *S v Ndiki and others* [2007] 2 All SA 185 (CK) where Van Zyl J expressed the view[2] that the first step in considering the admissibility of documentary evidence is to examine the nature of the evidence in issue in order to determine what kind of evidence one was dealing with and what the requirements for its admissibility are. In the present matter the evidence sought to be introduced by the State appears to

[2] At paragraph [53]

be photographs of the accused and its purpose in doing so is to offer proof, or render it more probable, that the phone, ***Exhibit 1***, on which they were found, belonged to the accused and must have been dropped by him at the scene of the crime. Adopting this approach, the ordinary requirements of our law for the admissibility of such evidence is that the document itself must be produced, which document, ordinarily speaking, must be the original and the authenticity of the document must be proved. These requirements are, of course, qualified by those specific provisions of the ECTA having a bearing on electronic communications.

[21] Applying these requirements to the present matter, the images in question were downloaded from the phone, reproduced in hard copy (paper) form and enlarged. There was no suggestion that either the devices or the software which Linnen used to produce or enlarge the images was unreliable or that he manipulated the data or electronic communication in any way.

[22] As regards the images being in their original form, sec 14 of the ECTA provides that a data message satisfies the requirements of original form if it meets the conditions in that section. These are, in short, that the integrity of the information from the time when it was first generated in its final form as a data message has passed assessment in terms of sec 14(2) and, secondly, that information is capable of being displayed or produced to the person to whom it is to be presented. The second requirement is clearly met. As regards the first requirement, sec 14(2) provides that integrity must be assessed:

> *'(a) by considering whether the information has remained complete and unaltered …*

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.'

[23] In the present matter the undisputed evidence is that the images could be traced back to a certain phone or phones which transmitted them to ***Exhibit 1***, all of this taking place within a minute or two on 7 March 2014. Linnen did not suggest that the images had been tampered with at any stage and no such proposition was put to him. He testified, furthermore, that the software he used precluded him from tampering with the images. The evidence of the phone being found at the crime scene and the fact that it was handed to the police shortly before midnight suggests that, accepting for the time being Cronje's evidence that it was dropped at the crime scene, the phone was in unknown hands for at most four hours that night before being handed over to Major Muller. There is no evidence or even a suggestion that any person tampered with the phone or, more accurately, the images stored thereon, during this period. Furthermore, what evidence there is indicates that the phone was in the hands of lay persons in the four hour period and it is thus improbable that any tampering with the images in question took place. Most significantly, Linnen's evidence was that the data downloaded revealed that the images in question had been transmitted to the phone two days before the shooting at a stage when, on the available evidence, the phone was in the hands of the original owner or possessor.

[24] In my view, on a conspectus of this evidence, the requirements of original form and of sec 14 of the ECTA have been met. In any event sec 15(1)(b) of the ECTA gives data messages a further exemption from the

requirement of original form *'if it is the best evidence that the person adducing it could reasonably be expected to obtain'*. In the light of the lack of any evidence as to who originally transmitted the images to the phone, ***Exhibit 1***, and the limited purposes for which the evidence was tendered, namely, to prove that the phone belonged to the accused, I consider that the State could not reasonably be expected to have produced better evidence of these images. Finally, as regards authenticity, I consider that, seen as a whole, Linnen's evidence establishes the authenticity of the images in question which, in any event, was not disputed by the accused, the apparent subject of the images.

[25] I turn now to deal with the various other objections to the admissibility of the images raised on behalf of the accused. Firstly, it was contended that the data message or images amounted to hearsay. Section 3(4) of the Law of Evidence Amendment Act, 45 of 1988 defines hearsay evidence as evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence. The three images which the State seeks to introduce as evidence are photographs, apparently of the accused, and, subject to proof of his identity and bearing in mind the limited purpose for which they are tendered, their probative value stands or falls by that simple fact. In this sense, at least, the images are more akin to being *'real evidence'* but, however they are classified, they do not constitute hearsay evidence.

[26] As previously mentioned defence counsel attacked the integrity of the chain from the time that the phone was allegedly picked up by Cronje to the

time that it was handed to the police. It is correct that there is a four hour window period during which any number of persons could have tampered with the phone. This is, comparatively speaking, a short period of time and there was no evidence that the phone or the images had been tampered with. To have done so would have required no small degree of technical skill. Furthermore, and most importantly, Linnen's undisputed evidence was that the images in question had been transmitted to the phone on 7 March 2014 and thus any form of interference or tampering would have to have involved the manipulation of pre-existing images on the phone, a much more unlikely scenario than the placing of such images on the phone in the four hour window period. Seen in the context of the evidence as a whole I consider that the lack of proof of the integrity of the phone for the four hour period is insufficient to justify the exclusion of the evidence.

[27] Defence counsel argued further that the images in question were downloaded without the authority of a magistrate and for that reason alone were unlawfully obtained. As I have indicated, the provisions of the CPA relating to the obtaining of a search warrant were inapplicable in the present case. In my view, moreover, the police were entitled to seize the phone in terms of sec 20 of the CPA when it was presented to them by the member of the neighbourhood watch with the explanation that it was found on the crime scene. To the extent that any further justification for seizing the phone was necessary this was provided the following day when a statement was taken from Cronje identifying the phone as the one which she picked up at the crime scene after it had been dropped by the gunman.

[28] Nor was any particular authority necessary from a judicial officer in order to download material from the phone with a view to identifying its owner or possessor. Clearly, that information was reasonably necessary in order to trace a suspect. Counsel could not direct my attention to any statutory prohibition against the downloading of material in circumstances such as these. To the extent that defence counsel relied on a right to privacy this approach was misconceived. The accused consistently denied that the phone was his and in the circumstances it would be untenable for him to deny, on the one hand, ownership, possession or a legal interest in the phone or the disputed images stored on it and, on the other hand, to assert a right to privacy over such images.

[29] Ultimately, the question must be whether the downloaded information was obtained in a manner that violated any right in the Bill of Rights and if so, whether it must be excluded because its admission would render the accused's trial unfair or otherwise be detrimental to the administration of justice. I can see no room for any such conclusion. The phone was found at the crime scene and the identity of its owner or possessor was clearly critical to establishing the identity of the gunman. No party asserted a claim to ownership or lawful possession of the phone or, given the circumstances in which it was apparently found, was likely to do so. Downloading data from the phone for the limited purposes of establishing the identity of its owner or possessor is hardly objectionable. By analogy, if the gunman had dropped a diary at the scene of the crime it could not credibly be suggested that the police would be precluded from opening and reading it with a view to establishing the identity of its owner or possessor.

[30] Finally, defence counsel contended that the downloading of the material from the phone fell outside the parameters of a subpoena issued by a magistrate in terms of sec 205 of the CPA in respect of the phone's RICA details and call records. This argument misconstrues both the purpose of the sec 205 procedure and the role it played in the present matter. Section 205 provides for a judicial officer, upon the request of the prosecuting authorities, to require before him or her the presence of any witness who can give material information as to any alleged offence provided that, if such person furnishes that information to the satisfaction of the prosecuting authority beforehand, he or she is excused from appearing before the judicial officer. This procedure, read with other provisions of the CPA, is regularly used to obtain documentation, including cell phone records kept by the major service providers, where such records are regarded as necessary for the investigation of crime. It was pursuant to these provisions that the investigating officer obtained RICA details relating to the phone, ***Exhibit 1***, and call records limited to a two day period.

[31] Where, as in the present case, the phone was already lawfully in the possession of the SAPS and it had the capacity to download data from it using its own software programme, the State was under no obligation to seek such further information or data from the service provider, using the sec 205 or any other procedure. As mentioned counsel was not able to draw to my attention, nor am I aware of, any provisions in our law which would preclude the SAPS in a situation such as the present from subjecting the phone to analysis and downloading information where that was objectively necessary

for the purposes of a criminal investigation[3]. It may well be that, at some future time, statutory intervention may be considered necessary or desirable in order to hold the balance between the privacy of private electronic communications or data and the interests of justice. Such legislation might conceivably provide that before the contents of any electronic device are analysed by the SAPS, the authority of a judicial officer will have to be obtained. That stage has, however, not yet been reached.

[32] Finally, it was contended that the admission of the disputed evidence violated the accused's right to a fair trial and would be in breach of sec 35(3) or (5) of the Bill of Rights. This contention was largely unsubstantiated, however, and I have already alluded to the anomaly of the accused denying ownership or possession of the phone but seeking to exclude the admission of images found on it which tend to prove the very issue in dispute, namely, ownership or possession of the phone at the relevant time. As regards sec 35(5) I find, for the reasons already furnished, that the evidence sought to be introduced was not obtained in a manner that violates any right in the Bill of Rights. Even if I am incorrect in this conclusion I consider that the admission of the evidence would not render the accused's trial unfair or otherwise be detrimental to the administration of justice.

[33] In conclusion it is worth noting that the process envisaged by sec 15(2) of the ECTA i.e. assessing the evidential weight of the electronic

[3] Subsequent to hearing argument I have had the opportunity of considering the reasons furnished by Gamble J for a ruling in a similar enquiry in the matter of S v P Miller and 8 others (SS13/2012, delivered on 2 September 2015). It appears that he was presented with full argument to the effect that the provisions of ECTA precluded SAPS from downloading data from seized mobile phones, at least without the authority of a 'cyber inspector' appointed in terms of ECTA. Gamble J ultimately rejected this argument and I find myself in agreement with his reasoning insofar as a similar argument could have been raised in the present matter.

communication sought to be introduced in evidence, and in so doing utilising the criteria furnished in sec 15(3), is one which will only be addressed after all the evidence has been heard.

[34] It was for these reasons that at the conclusion of the trial within a trial I made an order in the following terms:

> *The three images set out on pages 4 and 5 of **Exhibit S**, namely, photos 126.jpg, 127.jpg and 128.jpg and their corresponding enlargements in **Exhibit T** are held to be admissible evidence, as images found on **Exhibit 1** on 26 March 2014.*

_____

Bozalek, J