Impediments during the execution of a search and seizure warrant for digital information by forensic investigators in South Africa

Jacobus Gerhardus J. Nortje and Daniel Christoffel Myburgh
School of Accounting, North-West University, Potchefstroom, South Africa

Abstract

Purpose – This paper aims to identify impediments, discuss impediments and make recommendations for the impediments during the execution of a search and seizure warrant for digital evidence in South African criminal cases.

Design/methodology/approach – The discussion of this article, the second article of two, focuses on a literature review of international and local impediments identified in case law and published research literature and how it is approached in various jurisdictions.

Findings – This study found that impediments identified and addressed internationally during the execution of a search and seizure warrant for digital evidence are relevant to South African criminal cases and still need to be addressed during the execution of a search and seizure warrant for digital evidence in South African criminal cases.

Research limitations/implications – Although searches and seizures for digital evidence are relevant to civil, regulatory and criminal investigations, this study focuses on the search and seizure for digital evidence in criminal matters with an emphasis on the provisions of the Criminal Procedure Act 51 of 1977 and the Cybercrimes Act 19 of 2020.

Originality/value – The originality of this paper lies in the procedures followed during the physical search and seizure of digital information during the execution of search and seizure warrants for digital information in South Africa. If the South African Police Service follows the recommended procedures, it will contribute to the success of the South African Police Service, which would result in the improved quality of investigations and successful prosecution of crime in South Africa.

Keywords Search and seizure warrant, Digital information, Privilege information, Digital evidence, Segregation of evidence, Plain view, Overbroad, Two-step search

Paper type Literature review

1. Introduction

The discussion of this article, the second article of two, focuses on international and local impediments, as identified in case law, published in research literature and how it is approached in various jurisdictions during the execution of a search and seizure warrant for digital information by forensic investigators in South Africa (SA).

Journal of Financial Crime
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-05-2023-0125

In Article 1, the following impediments were discussed regarding the application and the compilation of a search and seizure warrant: a full disclosure with applications, the intelligibility of an application and the warrant, search protocol and *ex ante* restrictions and privileged information.

The logic of the study commenced with a thorough review of international and local impediments identified in case law and published research literature, highlighting the different approaches, processes and best practices used.

The missing knowledge is that no such research is known to have been conducted in SA. The failures of the South African Police Service (SAPS) during the execution of search and seizure warrants are evident from the large amount of evidence returned to suspects as a result of the defective execution of warrants.

The following research question is significant to this study: Will addressing the impediments during the execution of search and seizure warrants contribute to the success of the SAPS?

The purpose of this study is to identify impediments, discuss impediments and make recommendations regarding the impediments during the execution of a search and seizure warrant for digital evidence in South African criminal cases. To achieve the purpose of the study, the following impediments, as identified in international and local case law, are discussed: overbroad seizures, the two-step search process, including off-site searches, segregation of data, use of filter teams, retention of non-relevant data, plain-view discoveries and handling privileged information.

The use of search and seizure warrants is an important investigation technique that is well researched and frequently challenged in court, but little attention has been given to the execution thereof regarding the mentioned impediments of digital evidence. Various international case law identifies impediments that are relevant to SA. As mentioned in Article 1, the most relevant guidance for SA emanates from case law, law and guidelines of Australia, America, New Zealand, Canada and the UK.

As discussed in Article 1, related studies within a South African context that were conducted were, *inter alia*, that of Nieman (2006), Basdeo (2012) and Bouwer (2014).

The practical implication of this study is that if the SAPS could address the identified impediments during the execution of search and seizure warrants, it will contribute to the success of the SAPS, which would result in the improved quality of investigations and successful prosecution of crime in South Africa. Other interested stakeholders are the Departments of Justice, Forensic IT practitioners and lawyers, when drafting and executing civil search and seizure warrants (Anton Pillar orders), the Investigation Directorate, Independent Police Investigation Directorate, Special Investigation Unit, South Africa Revenue Service (SARS), Financial Intelligence Centre and Competition Commission.

The remainder of this article is structured as follows: Section 2 provides a background to the study, a conceptual scope of the study, followed by a literature review in Section 3. This is followed by conclusions and recommendations in Section 4.

2. Background

2.1 Relevance of this study

In the Constitutional Court case of the *Minister of Police and Others* v *Kunjana* (2016), the court held that the more a search intrudes on the "inner sanctum" of persons, such as their homes, the more the search infringes on their rights and the investigators can intrude where the expectations of privacy are very high – this is specifically so with computers and mobile phones. It is for this reason that heightened attention and care should be paid to the compilation, approval and execution of search and seizure warrants for digital evidence.

While the State has the authority of warrantless seizure, this research study is limited to searches and seizures with warrants. Because computers have become a reality in almost all criminal investigations, it would be a detrimental oversight to rely continually on section 22 of the Criminal Procedure Act (Criminal Procedure Act 51, 1977) and sections 31 and 32 of the Cybercrimes Act 19 (2020) as warrantless seizure authority when computers are encountered on scenes. This is in line with the ruling of the Constitutional Court in *Gaertner and Others* v *Minister of Finance and Others* (2013) case, where the court ruled that exceptions to the requirements of warrants should not become the rule and warned that search and seizure warrants are not a mere formality.

If a search and seizure warrant and the execution of it cannot stand scrutiny in court, the consequences are that the exhibits seized can be returned by the court and eventually, in the absence of the exhibits, result in an unsuccessful prosecution. Prior experiences in other countries, such as Australia, America, New Zealand, Canada and the UK, can aid SA because so few cases and aspects have been tested in South African courts.

2.2 Conceptual scope of the study

Currently, the SAPS does not have specific guidelines for the execution of the warrant, except for National Instruction, 1 of 2015, Crime Scene Management (SAPS, 2015). The SAPS was also required to publish standard operating procedures (SOPs) on 1 December 2022, in terms of section 26 of the Cybercrimes Act 19 (2020), but failed to do so.

In practice, if the digital forensic investigator is listed and available to assist with executing a warrant, the digital forensic investigator will be allowed to enter the scene and will be responsible for locating the evidence and seizing it. The evidence will be seized, in the form of a forensic sound duplicate, which will be removed from the scene. This forensic sound duplicate will be analysed and reported on by the digital forensic investigator who will compile a report and act as an expert witness.

2.2.1 Overview of SAPS digital forensic processes. An unstructured interview was held with a former police officer who is an expert in digital forensics and the management of digital forensic units of the SAPS. An unstructured interview was necessary to establish the current processes within the SAPS in relation to searches and seizures for digital evidence, as it is not available in the public domain. According to Myburgh (2016, p. 68), the relevant processes within the SAPS were as follows:

- Digital forensic investigators cannot attend all crime scenes where needed. When a computer is identified on the scene, it is seized in totality by the investigator and sent to a digital forensic lab, without a search performed on it at the scene.
- Digital forensic investigators are not supplied with copies of search and seizure warrants.
- Instructions pertaining to what analysis functions are required from digital forensic investigators are done on a separate application for analysis form.
- In most cases, digital forensic investigators are instructed to extract all data on a device and hand it over to the investigator irrespective of the content of the search warrant.

It has been confirmed to still be the process in 2023 from current projects with the SAPS.

3. Literature review

3.1 Local and international impediments

In August 2009, *United States* v *Comprehensive Drug Testing* (2009) case was taken before a full bench of judges (hereafter referred to as *en banc*) who reviewed the conduct of the State

and reflected on the balance between law enforcement's perhaps legitimate need in relation to digital evidence to over-seize, and the restrictions against overbroad searches. The court issued pre-emptive requirements (hereafter referred to as *ex ante* requirements), which authorised officers to enforce search warrants:

- The State must waive reliance on the plain view doctrine. If investigators find anything on computers that does not relate to the original search and seizure warrant, they are not allowed to use or access this information.
- Segregation of relevant and non-relevant data must be either done by specialised personnel or an independent third party or filter team.
- If segregation is done by the State, it must be agreed on in the search and seizure warrant application that computer personnel may not disclose to the investigators any information other than that which is the target of the warrant.
- The search protocol of the State must be structured to only uncover information containing probable cause, and only that information may be examined by investigators.
- The State must destroy or return non-related data.

Guzzi (2012, p. 329) reported that this ruling was criticised as costly, impractical and overbroad. The Ninth Circuit Court issued a revised *en banc* opinion in September 2010 and changed the requirements to guidelines.

3.2 Overbroad seizures

If only computer hardware found on a scene is described, it is technically correct, but seizing computers containing all the data is overbroad, as the computers contain a magnitude of non-relevant information. If only relevant data is described, a warrant is more focused and cured of an overbroad description, but considering all the practical problems involved, such as the possible encryption of evidence and the sheer size of data, it is virtually impossible to complete a search on a scene. In this case, the warrants will not encompass all the actions planned by investigators when computers containing all the data are seized and removed (Kerr, 2005, p. 102).

If search and seizure warrants are found to be overbroad or defective, South African courts will set these warrants aside completely or only the defective portions if defective portions of the warrants can be severed from the rest of the warrant. The practical aspect of this is that it might not be possible to strike or remove only portions of data in a forensic duplicate.

This situation places digital forensic investigators in an unattainable position. If only relevant keyword containing data may be forensically duplicated and not all the data on a computer, none of the system-related information regarding the files will be included. This can be severely detrimental to the interest of justice in a number of ways. Firstly, evidence can be interpreted incorrectly. Secondly, the digital forensic investigator may be unable to place the evidence within context, especially if the defence has the advantage of having access to all the data and make allegations outside of the ambit of what the digital forensic investigators were allowed to seize. Lastly, the British Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stores Material (British Attorney General, 2011, p. 10) also points out that if all the data is not copied, investigators will not be able to locate and analyse evidence pointing away from the guilt of suspects.

It has been recognised that to "effectively execute" warrants that investigators have to seize computers containing all the data or create forensic duplicates of all the data stored on

computers and conduct an off-site segregation of relevant and non-relevant data (Lowenstein, 2007, pp. 101–128). Unfortunately, this requirement seemingly carries a search outside the normally accepted ambit of traditional search and seizure warrants. This is specifically true, while concerns regarding constitutional rights are amplified, when the State is conducting comprehensive searches, which often unearth private, privileged and non-relevant information (Lowenstein, 2007, pp. 101–128).

3.3 A two-step search process and off-site search

Industry guidelines, such as the Association of Chief Police Officers (1997) Good Practice Guide for Computer-Based Electronic Evidence, dictate that the actions of investigators should not change or alter evidence, yet a traditional approach dictates that the evidence should be searched on the scene prior to being seized. These actions, for example, opening or printing files, are not neutral and influence the evidence (Vacca, 2005, p. 19). In other words, the actions of police officials on a scene and their subsequent interactions with digital evidence can have a direct impact on the acceptance of evidence in court. This is supported by the Explanatory Report to the Cybercrime Convention, which points to the fact that digital evidence should be retained in the state it was found – from when a search commenced to when prosecution takes place (Council of Europe, 2001, p. 33).

The most relevant statutory requirements for the authenticity and admissibility of digital evidence in SA are set out in sections 14 and 15 of the Electronic Communication and Transaction Act 25 of 2002 (Electronic and Transaction Act 25, 2002), which relate to the originality, integrity and reliability of evidence that must be maintained.

Search and seizure rules in the USA were based on a one-step search process, whereby law enforcement enters premises and seizes listed articles. Kerr (2005, p. 86) argues that new criminal procedures are necessary and that existing search and seizure rules should be adapted. The traditional one-step process should be replaced with a two-step search process, which includes investigators entering premises, seizing the listed hardware and taking the hardware off-site to search for relevant data (Kerr, 2005, p. 87).

It should be noted that, normally, the search step of data is performed after a seizure took place and at the location of investigators (Kerr, 2005, p. 85). During a normal process, articles can only be seized after a search action was performed, but data is seized before the information is searched (Chan, 2014, p. 442).

The need for allowing a two-step search process and off-site search is widely recognised in the industry, by academics (Kerr, 2005; Welty, 2011; Bouwer, 2014), court cases and regulatory guidelines (US Department of Justice, Guidelines for Searching and Seizing Computers and Obtaining Electronic Evidence for Use in Criminal Investigations and the British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners).

In 2009, Rule 41 of the Federal Rules of Criminal Procedure (Legal Information Institute, 2009) was amended by inserting Rule 41(e)(2)(B). This amendment is in line with Kerr's proposal and states that warrants may authorise a seizure or a forensic duplication of digital evidence and a later review of data.

In the American case of *Davis* v *Gracey* (1997), the court found that searching computers on-site is more disruptive than searching computers off-site. The court found it "obvious" that searching computers for evidence requires great skill, time and expertise. It was, therefore, found that it is more reasonable to conduct off-site searches than to stay at the house of a suspect for several days conducting a search. In the *United States* v *Hay* (2000) case, the seizure of physical computers was found lawful due to the "time, expertise and controlled environment required for a proper analysis".

While section 25 of the new Cybercrimes Act 19 (2020) provides a much-needed wider definition of seize, to the extent that digital evidence can be seized by "making and retaining a copy of data", it needs to be seen how section 29(2)(d)–(h), which stipulates "the extent set out in the warrant" of the Cybercrimes Act 19 (2020), will be interpreted. It might be interpreted to relate to the way the article will be searched and accessed and not indicate the description of the article – thereby possibly requiring describing in more detail the search, seizure and analysis methodology that will be followed. Because the SAPS has not yet published their SOPs, as required by section 26 of the Cybercrimes Act 19 (2020), on 1 December 2022, this aspect is still uncertain.

The British Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stores Material (British Attorney General, 2011, p. 5, 11) provide for investigators to remove computers from a scene if it is not possible to duplicate data on a scene and to conduct an off-site search.

In the case of *Thint (Pty) Ltd* v *National Director of Public Prosecutions and Others*, *Zuma and Another* v *National Director of Public Prosecutions and Others* (2008), the warrant stipulated that forensic duplicates will be made of the evidence and thereafter "at a location removed from the premises" evidence will be retrieved by means of a forensic analysis. This aspect was not challenged in court. In the unreported judgement of the then Transvaal Provincial Division of the High Court (2005), case 10828/2005, the court held that "it does not matter where a back-up of a hard drive is made".

The aspect of whether a computer can be seized, without as much as a preliminary assessment on the scene to determine whether it contains relevant evidence, is also a contentious point, and furthermore, if it can be searched off-site without the suspect is present. In the case of the *United States* v *Hill* (2006), the applicant appealed the seizure of his computers without the police conducting a search of these articles on the scene to determine whether they contained data as described in the warrant. The Ninth Circuit Court agreed with the trial court that it is unreasonable to bring computer equipment to a scene to determine whether the storage media contain evidence, but the court agreed with the applicant that the State had the burden to make at least a minimum showing why the blanket "seizure of the haystack is needed to search for the needle" and why an onsite search is impractical. McLain (2007, p. 1081) is of the opinion that the court was incorrect in its conclusion – it is unreasonable to expect the police to conduct an onsite preview. If it is expected of the police to always conduct previews on a scene, it can place the police in a position between two untenable situations – either conducting a preview and damaging evidence or making forensic duplicates and reviewing the duplicates to establish whether they contain evidence (McLain, 2007, p. 1083). It is possible to connect the computers of suspects to a write-protector device that can allow the police to conduct a preview to determine whether the data on the device is covered by the warrant without influencing the evidential value of the data. This approach is supported by the Australian Crimes Act (12 of 1914) (Australia, 1914), sections 3K and 3F, which allow for investigators to bring specialised tools to search and seize digital evidence on a scene and provide that digital devices may be seized, but only if these devices have been sufficiently examined to determine whether they contain evidence. The process of previewing data is time-consuming and can be inconvenient for suspects to have the police at their location for a long period. Division 2 of the Australian Crimes Act (12 of 1914) section 3K allows for the removal of articles to a different location if the creation of forensic duplicates on a scene is not practically possible, but these articles should be returned within 14 days (Australia, 1914). An extension can be requested for up to seven days at a time.

A request was made in the *Gaertner and Others* v *Minister of Finance and Others* (2013) case to restrict investigators of SARS to only duplicate and seize data in the presence of the suspect. This request was declined, but the undertaking was given that data should be seized and only extracted in the presence of the suspect. Section 21 of the Criminal Procedure Act (Criminal Procedure Act 51, 1977) does not require suspects to be present during a search and seizure and authorises the SAPS to search premises in the absence of suspects but also does not prevent them from being present.

In the UK, section 53 of the Criminal Justice and Police Act (2001) states that seized material should be examined as soon as practically possible to determine what should be retained and what not. The desirability of allowing owners to be present should be considered, but not precluded.

The main basis of concern against the off-site search of the data is the fact that the suspect is typically not present and cannot verify or determine whether the investigator stayed within the ambit of the search warrant. If proper protocols are put in place, in the SOPs of the SAPS in terms of section 26 of the Cybercrimes Act 19 (2020), in accordance with ISO/IEC DIS 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC DIS 27043, suspects and authorising officers will be placed in a position to scrutinise all search and analysis actions *ex post facto* and would therefore be legally acceptable (Nortjé and Myburgh, 2019, p. 33).

The main basis of concern against the off-site search of the data is the fact that the suspect is typically not present and cannot verify or determine whether the investigator stayed within the ambit of the search warrant. If proper protocols are put in place, which are envisaged in the SOPs of the SAPS in terms of section 26 of the Cybercrimes Act 19 (2020), suspects and authorising officers will be placed in a position to scrutinise all search and analysis actions *ex post facto* and would therefore be legally acceptable (Nortjé and Myburgh, 2019, p. 33). These protocols should be structured on principles that all actions taken must be performed by competent and proficient (ISO 27042) digital forensic investigators and their actions should be auditable, repeatable, reproducible by a third party and justifiable (ISO/IEC DIS 27037).

3.3.1 Privileged data. The aspects of privileged data are discussed under the heading of segregation of data and the use of filter teams.

3.3.2 Segregation of data. Computer data can be stored unorganised and intermingled and sometimes file names do not relate to the content (Kessler, 2010, p. 27). Relevant, non-relevant and privileged documents can be intermingled without the possibility of investigators separating relevant from non-relevant data on a scene. Law enforcement is generally permitted to carry out overbroad seizures by seizing computers, or forensic duplicates containing all the data, but they are not permitted to scour through devices indiscriminately (*R* v *Vu*, 2013). As soon as investigators realise that seized devices do not contain relevant evidence, these devices should be returned to owners as soon as reasonably possible [Search and Surveillance Act 24 (2012), British Attorney General (2013) Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners, p. 21].

The British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners (British Attorney General, 2013, p. 22) make provision for when relevant material is inextricably linked to non-relevant material, and it is not reasonably practical to segregate – then these devices can be retained. The test is whether the material can be removed without prejudicing the use of relevant material in a judicial process. It is strongly stated that inextricable-linked material may not be examined further, may not be further forensically duplicated or used for any purpose other than validating the integrity of relevant material. This approach is supported in the New Zealand Search and Surveillance Act 24 (2012),

section 161(2). Myburgh (2016, p. 68), established that the practice in SA does not distinguish between searching data to, firstly, only identify relevant information based on the ambit of warrants, but in many cases, all data created by users found on computers is handed over to investigators. This was confirmed to still be the practice in 2023 from current assignments with the SAPS. This is in contradiction to the court ruling in the unreported case of the then Transvaal Provincial Division of the High Court (2005), case 10828/2005, where the Computer Crime Investigation Unit of the SAPS acted as an independent filter team and only supplied information to the investigator that was found to be within the ambit of the search warrant.

An applicable case in this regard is the *Minister of Safety and Security and Others* v *Bennett and Others* (2007), where a blanket seizure and off-site search of 400,000 documents were held as lawful, as it was impossible and impractical to effectively search all files on the scene and to separate relevant files. Because it was impractical to perform segregation of relevant documents on the scene, the seizure of all documents was permitted to enable the State to secure evidence. The parties involved reached an agreement concerning the monitoring of the segregation of relevant and non-relevant data.

In *Lavallee, Rackel and Heintz* v *Canada (Attorney General)* (2002), the Supreme Court set a number of search protocols in relation to privileged data, which include that if the data cannot be segregated, it may be seized and examined by an independent legal filter team to determine whether it was privileged. Although case law recognises that privileged information may not be seized, but sealed and kept separate – this cannot happen when computers are seized and a forensic duplicate is created of the whole computer. The forensic duplicate should therefore be sealed in totality.

3.4 Plain view discoveries

The conclusion was expressed in *Thint (Pty) Ltd* v *National Director of Public Prosecutions and Others, Zuma and Another* v *National Director of Public Prosecutions and Others* (2008) that, when authorised officers approve applications for search and seizure warrants, it is done based on information given under oath that the investigators have a reasonable suspicion or a clear understanding that they will find the articles they seek. Searches are not fishing expeditions. The court further held that investigators are "never" entitled to simply search through everything present with the hope of finding something relevant. This is contrary to the process that is currently followed by the SAPS where "all data" of suspects is handed over to an investigation team or all data is searched with the "hope of finding something" and they are conducting "fishing expeditions" (Myburgh, 2016, p. 69).

Given the magnitude of information saved on computers, it can often occur that investigators discover evidence in plain view relating to other offences not specified in warrants (Welty, 2011, p. 10). Welty (2011, p. 11) mentions that many courts in the USA have expressed the view that plain view should be limited or even eliminated regarding digital evidence, as was seen in the restrictions enforced in the *United States* v *Comprehensive Drug Testing* (2009) case.

Thint (Pty) Ltd v *National Director of Public Prosecutions and Others, Zuma and Another* v *National Director of Public Prosecutions and Others* (2008) concluded that if it was argued that section 29 of the National Prosecuting Act 32 (1998) intended to authorise a complete examination of every single article on a premises to determine whether these articles have bearing on a case, this seemingly unbounded power is inimical to the constitutional right of privacy. The court further expressed the opinion that investigators should keep this duty in mind even if nobody is present to observe their actions.

In the case of Ontario Court of Appeals in *R.* v *Jones* (2011), the verdict of the court was that the search of computers pursuant to a search and seizure warrant must be limited to the

reasonable and probable grounds that were established as the basis for the application of the warrant or did they stray from the application of the warrant. The court held that the discovery of evidence of child pornography was lawful, but the focus change from that point forward to locate more evidence of child pornography was unauthorised, as it did not fall within the original objective.

The reality of seizing a whole computer and not only relevant information opens the door of continuous or unlimited searches. In a paper environment, investigators are only permitted to seize relevant information listed in a warrant. If investigators discover evidence off-site regarding another crime, they are not able to return to the original scene to further a new investigation without a new warrant. If the seizure of computers containing all the data is permitted, investigators can expand their search and repeatedly search these computers with the purpose to discover new evidence that falls outside the original warrant.

3.5 Use of filter teams

Independent filter teams are teams or individuals who are not connected to an investigation directly and their function is to sift through data and determine what is relevant and what is not or what is privileged and what is not (US Department of Justice, 2009, pp. 110–111).

A requirement can, therefore, be to require investigators to specify what keywords they should use to locate relevant information (Guzzi, 2012, p. 319) or to use independent filter teams to extract relevant information and only this information should be handed over to investigation teams (US Department of Justice, 2009, pp. 110–111).

In the unreported judgement of the then Transvaal Provincial Division of the High Court (2005), case 10828/2005, it was explained that the Computer Crime Investigation Unit of the SAPS functions in the same way as independent filter teams and only extracts and hands over relevant information to investigators. The court stated: "I am satisfied that no more information would have been conveyed to the respondent than was covered by the warrant". During an unstructured interview with a former police officer, Myburgh (2016, p. 95) established that this process is not followed anymore, but that all the data is handed over to investigators. This was confirmed to still be the practice in 2023 from current assignments with the SAPS.

If a forensic duplicate contains legally privileged information, a digital forensic investigator might not have the skills to identify privilege; therefore, the Supreme Court of Canada in *Lavallee, Rackel and Heintz* v *Canada (Attorney General)* (2002) specified that independent lawyers should examine the data.

4. Conclusions and recommendations

From the research, it is clear that international courts have grappled with the impediments that digital evidence poses to the traditional interpretation of law such as overboard seizures, the intermingled nature of relevant and non-relevant data and privileged data. These aspects are seemingly successfully being addressed by approaches such as the two-step search process, segregation of data protocols and using filter teams. It is clear that from a South African legal perspective, SA courts encounter the same challenges and by implementing or adopting some of the international approaches, these impediments can be successfully managed.

It is recommended that:

- Pre-search previews should be performed on scenes prior to seizing a device to establish whether the device contains relevant evidence or not. This should, however, not be mandatory. It must, however, only be performed in a forensically sound manner by competent digital forensic investigators before seizing the device.

If pre-search previews are done and no evidence is found due to possible constraints, such as data deletion and encryption, investigators may still have to seize computers to complete more in-depth searches.

- A digital forensic investigator should be present to create forensic duplicates on the scene. Devices should only be seized and removed if digital forensic investigators are not available or circumstances require it. Where devices are seized, a forensic duplicate should be created within a reasonable time and the device returned.
- A multi-step search process should be recognised in which computers are searched for on a scene while data is searched off-site. It is recommended that, due to the discussed impediments and in serving the interest of justice, overbroad seizures of computers should be permitted as a method to secure evidence – this practice has been adopted by the UK, the USA, Australia, New Zealand and Canada – but not as a blanket approval to investigate all data on computers unrestrictedly. The only way to guard against this leniency towards seizing all data on a computer becoming the norm for overbroad seizures is to use mechanisms to manage the review of data. Therefore, digital forensic investigators should limit all search protocols to identify data strictly as defined in the warrant; separate requests from investigators must not be entertained.
- The digital forensic investigator should act as an independent filter team following various search mechanisms structured around a documented approach of first following least intrusive means with the objective of first and foremost segregating relevant and non-relevant files. This is proposed as a mandatory step, and further analyses may not stray into non-relevant information. This should also be seen as the point where the original warrant has been fully executed. Only relevant information may be handed to investigators. If additional information outside of the original warrant is required by investigators, and a new search needs to be conducted, a new warrant should be applied for.
- Consideration should be given to a suspect when it is requested to be present during the segregation of relevant and non-relevant data; however, this must not be a requirement. It may be impractical to have hundreds of suspects present during the segregation of data, especially if this happens over long periods of time. It is recommended that the use of independent filter teams is more practical. Independent filter teams can be digital forensic investigators within the SAPS or external teams. The ISO/IEC DIS 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC DIS 27043 standards as well as the British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners (British Attorney General, 2013) provide a good structure in which the actions of filter teams are recorded and therefore monitored. These guidelines specify that the lead investigator should develop a strategy or search protocol on how the data should be analysed. A detailed record should be made of the strategy and the analytical techniques used to segregate data to allow for *ex post facto* assessments. The record should include the names of the persons who carried out the process and what keywords were used on the specified dates and times. The search protocol could involve a myriad of possible approaches to identify relevant information and should clearly show an approach of first looking in the most obvious places and then – when necessary – progressively moving from the obvious to the obscure as well as listing all parameters and keywords used to identify relevant information, while limiting and preventing access to non-relevant and privileged information.

The protocol should first rely on automated search mechanisms to locate responsive information without the content becoming known followed by an "exposure-based approach" of review and verification to establish relevance. It is, however, not advised that keywords should be viewed as the only mechanism to search data, as many files are not responsive to keywords alone.

- In cases where relevant and non-relevant information is inextricably linked and the removal of non-relevant information can prejudice the use of relevant material, the retention of both the relevant and non-relevant material is recommended. It is, however, specified that digital forensic investigators may not stray into non-relevant information during subsequent investigations.
- If privilege is claimed, the forensic duplicate should be sealed and only reviewed by a legal practitioner, who can identify/consider privilege and can be supported by an independent digital forensic investigator. Privileged data can only be identified after data recovery was performed or after relevant data was identified. If suspects are unable to identify privileged information, they can supply independent filter teams with keywords to facilitate and expedite this process or generic keywords can also be used. Even in cases where privileged information is not claimed, a digital forensic investigator should focus on preventing privileged material from being handed to a forensic investigator. Any privileged information should be separated from relevant data and should be submitted to an authorised independent party for review.
- If digital forensic investigators discover evidence, which falls outside the original warrant, in plain view, a new warrant should be obtained after initial discoveries were made to extend the search to locate more evidence relating to the new suspected offences.

References

Association of Chief Police Officers (1997), "Good practice guide for computer-based electronic evidence version 5", available at: www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (accessed 27 January 2023).

Australia (1914), "Australian Crimes Act 12 of 1914".

Basdeo, V. (2012), "The legal challenges of search and seizure of electronic evidence in South African criminal procedure: a comparative analysis", *South African Journal of Criminal Justice*, Vol. 25 No. 2, pp. 198-211.

Bouwer, G.P. (2014), "Search and seizure of electronic evidence: division of the traditional one-step process into a new two-step process in a South African context", *South African Journal of Criminal Justice*, Vol. 27 No. 2, pp. 156-171.

British Attorney General (2011), "Attorney General's guidelines on disclosure: supplementary guidelines on digitally stored material", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/16239/Attorney_General_s_guidelines_on_disclosure_2011.pdf (accessed 5 January 2023).

British Attorney General (2013), "Attorney General's guidelines on disclosure for investigators, prosecutors and defence practitioners", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf (accessed 10 January 2023).

Chan, G. (2014), "Life after Vu", *Supreme Court Law Review*, Vol. 67 No. 2, p. 442.

Council of Europe (2001), "Explanatory report to the convention on cybercrime", available at: https://rm.coe.int/16800cce5b (accessed 29 January 2023).

Criminal Justice and Police Act (2001), *Criminal Justice and Police Act 16 of 2001*.

Criminal Procedure Act 51 (1977), *Criminal Procedure Act 51 of 1977*.

Cybercrimes Act 19 (2020), *Cybercrimes Act 19 of 2020*.

Davis v *Gracey* (1997), 111 F.3d 1472 (10th cir. 1997).

Electronic and Transaction Act 25 (2002), *Electronic Communication and Transaction Act 25 of 2002*.

Gaertner and Others v *Minister of Finance and Others* (2013), (3) all SA 159 (WCC).

Guzzi, S. (2012), "Digital searches and the Fourth Amendment: the interplay between the plain view doctrine and search-protocol warrant restrictions", *American Criminal Law Review*, Vol. 49 No. 1, pp. 301-329.

Kerr, O.S. (2005), "Search warrants in an era of digital evidence", *Mississippi Law Journal*, Vol. 75 No. 1, pp. 85-108.

Kessler, G. (2010), "Judges' awareness, understanding, and application of digital evidence", PhD thesis, Nova South-eastern University, Graduate School of Computer and Information Sciences, Fort Lauderdale, FL.

Lavallee, Rackel and Heintz v *Canada (Attorney General)* (2002), (3) S.C.R. 209.

Legal Information Institute (2009), "Federal rules of criminal procedure: rule 41, search and seizure", available at: www.law.cornell.edu/rules/frcrmp/rule_41 (accessed 19 March 2023).

Lowenstein, A.S. (2007), "Search and seizure on steroids: United States v Comprehensive Drug Testing and its consequences for private information stored on commercial electronic databases", *Cardozo Public Law, Policy and Ethics Journal*, Vol. 6 No. 1, pp. 101-128.

McLain, G.R. (2007), "United States v Hill: a new rule, but no clarity for the rules governing computer searches and seizures", *George Mason Law Review*, Vol. 14 No. 4, pp. 1071-1104.

Minister of Police and Others v *Kunjana* (2016), (CCT253/15) ZACC 21.

Minister of Safety and Security and Others v *Bennett and Others* (2007), (302/06) 2007 ZASCA 136; 2007 SCA 136 (RSA); 2008 (2) All SA 26 (SCA); 2009 (2) SACR 17 (SCA).

Myburgh, D.C. (2016), "Developing a framework for the search and seizure of digital evidence by forensic investigators in South Africa", MCom dissertation, North-West University, p. 68.

National Prosecuting Act 32 (1998), *National Prosecuting Act 32 of 1998*.

Nieman, A. (2006), "Search and seizure, production and preservation of electronic evidence", PhD thesis, North-West University, Potchefstroom.

Nortjé, J.G.J. and Myburgh, D.C. (2019), "The search and seizure of digital evidence by forensic investigators in South Africa", *Potchefstroom Electronic Law Journal*, Vol. 22, p. 1, doi: 10.17159/1727-3781/2019/v22i0a4886.

R. v *Jones* (2011), ONCA 632.

R v *Vu* (2013), S.C.J. No. 60, 2013 (3) S.C.R. 657, at para. 22 (S.C.C.).

SAPS (2015), "National instruction, 1 of 2015, crime scene management".

Search and Surveillance Act 24 (2012), *Search and Surveillance Act 24 of 2012*.

Thint (Pty) Ltd v *National Director of Public Prosecutions and Others, Zuma and Another* v *National Director of Public Prosecutions and Others* (2008), (CCT 89/07, CCT 91/07) 2008 ZACC 13; 2008 (2) SACR 421 (CC); 2009 (1) SA 1 (CC); 2008 (12) BCLR 1197 (CC).

Transvaal Provincial Division of the High Court (2005), Case no. 10828/2005.

United States v *Comprehensive Drug Testing* (2009), 579 F.3d 989, 1006-07 (9th cir. 2009) (en-banc).

United States v *Hay* (2000), 231 F.3d 630 (9th Cir. 2000).

United States v *Hill* (2006), 459 F.3d 966, 977-78 (9th Cir. 2006).

US Department of Justice (2009), "Searching and seizing computers and obtaining electronic evidence in criminal investigations", US Department of Justice.

Vacca, J.R. (2005), *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed., Charles River Media, Boston, MA.

Welty, J. (2011), "Warrant searches of computers', Spring Public Defender and Investigator Conference organised by NCIDS", available at: www.ncids.org/Defender%20Training/Training%20Index.htm (accessed 21 January 2023).

Further reading

International Organisation of Standardization (2012), "Information technology – security techniques – guidelines for identification, collection, acquisition, and preservation of digital evidence", ISO/IEC 27037, Switzerland.

International Organisation of Standardization (2015a), "Information technology – security techniques – guidance on assuring suitability and adequacy of incident investigative method", ISO/IEC 27041, Switzerland.

International Organisation of Standardization (2015b), "Information technology – security techniques – guidance for the analysis and interpretation of digital evidence", ISO/IEC DIS 27042, Switzerland.

International Organisation of Standardization (2015c), "Information technology – security techniques – incident investigation principles and processes", Switzerland ISO/IEC (ISO/IEC DIS 27043).

Corresponding author

Jacobus Gerhardus J. Nortje can be contacted at: Koos.Nortje@nwu.ac.za