The Originality of Digital Evidence and the Retention of Seized Digital Devices by Law Enforcement Officers in South Africa

Jacobus Gerhardus Johannes Nortjé
https://orcid.org/0000-0001-8355-4559
North-West University, South Africa
koos.nortje@nwu.ac.za

Daniel Christoffel Myburgh
https://orcid.org/0000-0001-9720-6109
North-West University, South Africa
danny@cyanre.co.za

Abstract

Information and communication technology (ICT) devices, including mobile phones, laptops, computers and data storage mediums, such as memory sticks, are being seized daily by law enforcement agents. These devices are seized for different reasons in terms of the provisions of sections 21 to 23 of the Criminal Procedure Act 51 of 1977 and now, in terms of the provisions of sections 28 and 29 of the Cybercrimes Act 19 of 2020. The seizure and extended retention of such devices by law enforcement can have a devastating impact on businesses and individuals. In virtually all cases, the main objective of seizing an ICT device is to secure its data for purposes of investigation and the collection of evidence. This excludes, inter alia, cases where a device contains contraband and cannot be handed back to the suspect or in a case where circumstances justify forfeiture to the state. This article is limited to cases where the physical device has no evidential value. It is contended that the content of the evidential data and the requirement of originality on an ICT device is met by scientifically created forensic duplicates of the data, which negate law enforcement from unnecessary seizure and retaining the original device. The authors contend that ICT devices should only be seized in situations where a forensic duplicate of the evidential data cannot be created on the scene and, if seized, the evidential data should be forensically duplicated, and the original device returned within a pre-determined period. An extension of the pre-determined period should only be granted by a magistrate upon application. It is recommended that the subject be researched further, to arrive at a reasonable, pre-determined period, and that the Criminal Procedure Act 51 of 1977 and Cybercrimes Act 19 of 2020 be amended accordingly.

UNISA university of south africa PRESS
Southern African Public Law
https://unisapressjournals.co.za/index.php/SAPL
Volume 38 | Number 2 | 2023 | #14381 | 17 pages

https://doi.org/10.25159/2522-6800/14381
ISSN 2522-6800 (Online), 2219-6412 (Print)

Keywords: Digital forensics; forensic investigation; search and seizure; digital evidence; digital devices; original evidence; retention of evidence

Introduction

The implications for an individual, in the event of their phone or computer being seized and kept for an extended period, could be devastating. Mobile phones, especially, are extremely private devices and an integral part of every person's communication, finances, and security. Here, reference is made specifically to multi-factor authentication codes, that are required from accessing mail to authorising financial transactions and making payments by using applications such as SnapScan and Zapper.[1] This would render the individual incapable of conducting any financial transactions. Applications such as password vaults (which hold all a person's passwords for all types of access control), health monitoring applications, vehicle tracking, insurance applications and even the tracking of children's locations which have been linked to a mobile phone, are critical examples.

There are no legal requirements as to the duration that law enforcement agents are permitted to retain seized computers and mobile phones after a forensic duplicate is created of the evidential data on the device. The Criminal Procedure Act 51 of 1977 and the Cybercrimes Act 19 of 2020, which regulate searches and seizures in criminal cases, are silent regarding a specific timeframe to return seized devices. The question therefore is what approach, in terms of seizing a device to create a forensic duplicate, would be reasonable to limit the period that a device is removed and kept by law enforcement in South Africa.

Lowenstein[2] emphasised the fact that an individual's constitutional rights are heightened due to the seizure of the full content of computers as well as mobile devices. Since all the data on the device is seized and not only that which is relevant to the investigation, the risk of violating a suspect's constitutional rights is high. Because the device will inevitably contain a considerable amount of confidential, privileged and private information. The seizure of these devices should therefore be viewed as extremely intrusive. Casey[3] supported this viewpoint and emphasises the importance of the individual's constitutional rights, especially in a digital age, when a high level of privacy is associated with electronic devices on which large amounts of communication and private information are stored.

1 SnapScan and Zapper are mobile applications that are linked to an individual's credit card for the purpose of contactless payments from a mobile phone.

2 Aaron Lowenstein, 'Search and Seizure on Steroids: *United States v Comprehensive Drug*, 2007 Testing and its Consequences for Private Information Stored on Commercial Electronic Databases' (2007) 6 Cardozo Public Law, Politics and Ethics.

3 Eoghan Casey, *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet* (3rd edn, Elsevier 2013) 1.

In *Minister of Police and Others v Kunjana*,[4] it was held that if a search intrudes on a person's 'inner sanctum,' such as their home, the more the search will infringe upon the individual's constitutional right to privacy. The heightened expectation of privacy that individuals hold in relation to their digital devices was also recognised in the Supreme Court of Canada's case of *R v Vu*.[5] In the application for the search warrant, it was not explicitly stated that a computer would be seized. The Supreme Court criticised the Appeal Court's ruling that digital devices are no different from normal filing cabinets and investigators are therefore permitted to search all items in a location. The court held that digital devices are very different from filing cabinets and was of the opinion that if digital devices are considered equal to filing cabinets, then presiding officers would not pay enough attention or give due consideration to the level of intrusion that they are authorising in light of the unique privacy concerns that they pose.

To address the inadequacies as identified in the Criminal Procedure Act 51 of 1977 and the Cybercrimes Act 19 of 2020 a comparative approach was followed in comparing this legislation with the way in which the same issues have been regulated in other countries. This methodology has become almost compulsory in legal research[6] and it is evident that South Africa can gain valuable knowledge from other countries with more legal experience in this field.

This article will show that international standards and best practices promote the creation of forensic duplicates of original copies of digital evidence and that such forensic duplicates, if the correct forensic processes are followed, also address the requirement of originality in local South African legislation. The article will show that there is therefore no requirement for law enforcement in South Africa to retain an original device and that the forensic duplicate of the evidential data must be recognised as a duplicate original. It is concluded that there is no defined guideline or updated legal parameter set for the period that law enforcement can seize and retain digital devices in South Africa after a forensic duplicate has been created of the evidential data, since the Criminal Procedure Act 51 of 1977 was written and last amended prior to the existence of mobile devices and digital forensic duplicate original copies.

Originality of Forensic Copies

Some basic procedural requirements of the digital forensic process are explained below to provide context. The leading standards in this regard are the International Organization for Standardization's (ISO) ISO/IEC DIS 27043[7] and ISO/IEC DIS

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

5 *R v Vu* [2013] SCJ No 60, 2013 (3) SCR 657, para 22 (SCC).

6 Mark van Hoecke, 'Methodology of Comparative Legal Research' (2015) Law and Method 1. 0

7 ISO, Information Technology – Security Techniques − Incident Investigation Principles and Processes, ISO/IEC DIS 27043 (2015) <https://www.iso.org/standard/44407.html> accessed 15 January 2023.

27037.[8] The ISO/IEC DIS 27037-27043 standards have been adopted and enforced by the South African Association of Certified Fraud Examiners (ACFE) as the ACFE SA Digital Forensic Standard for Digital Forensic Practitioners in South Africa,[9] of which law enforcement bodies are members who have signed a MOU to adhere to the ACFE SA and ACFE Code of Ethics and Professional Standards.[10]

When investigators perform a preliminary physical review of devices by for example, opening, viewing or printing files in their native format, their actions are not neutral and will influence or modify the evidence.[11] The South African Police Service (SAPS) very seldom performs a preliminary assessment on the scene to determine whether a device contains relevant information, but rather seizes the physical device in totality and sends it to a digital forensic investigator to conduct an off-site search to create a forensic duplicate.[12] Schulman[13] prescribes that, from the point of original seizure to prosecution, no modification or change should be made to digital evidence, and it should be retained in the original format.

Kessler[14] emphasised the fact that the integrity and originality of the evidence must be preserved during each process involved in the digital forensic model. The South African Law Reform Commission (SALRC)[15] also supported the fact that if an investigator accesses files in their original format, their actions are not neutral and could modify the evidence. This would make it difficult to prove the originality and integrity of the evidence and the improper following of digital forensic procedures could render the evidence susceptible to allegations of prejudicial alteration and therefore useless.

8 ISO, Information Technology – Security Techniques − Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence, ISO/IEC (ISO/IEC DIS 27037 (2012) <https://www.iso.org/standard/ 44381.html#:~:text=ISO%2FIEC%2027037%3A2012%20provides,can%20be%20of%20evidential%20value> accessed 20 January 2023.

9 Association of Certified Fraud Examiners of South Africa, *ACFE SA Digital Forensic Standard for Digital Forensic Practitioners in South Africa* (2019) <https://acfesa.co.za/sites/default/files/content-files/Professionl%20Standards/Digital%20Forensic%20Standards%20for%20Digital%20Forensic%20Practitioners%20in%20South%20Africa_V02.pdf> accessed 31 August 2023.

10 ACFE –MOU signed with the DPCI (2023) <https://www.youtube.com/watch?v=W-Pp1NnDt2A> accessed 10 October 2023.

11 John Vacca, *Computer Forensics Computer Crime Scene Investigation* (2nd edn, Charles River Media 2005) 19.

12 Jacobus Nortjé and Daniel Myburgh, 'The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa' (2019) 22 PELJ 22.

13 Cristina Schulman, *Explanatory Report to the Convention on Cybercrime* (European Treaty Series 185, Council of Europe 2016) 38 <http://www.oas.org/ juridico/english/ cyb_pry_coe.pdf> accessed 29 January 2023.

14 Gary Kessler 'Judges' Awareness, Understanding, and Application of Digital Evidence' (DPhil thesis, Nova Southeastern University 2010) 6.

15 South African Law Reform Commission, *Review of the Law of Evidence Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues, Project 126* (SALRC 2010).

Schulman proposes that specific procedural measures are required to ensure that digital evidence is seized in the same way and as effectively as the seizure of tangible items;[16] because it cannot be removed in the same manner as hard copies.[17] It further explores the various ways in which digital evidence can be 'seized', for instance information can be printed, and by seizing the printed documents (which may not be plausible), the physical device on which the evidence is saved can be seized or a forensic duplicate can be made thereof.[18] The report recommends that local legislation should provide for the authorisation to create such duplicates.[19] Section 25 of the new Cybercrimes Act 19 of 2020 addresses this requirement by defining the word 'seize' to include 'to make and retain a copy of data or a computer programme.'

Creating a forensic duplicate usually requires the investigator to connect to the suspect's device via a write-protector device.[20] This corresponds with the principles of the Association of Chief Police Officers (ACPO)[21] and the ISO standards,[22] which stipulate that the actions of an investigator should not alter the evidence. It is recommended that a forensic duplicate of the digital evidence be created and that the forensic duplicate should be the item up for analysis.

Data is placed in a read-only form by means of a write-protector device[23] and prevents the actions of investigators, such as accessing and viewing files to influence or change the metadata of files. This device permits an investigator to conduct a preliminary search on a device to establish whether the device contains any relevant information.[24] A write-protector device can be a hardware device or a software programme, which is used to prevent any changes from being made to the data under investigation.

Should it be established that a device contains evidence, a forensically sound duplicate should be made. This can be done accurately by using various forensic software programmes that create forensically sound duplicates of devices.[25] Nieman[26] explains

16 Schulman (n 13) 32.
17 ibid.
18 ibid.
19 ibid.
20 Annamart Nieman, 'Cyberforensics: Bridging the Law/Technology Divide' (2009) 1 J Information, Law & Technology 22.
21 Association of Chief Police Officers, *Good Practice Guide for Computer-Based Electronic Evidence Version 5* (1997) 4 <http://www.digitaldetective.net/digitalforensicsdocuments /ACPO_ Good_Practice _Guide _for_ Digital_Evidence_v5.pdf> accessed 27 December 2015.
22 ISO/IEC(ISO/IEC DIS 27037 (n 8) 6–8.
23 John Ashcroft, Deborah Daniels and Sarah Hart, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (US Department of Justice 2004) 41.
24 Jacobus Nortjé and Daniel Myburgh, 'The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa' (2019) 22 PELJ 22.
25 Sally Vandeven, 'Forensic Images: For Your Viewing Pleasure' (*SANS Institute* 2014) 1 <https://www.sans.org/readingroom/whitepapers/forensics/forensic-images-viewing-pleasure-35447> accessed 2 October 2015.
26 Nieman (n 20).

that copies created on a bit-by-bit basis are exact replications of a hard drive. Angermeier[27] also stated that a bit-by-bit copy is an exact reproduction of data that contains even deleted or hidden data. The forensic duplicate and original data contained on the device have been scientifically proven to be a precise version of each other and can, therefore, be accepted as a duplicate of the original.[28] Creating forensic duplicates could be time-consuming, bearing in mind that the best possible transfer rate is thirty-two gigabytes[29] per minute, with actual results achieved in the field closer to an average rate of approximately six gigabytes per minute. The copying of a one terabyte hard drive could take almost three hours as will the time to verify the integrity of the duplicate. Creating a forensic duplicate of a server could therefore take more than twenty-four hours, depending on the storage size. The number of mobile phones, computers and servers on a scene has a great impact on the duration of the forensic duplication or seizure of the data on a scene.

The 'proven and scientific principles' of forensic duplicates entail the following: in creating a forensic duplicate, the forensic programme runs a cryptographic hashing algorithm that records the hash value of the subject data. This is called the MD5 or SHA1 hash value/algorithm. Nieman[30] stated that this is commonly referred to as the 'electronic fingerprint' of the data.

The SHA1 hash is a secure algorithm and produces a 160-bit (character) hash value[31]. Schneier[32] stated that with a hash of even 128 bits, the possibility of multiple files producing the same hash value is computationally infeasible. Based on the hash value not changing, investigators can mathematically show during a trial that digital evidence has not been modified in the slightest manner.

As an example: The hash value for the word 'Dog' is: SHA1 hash value - b86784a4ef3c83b56393632ee6b1dd746622caf1. Losey[33] states that if even one character in a whole laptop is altered, the hash will change. Therefore, if 'Dog' is

27 Vincent Angermeier, 'Swinging for the Fences: How Comprehensive Drug Testing Inc Missed the Ball on Digital Searches' (2010) 100(4) J Criminal Law and Criminology 1615.

28 Sarah Van Deusen Phillips, 'Legal Considerations for Electronic Evidence, Part 5: Original vs. Duplicate Documents & Unfair Prejudice' (*The Documentalist* 2010) <https://crlgrn.wordpress.com/2010/07/27/ legal-considerations-for-electronic-evidencepart-5-original-vs-duplicate-documents-unfair-prejudice/> accessed 23 October 2015.

29 Media Clone <https://www.media-clone.net/SuperImager-Plus-8-3-NVME-7-SATA-SAS-Forensic-p/sif-0037-00a.htm> accessed 25 January 2023.

30 Nieman (n 20).

31 Eric Thompson, 'MD5 Collisions and the Impact on Computer Forensics' (2005) 2(1) Digital Investigation 36–40.

32 Bruce Schneier, *Applied Cryptography, Second Edition Protocols, Algorithms and Source Code in C* (Wiley 1996) 436–441, 582.

33 Ralph Losey, 'Hash' (*Ediscovery team* 2007) <https://e-discoveryteam.com/school/computer-hash-5f0266c4c326b9a1ef9e39cb78c352dc/> accessed 8 November 2023.

changed to for example 'DOG', the hash value will change to: SHA1 hash value - bbbd558a572a105c718e04894e9ffa8756ef8402.

The statutory requirements of digital evidence in SA are defined by sections 14 and 15 of the Electronic Communications and Transaction Act 25 of 2002—the originality of digital evidence is accessed against the integrity of the data by considering 'whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display.' Vacca[34] stated that a paramount feature of digital forensics is the fact that it revolutionises the 'best evidence concept' in relation to digital evidence. Vacca[35] explains that a new concept of 'representational accuracy' has emanated in relation to digital evidence—where forensic duplicates are created, it is unnecessary to table the original devices as the original copy. When a forensic duplicate is created, and it is established to be an exact replication of the original, the duplicate is considered original[36] for purposes of submitting it during a judicial process as original evidence. The acceptance of copied data as evidence has already been acknowledged in South African courts as early as 2004, when the court held in the *Beheersmaatschappij and Another v The Magistrate Cape Town* (2004)[37] case that 'It was in any event unnecessary for the police to remove these articles from the South African applicants' premises. The electronic data found by the police at Mowbray could effectively have been searched and copied at the premises within a few hours, using technology which is readily available.'

In the Canadian case of *R v Munshi*,[38] it was commented that due to the innovation in technology and forensic practices, forensic duplication has advanced to such a degree that duplicate originals can be accepted. The court held that if exact duplication processes are followed, it is generally not compulsory to compare duplicate originals with original documents.

Van Deusen Phillips[39] stated that the test to establish whether digital documents can be accepted as evidence was to determine whether the content of the duplicate was unchanged and exactly the same as the original. In the case of *Lorraine v Markel American Ins Co*,[40] the court found that an original can be the original writing itself or a version that has the exact same content and that if the information is stored digitally, a printout or other output, which reflects the information precisely, can be accepted as

34 Vacca (n 11) 795.
35 ibid 237.
36 Vacca (n 11).
37 *Beheersmaatschappij and Another v The Magistrate Cape Town* (in the Supreme Court of South Africa (Cape Provincial Division) Case no 5635 / 2004).
38 *R v Munshi* 2002 CanLII 39110 (ON SC).
39 Van Deusen Phillips (n 28).
40 *Lorraine v Markel American Ins. Co.* (2007), 241 FRD 534, 544 (D Md 2007).

an original. The South African case of *Muller v BOE Bank Ltd and Others*[41] recognised that, and since the inception of carbon copies, local courts have accepted the existence of 'copies', which are recognised as duplicate originals.

Retention of Physical Devices

Myburgh[42] found that the Directorate for Priority Crime Investigation (DPCI) generally returns seized computers within two weeks and mobile telephones within a week, but in more complicated cases it could take up to two months. Other divisions of the South African Police Service (SAPS) generally take up to two months on average to return seized items. In South Africa, the Criminal Procedure Act 51 of 1977, sections 30 to 35 regulate the retention of and action regarding seized items. This Act, however, makes no mention about how long seized devices may be kept o create a forensic duplicate, and the return the original seized device after the duplicate has been made. Law enforcement officials are therefore permitted to seize digital devices and keep them for an unstipulated period. The new Cybercrimes Act 19 of 2020 also does not address any periods of retention. It does however require that Standing Operating Procedures[43] (SOPs) be developed and published by the SAPS, which was done in October 2023. The SOPs acknowledge that the Cybercrimes Act 19 of 2020 is silent on this aspect and state that the provisions of the Criminal Procedure Act 51 of 1977 still apply. The current situation places all suspects in an undesirable position—in that their only remedy is to rely on law enforcement to act in utmost good faith or to apply to the court on an urgent basis to have their seized items returned. Section 31(1)(*a*) of the Criminal Procedure Act 51 of 1977 relates closest to the aspect under discussion and states that 'If no criminal proceedings are instituted in connection with any article referred to in section 30(c) or if it appears that such article is not required at the trial for purpose s of evidence … the article shall be returned to the person from whom it was seized.' Du Toit[44] correctly concludes that the Criminal Procedure Act 51 of 1977 has not 'kept pace with technological advancements' and that the Criminal Procedure Act 51 of 1977 should incorporate the search and seizure provisions of the Cybercrime Act 19 of 2020. It must be borne in mind that The Criminal Procedure Act was originally drafted without any reference to intangible items such as data at a time before highly private items such as

41 *Muller v BOE Bank Ltd and Other* (8723/98) 2010 ZAWCHC 121; 2011 (1) SA 252 (WCC); 2011 (1) All SA 166 (WCC).

42 Daniel Myburgh, 'Developing a Framework for the Search and Seizure of Digital Evidence by Forensic Investigators in South Africa' (MCom dissertation, North-West University 2016) 68.

43 SAPS, 'Standard Operating Procedures in terms of Section 26 of the Cybercrimes Act, No 19 of 2020 for the Investigation, Search, Access or Seizure of Articles' (2023) <https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf> accessed 10 October 2023.

44 Pieter Du Toit, 'The Search Warrant Provisions of the Cybercrimes Act and Their Relationship with the Criminal Procedure Act' (2022) Obiter (43 4) 764-778 <http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1682-58532022000400007&lng=en&nrm=iso>. accessed 6 August 2023.

mobile phones existed. It therefore is clear that it does not speak to the current situation as discussed above where the SAPS is seizing devices without verifying whether they may contain any relevant data for off-site searches.

Additionally, no guideline is provided about the fact that the SAPS will not only have the physical device, but also a forensic duplicate of the data. The same disposal action will have to be taken with the forensic duplicate as with the actual device. While the original device is the property of the suspect, the forensic duplicate is kept on a hard drive or storage device owned by the SAPS and while the data should be returned, the hard drive cannot.

In the *Beheersmaatschappij and Another v The Magistrate Cape Town*,[45] the court expressed the opinion that, as already mentioned, 'the electronic data found by the police at Mowbray could effectively have been searched and copied at the premises within a few hours, using technology which is readily available' and further 'It is trite that search and seizure of this kind must be carried out by the authorities in the least intrusive and disruptive manner possible. The police had no power, in the circumstances, to disrupt the South African applicants' business more than was necessary.'

While ISO/IEC DIS 27037[46] provides that devices may be seized and taken to a different location to create a forensic duplicate, this verdict indicates that firstly, data can be seized by making a copy; secondly, seizing devices is not the least intrusive of measures; and thirdly, it is unlawful to remove a device to made copies elsewhere when it can be copied on the scene. From this it is inferred that when circumstances allow, the device must be removed and returned with the minimum disruption and with high priority.

In *US v Comprehensive Drug Testing Inc*[47] the court cautioned that if rules of search and seizure were to be relaxed to such an extent as to accommodate the complications posed by digital evidence, there is a severe and real risk that all digital search and seizure warrants will become over-broad, thereby making the Fourth Amendment rights, and the local Constitutional rights of individuals, irrelevant. This can also be relevant to the South African Constitutional rights of individuals.

It is generally acknowledged that digital evidence is stored intermingled with other files and that file names need not relate to the content of a file.[48]

45 *Beheersmaatschappij and Another v The Magistrate Cape Town* (in the Supreme Court of South Africa (Cape Provincial Division) Case no 5635 / 2004).

46 ISO/IEC(ISO/IEC DIS 27037 (n 8)

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

48 Kessler (n 14) 27.

The seizure of all data on a computer (even if not relevant) has therefore raised the question[49] of whether a further offsite search to only locate relevant evidence and to segregate relevant and non-relevant files would not be more appropriate.[50] It is recommended that this action be performed by a filter team that only hands over relevant evidence to the investigator.[51] If the broad seizure of digital evidence is permitted, one needs to consider: what period is reasonable for the creation of a forensic duplicate after the seizure; the search and segregation of the data to locate non-relevant and related data; and what would be a reasonable period after which to return the original device and/or the non-relevant data?

Investigators in the United Kingdom face high legal barriers in obtaining a digital search warrant, for which they need to be circumspect in their application. Investigators rightfully need to consider the impact it will have on seizing many devices as well as their timeframe for return. The forensic duplicates must be made as soon as is reasonably possible. While the seizure of devices, to permit the creation of forensic duplicates offsite is permitted, no additional material, which is not justifiable,[52] may be removed. Non-relevant material may also not be kept.

A restriction of fourteen days is placed on investigators in America by Rule 41(e)(2)(B) of the Federal Rules of Criminal Prosecution of 2009 to 'execute' warrants. This pertains to the seizure of devices or the forensic duplication on-site and no further off-site duplications or searching for evidence. The United States Department of Justice advises that original devices should not be retained and that forensic duplicates should be created, whereafter the originals should be returned within a reasonable time frame.[53] Section 3L of the Australian Crimes Act 12 of 1914, allows investigators to secure digital devices for up to twenty-four hours to examine or create forensic duplicates. With modern-day duplication processes, which should be sufficient time to create the forensic duplicate. Section 3K of this Act further provides that digital devices may be seized and removed but governs that the devices should be returned within fourteen days. A request for an extension can be made for only seven days at a time. The court, in *United States v Hernandez*,[54] stated that neither the Fourth Amendment nor the Federal Rules of Criminal Procedure of 2009 place any specific limit on the duration of the analysis of digital evidence. The court held that if the items are seized properly

49 Paige Bartholomew, 'Seize First, Search Later: The Hunt for Digital Evidence' (2014) 30(4) Touro Law Review 1035.

50 British Attorney General, *Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners* (2013) 21–22.

51 Orin S Kerr, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (USA Department of Justice 2009) 110–111.

52 British Attorney General, *Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material* (2011) <https://www.gov.uk/government/uploads/system/uploads/attachment _data/file/16239/Attorney_General_s_guidelines_on_disclosure_2011.pdf> accessed 5 January 2016.

53 Kerr (n 51).

54 *United States v Hernandez* 183 F Supp 2d 468, 480–81 (DPR 2002).

within the allowed period and within the ambit of the search warrant, the retention of the information and not the original devices, and the prolonged review thereof, does not require extension applications or additional warrants, nor does it automatically qualify as evidence for suppression.

Certain US courts held the opinion that investigators are required to search computers to identify relevant evidence before too much time has passed, under the reasonable standards of the Fourth Amendment.[55] This, however, does not relate to the further analysis and further investigation of the relevant data, but only to the period of segregating non-relevant and relevant data after seizure.

In *United States v Syphers*[56] and others, the American court held that a prolonged delay in the analysis of digital evidence does not constitute an unconstitutional seizure. When no search or analysis of seized data is performed, or it is prolonged for no reasonable reason, a court that originally authorised an 'overbroad' seizure could find that the warrant has become less reasonable as time elapses.[57] An example of this is the case of *United States v Metter*,[58] where the court acknowledged that while the complexities that digital devices pose to investigations do allow for some flexibility, the state cannot be allowed to ignore its responsibilities. In this case, the devices, were seized and forensic duplicates were created and the original devices returned as per the periods specified in the warrant, but the officers in charge failed to analyse the data over a period of fifteen months. The court held that if this dereliction of responsibility by the state is permitted, the Fourth Amendment requirements would lose its power within the digital search and seizure environment. However, in the *United States v Triumph Capital Grp*[59] case, the court held the opinion that in computer-related investigations, large sets of information are normally involved and that it requires more stringent and comprehensive investigation and analysis, which prolongs the investigation. The court therefore ruled that where a delay in the review is reasonable under the circumstances, the delay does not make the seizure unconstitutional.

From a South African perspective, both section 35(3) of the Constitution of the Republic of South Africa 1996 and section 342A of the Criminal Procedure Act 51 of 1977 specify that a person has the right to a fair trial, which includes that the trial starts and ends without unreasonable delay.

Most global jurisdictions recognise the need to create a forensic duplicate of digital devices and to return the physical device in a reasonable time by explicitly specifying a

55 Orin Kerr, 'Search Warrants in an Era of Digital Evidence' (2005) 75(1) Mississippi Law Journal 122, 137.

56 *United States v Syphers* 426 F.3d 461, 469 (1st Cir 2005).

57 ibid.

58 *United States v Metter* [no10-CR-600 (EDNY 05/17/2012)].

59 *United States v Triumph Capital Grp, Inc* 211 FRD 31, 66 (D Conn 2002).

time period within days. As a prerequisite, this is only possible if legislation and courts recognise that forensically sound duplicates are original records or accepted as originals.

Conclusion

The definition of 'seize' in section 25 of the new Cybercrimes Act 19 of 2020 already recognises that data can be seized by making a copy of the data. This should not be a normal copy of the data, since normal copying could influence the content and modification could occur. The creation of such a copy must meet the requirements of sections 14 and 15 of the Electronic Communications and Transactions Act 25 of 2002, which requirements are only met by a forensic duplicate. The forensic duplication of data must be done in a reliable manner whereby no alteration of the data occurs to ensure that the forensic duplicate can be accepted as original. The duplicate original copy must therefore remain complete and unaltered to protect the integrity of the duplicate.

The forensic process whereby digital evidence is collected is widely recognised and is subject to stringent processes and controls to ensure that the evidence can be scientifically proven to be an exact duplicate of the original data. It is concluded that forensic duplicates, if created in the correct manner and proven to be an exact duplicate, can be viewed as originals or duplicate originals including any subsequently created forensic duplicates. The forensically sound duplicate is acceptable in judicial standards as originals and the retention of the original device should be superfluous when the device itself is not needed for judicial purposes.

It must be kept in mind that if a forensic duplicate is created and the original device is handed back to the suspect, the content will change as soon as the suspect starts to access the device. The forensic duplicate that was created by the investigator should therefore be seen as the only remaining original version of what the seized device contained at the exact moment of seizure and the forensic duplicate should therefore be recognised as the only original copy, susceptible to further judicial reference.

In recognising a person's constitutional right to a fair trial, which unreasonable delays could impact, the period of seizing and retaining digital devices to create forensic duplicates should be as short as is reasonably possible. The most acceptable situation would be if all digital devices were inspected at a scene and, should it be determined that relevant evidence is contained, a forensic duplicate must be created at the scene.

When the original device is not needed for judicial purposes, it should only be seized and removed if a digital forensic investigator cannot attend to the scene, if the device cannot be accessed due to technical or security reasons or if there are too many devices encountered at a scene, whereafter it must be returned within a defined period.

Recommendations

- It is recommended that international guidelines, legal principles, and best practices be adopted and that parameters be set for law enforcement for the period that they are permitted to retain a physical device, to allow them to create a forensic duplicate and return the physical device to the owner.

- Forensically sound duplicates must be accepted and recognised as original and should be susceptible to seizure, while the original device need not be retained.

- The Standing Operating Procedures[60] of the SAPS failed to prevent unnecessary seizure and detention of ICT devices, by stating that the provisions of the Criminal Procedure Act 51 of 1977 stands, and could have prescribed:

- That a preliminary assessment should be done on a scene by a qualified digital forensic investigator to determine whether a device contains any relevant data prior to seizure. Forensic duplicates should be created on the scene and that devices are not seized and removed, but only in exceptional cases, such as, where a digital forensic investigator is not available, where technical difficulties are encountered or where too many devices are encountered The Criminal Procedure Act 51 of 1977 must therefore be amended.

- The Criminal Procedure Act 51 of 1977 should be amended similar to the Australian Crimes Act 12 of 1914, sections 3L and 3K, which provide for the securing and removal of devices for examination or to create a forensic duplicate for up to twenty-four hours. With modern forensic technology, this should be sufficient; however, the data size and quantity of devices could be a consideration in permitting a longer period. The devices should, however, be returned within a period of fourteen days. An extension of seven days, at a time, can be applied for. Or, provisions according to the British Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material[61] and the British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners[62] or the American, Federal Rules of Criminal Prosecution of 2009 can be considered. This recommendation however needs further comparative research into relevant international law for adoption of a pre-set time period by South Africa.

- Du Toit's[63] conclusion that the Criminal Procedure Act 51 of 1977 should incorporate the search and seizure provisions of the Cybercrime Act 19 of 2020, is supported.

60 SAPS (n 43).
61 British Attorney General (n 50).
62 British Attorney General (n 52).
63 Du Toit (n 44).

- The Criminal Procedure Act 51 of 1977 should be amended to regulate the retention and return of forensic copies in terms of sections 30, 31, 32, 34 and 35 and not only physical devices. It is recommended that provision is made for the copies to be destroyed, instead of returned, if the suspect has received the physical device containing the data.

References

Angermeier V, 'Swinging for the Fences: How Comprehensive Drug Testing Inc Missed the Ball on Digital Searches' (2010) 100(4) Journal of Criminal Law and Criminology.

Ashcroft J, Daniels DJ and Hart SV, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (US Department of Justice 2004) <https://www.ojp.gov/ pdffiles1/ nij/199408.pdf> accessed 5 January 2023.

ACFE, *ACFE SA Digital Forensic Standard for Digital Forensic Practitioners in South Africa* (2019) <https://acfesa.co.za/sites/default/files/content-files/Professionl%20Standards/Digital%20Forensic%20Standards%20for%20Digital%20Forensic%20Practitioners%20in%20South%20Africa_V02.pdf> accessed 31 August 2023.

ACFE MOU signed with the DPCI (2023) <https://www.youtube.com/watch?v=W-Pp1NnDt2A> accessed 10 October 2023.

Association of Chief Police Officers, *Good Practice Guide for Computer-Based Electronic Evidence version* (1997) 5 <http://www.digitaldetective.net/digitalforensicsdocuments/ ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf> accessed 27 January 2023.

Bartholomew P, 'Seize First, Search Later: The Hunt for Digital Evidence' (2014) 30(4) Touro Law Review.

British Attorney General, *Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material* (2011) <https://www.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, *Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners* (2013) <https://www.gov.uk/ government/ uploads/system/uploads/attachment_data/file/ 262994/AG_ Disclosure_ Guidelines_-_December_2013.pdf> accessed 10 January 2023.

Casey E, *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet* (3rd edn, Elsevier Academic Press 2013).

Du Toit P, The Search Warrant Provisions of the Cybercrimes Act and Their Relationship with the Criminal Procedure Act' (2022) Obiter (43 4) <https://doi.org/10.17159/obiter.v43i4.13191>

International Organisation for Standardization, *ISO/IEC 27037:2012 Information Technology – Security Techniques − Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence* (2012) <https://www.iso.org/standard/44381.html#:~:text=ISO%2FIEC%2027037%3A2012%20provides,can%20be%20of%20evidential%20value> accessed 15 January 2023.

International Organisation for Standardization, *ISO/IEC 27043:2015 Information Technology – Security Techniques − Incident Investigation Principles and Processes* (2015) <https://www.iso.org/standard/44407.html> accessed 20 January 2023.

Kerr OS, 'Search Warrants in an Era of Digital Evidence' (2005) 75(1) Mississippi Law Journal.

Kerr OS, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (United States of America Department of Justice 2009).

Kessler G, 'Judges' Awareness, Understanding, and Application of Digital Evidence' (PhD thesis, Nova Southeastern University 2010).

Losey R, 'Hash' (*Ediscovery team* 2007) <https://e-discoveryteam.com/school/computer-hash-5f0266c4c326b9a1ef9e39cb78c352dc/> accessed 8 November 2023.

Lowenstein AS, 'Search and Seizure on Steroids: *United States v Comprehensive Drug: Testing* and its Consequences for Private Information Stored on Commercial Electronic Databases' (2007) 6 Cardozo Public Law, Politics and Ethics.

Media Clone <https://www.media-clone.net/SuperImager-Plus-8-3-NVME-7-SATA-SAS-Forensic-p/sif-0037-00a.htm> accessed 25 January 2023.

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

Nieman A, 'Cyberforensics: Bridging the Law/Technology Divide' (2009) (1) Journal of Information, Law & Technology.

Nortjé JG and Myburgh DC, 'The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa' (2019) 22 Potchefstroom Electronic Law Journal <http://dx.doi.org/ 10.17159/ 1727-3781/2019/v22i0a4886>

Schneier B, *Applied Cryptography, Second Edition Protocols, Algorithms and Source Code in C* (Wiley 1996).

Schulman C, 'Explanatory Report to the Convention on Cybercrime' (2016) <http://www.oas.org/juridico/english/cyb_pry_coe.pdf> accessed 29 January 2023.

South African Law Reform Commission, *Review of the Law of Evidence Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues, Project 126* (SALRC 2010) <https://www.justice.gov.za/salrc/ipapers/ip27_pr126_2010.pdf> accessed 25 January 2023.

S*APS* Standard Operating Procedures in terms of Section 26 of the Cybercrimes Act, No 19 of 2020 for the Investigation, Search, Access or Seizure of Articles (2023) <https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf> accessed 10 October 2023.

Thompson E, 'MD5 Collisions and the Impact on Computer Forensics' (2005) 2(1) Digital Investigation <https://doi.org/10.1016/j.diin.2005.01.004>

Van Hoecke M, 'Methodology of Comparative Legal Research' (2015) Law and Method <https://doi.org/10.5553/REM/.000010>

Vacca JR, '*Computer Forensics Computer Crime Scene Investigation'* (2nd edn, Charles River Media 2005).

Vandeven S, 'Forensic images: For your viewing pleasure' (*SANS* 2014) <https://sansorg .egnyte. com/dl/HvbeBjwKSy> accessed 25 January 2023.

Van Deusen Phillips S, 'Legal Considerations for Electronic Evidence, Part 5: Original vs. Duplicate Documents & Unfair Prejudice' *The Documentalist* (27 July 2010) <https://crlgrn.wordpress.com/2010/07/27/legal-considerations-for-electronic-evidence-part-5-original-vs-duplicate-documents-unfair-prejudice/> accessed 23 January 2023.

Cases

Beheersmaatschappij and Another v The Magistrate Cape Town 2004 SA SCA 5635.

Lorraine v Markel American Ins. Co. 2007 241 FRD 534, 544 (D Md).

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

Muller v BOE Bank Ltd and Others 2011 (8723/98) 2010 ZAWCHC 121; 2011 (1) SA 252 (WCC); 2011 (1) All SA 166 (WCC).

R v Munshi 2002 CanLII 39110 (ON SC).

R v Vu 2013 SCJ No 60, 2013 (3) SCR 657.

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

United States v Hernandez 183 F Supp 2d 468, 480–81 (DPR 2002).

United States v Metter [no 10-CR-600 (EDNY 05/17/2012)].

United States v Syphers 426 F 3d 461, 469 (1st Cir 2005).

United States v Triumph Capital Grp., Inc. 211 FRD 31, 66 (D Conn 2002).

Legislation

Australian Crimes Act 12 of 1914.

Constitution of the Republic of South Africa 1996.

Criminal Procedure Act 51 of 1977.
Cybercrimes Act 19 of 2020.

Electronic Communications and Transactions Act 25 of 2002.

US Constitution.

US Federal Rules of Criminal Procedure Rule 41, Search and Seizure 2009.