**RESEARCH TITLE:**

Discovery of electronic information in legal proceedings in South Africa with specific reference to Rule 23 of the Magistrates' Court Rules and Rule 35 of the Uniform Rules of Court

Name: **MR. ELTON ROMEO HART**
Student Number: **19401630**
Degree: **LLM (FULL DISSERTATION)**
Supervisor: **DR WILLEM GRAVETT**

**CHAPTER 1: INTRODUCTION**



**CHAPTER 2: DEVELOPMENT OF THE TERM DOCUMENT**



**CHAPTER 3: PRESERVATION AND RETENTION OF ELECTRONICALLY GENERATED AND STORED INFORMATION IN THE FOURTH INDUSTRIAL REVOLUTION**



**CHAPTER 4:THE IMPACT OF THE BILL OF RIGHTS ON PRIVACY, CONFIDENTIALITY AND PRIVILEGE ARISING DURING THE DISCOVERY OF ELECTRONICALLY GENERATED AND OR ELECTRONICALLY STORED INFORMATION IN PRE-TRIAL STAGES AND TRIAL**

## 8. BIBLIOGRAPHY

# CHAPTER ONE

## 1. INTRODUCTION

## 1.6 IMPORTANCE OF STUDY

> "I am therefore unable, in terms of the prevailing law, to admit as evidence the disputed documents which contain information that has been processed and generated by a computer. All that I can do is add my voice to the call that this lacuna in our law be filled and for new legislation relating specifically to computer evidence in criminal cases be considered and promulgated."[1]

The explosive growth in the use of digital devices in South Africa to generate and disseminate information and the increased flow of information on digital media to conduct business and conclude agreements have brought a new source of evidence to the legal fraternity in the form of electronically generated information[2] and electronically stored information.[3] This study will refer to EGI and ESI simply as electronic information. In the matter of *Trustees for the Time Being of the Delsheray Trust and Others v ABSA Bank Limited*[4], the Court made this observation:[5]

> It is well known that modern technological developments have brought about a revolution in the way that information, including legal information, is captured and disseminated. These

---

1 *S v Mashiyi* 2002 (2) SACR 387 (Tk) at paragraph. See De Villiers "Old "documents," "videotapes" and new "data messages" – a functional approach to the law of evidence (Part 1)" (2010) TSAR 563. De Villiers disagrees with the Court in Mashiyi and is of the view that the court ignored the common law.

2 Schmidt and Rademeyer *Law of Evidence* (2017) 12-10; Wheater and Raffin *Electronic Disclosure Law and Practice* (2017) 5; Hughes "The rise of electronic discovery" 2012 *De Rebus* 24; See Herbstein and Van Winsen *The Civil Practice of the High Courts of South Africa* (2015) 812-813 and De Villiers "Old "documents", "videotapes" and new "data messages" – a functional approach to the law of evidence" (Part 2) 2010 *TSAR* 720. In these two aforementioned works, the authors said that crucial evidential information is generated electronically and stored on mechanical devices such as laptops, cellular phones, and other digital devices. For purposes of this study writer will refer to electronically generated information as **"EGI"**.

3 Cohen and Lender *Electronic Discovery: Law & Practice* (2012) 2-3; See Schwerha; Bagby and Esler "United States of America" in Mason *Electronic Evidence* (3rd ed) 798; Van Dorsten "Discovery of electronic documents and attorneys' obligations" November 2012 *De Rebus* 34; Chorvat and Palenek "Electronically Stored Information in Litigation" *The Business Lawyer (Bus. Law)* 287; Takombe "The rise of the machines - understanding electronic evidence" August 2014 *De Rebus* 32 and Smith "Electronic Discovery and the Constitution: Inaccessible Justice" *Journal of Legal Technical and Risk Management* (2012) 125. According to Smith, electronically stored information which the writer will refer to as **"ESI",** is available on: "digital devices, such as computers, laptops, smartphones and includes email, web pages, word processing files, audio, and video files, images, computer databases and virtually anything that is stored on a computing device- including but not limited to servers, desktops, laptops, cell phones, hard drives, flash drives, PDAs and MP3 players".

4 [2014] 4 All SA 748 (WCC).

5 See *Trustees for the Time Being of the Delsheray Trust and Others v ABSA Bank Limited* at paragraph18.

developments brought about substantial changes in the law of computer-generated evidence, internationally and in South Africa.

This research will examine if electronic information falls within the scope and ambit of the term "document" or whether the definition of the "term" "document" should be extended to include this new source of evidence. Further, this study will also examine if electronic information is discoverable within the current procedural framework in South Africa. This source of evidence can prove to be useful in legal proceedings.

The process of discovery in South African law is regulated by the Rules Regulating the Conduct of Proceedings in the Magistrates' Court in terms of the Magistrates' Court Act[6] (hereinafter referred to as the Magistrates' Court Rules)[7], the Rules Regulating the Conduct of Proceedings of the Several Provincial and Local Divisions of the High Courts of South Africa in terms of the Supreme Court Act[8] (hereinafter referred to as the Uniform Rules of Court)[9] and Rules for the Conduct of Proceedings in the Labour Court in terms of the Labour Relations Act (hereinafter referred to as the Labour Court Rules)[10] respectively in civil proceedings.

Electronic information contains hidden information that is known as metadata in digital form on digital devices.[11] Metadata is information embedded in documents generated and stored in electronic or digital form.[12] Metadata is hidden when documents generated

6 Act 32 of 1944.
7 Rule 23(1) of the Magistrates' Court Rules.
8 Act 59 of 1959.
9 Rule 35(1) of the Uniform Rules of Court.
10 Act 66 of 1995.
11 Basdeo "The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis" *SACJ* (2012) 2 198 and Basdeo "Criminal and procedural legal challenges of identity theft in the cyber and information age" SACJ 363. See *Byers v. Illinois State Police*, 53 Fed.R.Serv.3d 740, No. 99 C 8105, 2002 WL1264004 (N.D. Ill. May 31, 2002).
12 According to Hughes (n 2 above) 24, "there is a lot of detail attached to electronic information captured as metadata of that information in case of an email that includes the time that information was dispatched or received by the mail servers and the exact route that the mail message followed." See South African Law Reform Commission *"Electronic Evidence in Civil proceedings: Admissibility and Related Issues"* Discussion Paper 131, Project 126. Review *of the Law of Evidence* (31 October 2014) 30. For a more thorough discussion, *See The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (2nd ed) 2007, where the authors crafted the following definition of metadata: "Data typically stored electronically that describes characteristics of ESI, found in different places in different forms." Metadata can be supplied by applications, users or the file system. Metadata can describe how, when and by whom ESI was collected, created, accessed, modified and how it is formatted. Metadata can be altered intentionally or inadvertently. Certain metadata can be extracted when native files are processed for litigation. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users

and stored in electronic or digital form are viewed on the screens of digital devices or printouts.[13] This form of information may contain vital characteristics of the information viewed on the screens of digital devices. This embedded information may contain privileged and confidential information that is not apparent to the reader when viewed on the screens of digital devices or printouts. The Sedona Conference Working Group identified the following types of metadata:[14]

> Application Metadata: Data created by the application-specific to the ESI being addressed, embedded in the file, and moved with the file when copied; copying may alter application metadata.
>
> Document Metadata: Properties about the file stored in the file, as opposed to document content. Often this data is not immediately viewable in the software application used to create/edit the document but often can be accessed via a "properties" view. Examples include document author and company and create and revise dates.
>
> Email Metadata: Data stored in the email about the email. Often this data is not even viewable in the email client application used to create the email, e.g., blind copy addresses received to date. The amount of email metadata available for a particular email varies greatly depending on the email system. Contrast with File System Metadata and Document Metadata.
>
> Embedded Metadata: Generally hidden, but an integral part of ESI, such as "track changes" or "comments" in a word processing file or "notes" in a presentation file. While some metadata is routinely extracted during processing and conversion for e-discovery, embedded data may not be. Therefore, it may only be available in the original, native file.
>
> File System Metadata: Metadata generated by the system to track the demographics (name, size, location, usage, etc.) of the ESI and, not embedded within, but stored externally from the ESI.

---

who are not technically adept. Metadata is generally not reproduced in full form when a document is printed on paper or electronic image. *See also* Application Metadata, Document Metadata, Email Metadata, Embedded Metadata, File System Metadata, User-Added Metadata and Vendor-Added Metadata."

13 See Schafer and Mason "The characteristics of electronic evidence" Mason and Seng *Electronic Evidence* (4th ed) 28. The authors stated: "metadata can be categorized in three broad categories namely (i)Descriptive metadata; (ii)Structural metadata and (iii)Administrative metadata."
Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not tech savvy. Metadata is generally not reproduced in full form when a document is printed to paper or electronic image. For a more thorough discussion, *see The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* ( 2nd ed) 2007.

14 See The Sedona Conference Glossary: *E-Discovery & Digital Information Management* (3rd ed) 2011 at 35.

> User-Added Metadata: Data, possibly work product, created by a user while copying, reviewing, or working with a file, including annotations and subjective coding information.
>
> Vendor-Added Metadata: Data created and maintained by the electronic discovery vendor as a result of processing the document. While some vendor-added metadata has direct value to customers, much of it is used for process reporting, chain of custody, and data accountability. Contract with User-Added Metadata."

One of the major challenges of electronic discovery is the identification, collection, preservation, and production of relevant metadata.[15] This requires that parties need to discuss the preservation and discovery of electronic information and the metadata that attaches to the electronic information. Parties need to confine the discussion to electronic information and metadata that is relevant and admissible, and all parties should have a common understanding of what metadata entails.

The availability of electronic information sometimes referred to as "electronic evidence"[16] brought substantial challenges and changes to the legal fraternity on how to handle electronic information as evidence.[17] In the matter of *S v Ndiki*[18] Van Zyl J stated:

> It seems that it is often too readily assumed that, because the computer and the technology it represents is a relatively recent invention and subject to continuous development, the law of evidence is incapable or inadequate to allow for evidence associated with this technology to be admissible in legal proceedings.

This opinion expressed by Van Zyl J can be interpreted to imply that our law of evidence is geared to facilitate the discovery of electronic evidence in legal proceedings and must be developed to keep pace with changing technology. In most instances, electronic information is never reduced to paper.[19] According to Bouwer, the concept of electronic

---

15 Scheindlin *Electronic Discovery and Digital Evidence* (2nd ed) 215.

16 Schwikkard and Van der Merwe *Principles of Evidence* (4th ed) 437.

17 Hofman "Electronic evidence in criminal cases" (2006) SACJ 257 and Bouwer "Search and seizure of electronic evidence: Division of the traditional one step process into a new two-step process in a South African context" 2014 *SACJ* 158 and Takombe (n 3 above) 32.

18 2008 (2) SACR 252 (Ck).

19 De Villiers (n 2 above) 723; Cassim "The use of electronic discovery and cloud computing technology by lawyers in practice: lessons from abroad" *Journal for Juridical Science* 19; Hughes (n 2 above) 24 and Theophilopoulos "The admissibility of data, data messages, and electronic documents at trial" 2015 *TSAR* 463 made the following remark: "an electronic document is superficially defined as data or electronic information which when generated, sent, received and stored electronically becomes a data message." This implies that the data message and an electronic documents equates to electronic information.

evidence is new to the South African legal fraternity and challenges the operation of rules of evidence in South Africa.[20] This raises the question: under what circumstances is this new source of evidence admissible, and how must this type of evidence be handled by litigants during the discovery process in pre-trial preparation?

20 Harrison "Bringing advancing technology in litigation – time to explore electronic discovery" August 2019 *De Rebus* 22 and Bouwer (n 17 above) 156.

## 1.2 BACKGROUND OF STUDY

As the position stands in South Africa, it is uncertain if the term "document" referred to in the Magistrates' Court Rules,[21] the Uniform Rules of Court[22] , and the Labour Court Rules[23] can be read to include electronically generated information and electronically stored information for purposes of discovery, as set out on the Magistrates' Court Rules, the Uniform Rules of Court and the Labour Court Rules.[24]

This study will examine if the definitions of the term "document" that is contained in national legislation can be read to include electronic information for purposes of discovery. Alternatively, if the definitions of the term "document" in the Civil Proceedings Evidence Act 25 of 1965 (hereinafter referred to as the CPEA)[25] and Criminal Procedure Act 51 of 1977 (hereinafter referred to as the CPA)[26] can be equated to a "data message" as defined in the Electronic Communications and Transactions Act 25 of 2002 (hereinafter referred to as the ECTA).[27] If the definition of the term document in the CPEA and CPA cannot be extended to include electronically generated information and electronically stored information, can measures be introduced to ensure that electronically generated information and electronically stored information are not merely inadmissible as evidence because of its electronic nature?

This study will investigate the evidentiary issues that attach to the discovery of electronic information in light of the Constitutional dispensation in South Africa.[28] In particular, the study refers to the right to privacy[29], right to access to information,[30] an accused

---

21 See reference to the term document in rule 23(1) of the Magistrates Court Rules. The definitions clause of the Magistrates' Court Rules does not contain a definition for the term document.

22 See reference to the term document in rule 35(1) of the Uniform Rules of Court. The definitions clause of the Uniform Rules of Court does not contain a definition for the term document.

23 See reference to the term document in Rule 6(9) and the definitions clause of the Labour Court Rules do not define the term document.

24 Van Heerden *Voorbereiding vir verhoor ter verwesenliking van die waarborg van 'n billike verhoor* (unpublished LLD thesis RAU May 2004) 106; See *S v Ndiki* (n 18 above) and *Ndlovu v Minister of Correctional Services* 2006 4 ALL SA165 (W).

25 Act 24 of 1965. The CPEA was assented to and promulgated on 30 June 1967. The aim of the CPEA was to codify evidentiary issues pertaining to civil matters.

26 Act 51 of 1977 (as amended).

27 Act 25 of 2002. The ECTA was assented to on 31 July 2002 and came into operation on 30 August 2002.

28 The Constitution of the Republic of South Africa, 1996 (hereinafter referred to as the Constitution).

29 Section 14 of the Constitution.

30 In the matter of *My Vote Counts NPC v Speaker of the National Assembly and Others* 2016 (1) SA 132 (CC), the court held that: "PAIA is the legislation envisaged in terms of Section 32(2) of the

Constitution that was intended fully to give effect to the right of access to information." Section 32 states as follows: "everyone has the right of access to – (a) any information held by the state; and (b) any information that is held by another person and that is required for the exercise or protection of any rights. National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state." In order to fully comprehend the operation of the right to access to information, one must read section 9(a) (ii), section 11(1) and section 50(1)(a) of PAIA. PAIA was enacted to give effect to the right of access to information guaranteed by section 32(1) (b) of the Constitution. See Van der Merwe *et al. Information and Communications Technology Law* (2008) 24. Section 11(1) read as follows: "A requester must be given access to a record of a public body if –(a) that requester complies with all the procedural requirements in this Act relating to a request for access to that record; and (b) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.". Section 50(1) (a) of PAIA provides: "A requester must be given access to any record of a private body if that record is required for the exercise or protection of any rights." In the matter of *Unitas Hospital v Van Wyk* 2006 (4) SA 436 (SCA) the court held: "that anyone who requests information must first establish a right to the required information before you can request the information."

person's right to a fair trial,[31] and access to justice[32] to determine whether electronic evidence is admissible and discoverable within the South African procedural framework, subject to the evidentiary rules applicable in South African law. Recently in *S v Pistorius*,[33]the accused's cellular phone was seized to retrieve electronic evidence that was allegedly generated and stored thereon.[34]

---

31 See section 35 of the Constitution, which reads as follows:

(1) "Everyone who is arrested for allegedly committing an offence has the right (a). to remain silent; (b). to be informed promptly (i). of the right to remain silent; and (ii). of the consequences of not remaining silent; (c). not to be compelled to make any confession or admission that could be used in evidence against that person; (d). to be brought before a court as soon as reasonably possible, but not later than (i). 48 hours after the arrest; or (ii). the end of the first court day after the expiry of the 48 hours, if the 48 hours expire outside ordinary court hours or on a day which is not an ordinary court day; (e). at the first court appearance after being arrested, to be charged or to be informed of the reason for the detention to continue, or to be released; and (f). to be released from detention if the interests of justice permit, subject to reasonable conditions."

(2) "Everyone who is detained, including every sentenced prisoner, has the right (a). to be informed promptly of the reason for being detained; (b). to choose, and to consult with, a legal practitioner, and to be informed of this right promptly; (c). to have a legal practitioner assigned to the detained person by the state and at state expense, if substantial injustice would otherwise result, and to be informed of this right promptly; (d). to challenge the lawfulness of the detention in person before a court and, if the detention is unlawful, to be released; (e). to conditions of detention that are consistent with human dignity, including at least exercise and the provision, at state expense, of adequate accommodation, nutrition, reading material and medical treatment; and (f). to communicate with, and be visited by, that person's (i). spouse or partner; (ii). next of kin; (iii). chosen religious counsellor; and (iv). chosen medical practitioner."

(3) "Every accused person has a right to a fair trial, which includes the right (a). to be informed of the charge with sufficient detail to answer it; (b). to have adequate time and facilities to prepare a defence; (c). to choose, and be represented by, a legal practitioner, and to be informed of this right promptly; (g). to have a legal practitioner assigned to the accused person by the state and at state expense, if substantial injustice would otherwise result, and to be informed of this right promptly; (h). to be presumed innocent, to remain silent, and not to testify during the proceedings; (i). to adduce and challenge evidence; (j). not to be compelled to give self-incriminating evidence; (k). to be tried in a language that the accused person understands or, if that is not practicable, to have the proceedings interpreted in that language; (l). not to be convicted for an act or omission that was not an offence under either national or international law at the time it was committed or omitted; (m). not to be tried for an offence in respect of an act or omission for which that person has previously been either acquitted or convicted; (n). to the benefit of the least severe of the prescribed punishments if the prescribed punishment for the offence has been changed between the time that the offence was committed and the time of sentencing; and (o). of appeal to, or review by, a higher court."

(4) "Whenever this section requires information to be given to a person, that information must be given in a language that the person understands. Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice."

32 See section 34 of the Constitution that reads as follows: "Everyone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum."

33 [2014] ZAGPPHC 793.

34 The state in casu intended to examine the data messages that was disseminated between the accused and the deceased prior to the deceased's death.

One should be mindful that gathering electronic evidence must be done expertly and with due observance of constitutional values.[35] A clear example of this is seen in Europe, where the European Parliament adopted the European Community Data Protection Directive.[36] The directive protects fundamental rights and freedoms, particularly the right to privacy and regulates the flow of personal data around the European Union.

Legal practitioners must possess the necessary computer literacy skills to protect their client's interests in matters involving electronic information as evidence.[37] On the other hand, judicial officers must be aware of the ever-changing technology to adjudicate matters in the digital age.[38] The fact that legal practitioners and information technology specialists do not work from the same frame of reference further complicates issues brought about by the fourth industrial revolution.[39]

The ECTA has now been in operation for more than 18 years.[40] This study will examine if the ECTA sufficiently developed our procedural law framework to keep abreast with the technological advancements to identify, collect, record, preserve, retain and produce electronic information in a readable format when litigation is pending or foreseen.[41]

According to Bouwer and Hofman, the lack of detailed procedures for the identification, collection, preservation, management, and production of electronic information in South Africa contributes to the uncertainty of how legal practitioners and their clients handle electronic information, before legal proceedings commence or when legal proceedings are pending.[42]

---

35 See Bouwer (n 17 above) 156 and Schwikkard and Van der Merwe *Principles of Evidence* 3rd edition 417.

36 The European Convention on Human Rights incorporates privilege into domestic English law by the Human Rights Act 1998. See http://www.wipo.int/wipolex/en/text.jsp?file_id=313007 accessed on 16 July 2018.

37 See Cohen and Lender (n 3 above) 14-1.

38 Cassim (n 19 above) 19.

39 Cohen and Lender (n 3 above) 16-12-16-13; De Villiers (n 1 above) 558; Hughes (n 2 above) 24; Herbstein & Van Winsen (n 2 above) 811; Papadoulos and Snail *The law of the Internet in South Africa* (3rd ed) Cyberlaw@SA III 19 and Reavis "How technically savvy is your legal council?" 2008 *Journal of International Commercial Law and Technology* 276-277.

40 The Act was assented to on 31 July 2002 and came into operation on 20 August 2002.

41 Smith (n 3 above) 122 129.

42 See Bouwer (n 17 above) 170 and Hofman (n 17 above) 274.

One should be mindful that this problem does not seem to be confined to South Africa but is a global phenomenon in litigation.[43] This led to the establishment of the Forensic Science Regulator in the United Kingdom in 2008 to develop guidelines and standards for digital forensics.

The available academic writing on the topic of electronic discovery and the successful implementation of electronic discovery in the United Kingdom and the United States of America has greatly motivated the quest for research into this area of procedural law in South Africa.

43 Schafer and Sheldon "Proof: the technical collection and examination of electronic evidence" in Mason and Seng *Electronic Evidence 4th* ed 285.

## 1.3 THE RESEARCH QUESTIONS

The exponential growth in using and disseminating electronic information to conduct business and conclude agreements has brought substantial challenges to modern-day litigation and legal processes.[44] This research will attempt to answer the following questions:

1. ANALYSIS OF THE TERM DOCUMENT

   1.1. What constitutes a "document" in the digital age as mentioned in Rule 23 (1) of the Magistrates' Court Rules, Rule 35(1) of the Uniform Rules of Court, and Rule 6(9) of the Labour Court Rules?

   1.2. Can the definitions of the term "document" as provided in CPA and CPEA, be extended to include electronic information for purposes of discovery?[45]

   1.3. Is a "document" and "data message" on equal footing as stipulated in the Electronic Communications and Transactions Act?[46]
2. Does the current procedural framework in South Africa make provision for the preservation, retention, and discovery of electronic information in legal proceedings?
3. Are legal practitioners aware of what is expected of them to preserve and retain electronic information in readable form when litigation is pending or foreseen?
4. Is electronic information admissible as evidence, and how should litigants deal with electronic evidence during the process of discovery?
5. Are the rules of evidence in South Africa adequate to admit evidence in electronic form in legal proceedings?[47]
6. Is electronic evidence so different from paper-based evidence that legislative reform is required to regulate the discovery of electronic evidence?
7. Has the South African judiciary developed the law of evidence to keep abreast of the rapidly changing technological environment in South Africa? This will be done with a view to the Constitutional dispensation, with specific reference to confidentiality, privacy, and privilege.

---

44 Swales *"An analysis of the regulatory environment governing electronic evidence in South Africa: Suggestions for reform"* (unpublished LLD thesis UCT 2018) 26.

45 See *Makate v Vodacom* 2013 JOL 30668 (GSJ).

46 See section 17 of Act 25 of 2002.

47 See *S v Brown* 2016 (1) SACR 206 (WCC) 206.

This study will revisit the process of discovery, with specific reference to the impact of technological advancements on legal proceedings. One of the underlying hypotheses of the proposed research is based on the analysis of the term "document", which must include electronic information.

One of the focal points of this study is to ascertain if the Magistrates'Court Rules, the Uniform Rules of Court, and the Labour Court Rules need to be amended to keep up with technology in South Africa[48] and the United Kingdom.[49]

## 1.4 RESEARCH METHODOLOGY AND STRUCTURE

The *rationale* for the proposed research emanates from the exponential growth in the capturing and disseminating of electronic information. The proliferation of electronic information may cause that tainted evidence to be admitted and relevant evidence to be excluded in criminal or civil proceedings. To maintain the integrity of a system.

As part of this study, I previously studied the process of discovery in the United States of America and the United Kingdom. Both the aforementioned jurisdictions adapted their respective procedural frameworks and how they applied their respective evidentiary rules to facilitate the discovery of electronic information.

This study will also consider ethics and the rules applicable to the profession to ensure that information is accessible,[50] and that trials are conducted fairly.[51] The lack of detailed guidelines and principles in the current Court Rules and legislation in South Africa on how to deal with the discovery of electronic information creates uncertainty amongst legal practitioners and judicial officers.[52] This dissertation will examine if the ECTA has developed South African law to such an extent that certain shortcomings of

---

48 The discussion in this study relates to e-discovery in disputes that is subject to the Federal Rules of Civil Procedure. Parties need to consult state common and statutory laws, for the e-discovery rules applicable to other disputes not covered by the Federal Rules of Civil Procedure.

49 The United Kingdom comprises three separate legal jurisdictions: England & Wales, Scotland and Northern Ireland. In this study writer will focus on England and Wales, which is the largest jurisdiction where the main rules governing e-discovery are contained in the Civil Procedure Rules that govern all civil proceedings. New rules updating the section on electronic disclosure was introduced in October 2005.

50 See section 32 of the Constitution.

51 See section 35 of the Constitution.

52 See Harrison (n 20 above) 22.

the current legislative framework have been bridged to keep pace with the technological developments in business transactions and the global economy. The study will further attempt to establish whether electronically generated or stored information falls within the ambit of the term "document" in terms of Rule 23(1) of the Magistrates' Court Rules or the Uniform Court Rules.

As part of this study, I have consulted primary sources such as academic journal articles, published academic research works, and some electronic sources that analysed the process of discovery of electronic information in the United States of America and the United Kingdom.

This is a brief overview and outlines the seven chapters of this study. The aim and composition of each Chapter are set out below.

## 1.5 CHAPTER OVERVIEW

### CHAPTER 1: INTRODUCTION

This chapter sets out the importance, aim, research questions, methodology, and structure of this study.

### CHAPTER 2: DEVELOPMENT OF THE TERM DOCUMENT

The chapter will analyse the systematic development of the definition of the term "document" in court cases and pursuant to legislation in South Africa. However, the issue will not be analysed in-depth. The purpose is only to give context to the definition of the term "document" as captured in South African legislation. Secondly, this chapter will examine if electronic information could be classified as real or documentary evidence and how the existing evidentiary rules and principles must be applied to admit electronic information as evidence.

### CHAPTER 3: PRESERVATION AND RETENTION OF ELECTRONICALLY GENERATED AND STORED INFORMATION IN THE FOURTH INDUSTRIAL REVOLUTION

The first part of this chapter will investigate how courts in the United States of America and the United Kingdom have dealt with the identification, preservation, and retention of electronic information during pre-trial preparation and discovery.

Secondly, it will briefly focus on the ethical duties of legal practitioners and their clients to preserve and retain electronic information in its original form. It is also important to note that electronic information contains hidden information, generally referred to as metadata.[53] Burke defines metadata as follows: "This embedded data provides information about an electronic file, such as when the document was created, the author's identity, when and by who is what edited, all of which is known as metadata." Metadata can prove to be a vital source of evidence associated with electronic information.[54]

## CHAPTER 4: THE IMPACT OF CONFIDENTIALITY, PRIVACY, AND PRIVILEGE ON DISCOVERY OF ELECTRONIC INFORMATION IN PRE-TRIAL STAGES AND TRIAL

The gathering of evidence must be done expertly and with due observance of the Constitution, specifically where the evidence will be used in criminal proceedings.[55] The chapter will firstly examine the constitutional questions raised by the discovery of electronic information in legal proceedings. Secondly, it will investigate how the common law principle of privilege affects the discovery of electronic information in legal proceedings.[56] Evidence obtained in breach of a person's constitutional rights might render that evidence inadmissible.[57] According to Schwikkard and Van der Merwe, privilege can be described as a personal right to refuse to discover admissible evidence.[58]

## CHAPTER 5: CURRENT DEVELOPMENTS

53 See Hughes (n 2 above) 25 and Burke et al "Electronic Discovery: Rules for a Digital Age" 2012 *Boston University Journal of Science & Technology Law B.U.J.SCI. &TECH.L.* 150 165.
54 See Harrison (n 20 above) 22.
55 Schwikkard and Van der Merwe (n 35 above) 417.
56 George "Someone's watching: Protecting Privilege on Both Sides of the Table During Electronic Discovery" *Journal of Law, Technology and Policy* J.L. Tech & Poly 2004 288.
57 Schwikkard and Van der Merwe (n 16 above) 50.
58 Schwikkard and Van der Merwe (n 35 above) 124.

This chapter will provide an overview of the latest developments in case law with reference to the preservation, retention, admissibility, and eventually, the discovery of electronic information.

## CHAPTER 6: DISCOVERY

This chapter will briefly introduce the rules that facilitate the discovery of electronic information in the United States of America, the United Kingdom and the process of discovery as envisaged in rule 23 of the Magistrates Court Rules and Rule 35 of the Uniform Rules of Court in South Africa. Thereafter this chapter will compare and discuss the process of discovery of electronic information in the United States of America, the United Kingdom and compare South Africa against these jurisdictions in both pre-trial preparation and trials. According to Hughes, the discovery of electronic information is not adequately addressed by the Magistrates' Court Rules or the Uniform Rules of Court. [59]

This chapter will also specifically refer to the development of the court rules applicable to the discovery of electronic information in the United States of America and the United Kingdom to determine whether any of these developments may have an influence on the rules of court in South Africa, and thus inform the dissertations' conclusion.

## CHAPTER 7: CONCLUSION AND RECOMMENDATIONS

This final chapter will give an overview of this study and summarise the conclusion and recommendations of this study.

---

59 South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic evidence in Criminal and Civil proceedings: Admissibility and Related Issues Review of Law of Evidence* 81.

## CHAPTER 2: DEVELOPMENT OF THE TERM DOCUMENT

### 2.1 Overview

In South Africa, the definition of the term "document" varies between statutes. To comprehend the aim of the existing statutory definitions of "document", it is illustrative to look at the jurisprudential development of these statutory provisions.

As early as 1908, in *R v Daye*[60], the question of what constitutes a "document" was considered by courts in common law jurisdictions. Darling J said: "it is a document no matter on what material it be."[61] The Concise English Oxford dictionary defines a document as follows: "a piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record."[62] One needs to ascertain what the statutory definitions of the term "document" are in South African law. In two of the three jurisdictions referred to in this study, namely the United States and the United Kingdom, legislation has been enacted to provide definitions for the term "document".[63]

In the matter of *Seccombe v Attorney General*[64], the term document is described as follows:[65]

> The word document is a very wide term and includes everything that contains the written or pictorial proof of something. It does not much matter of what material it is made. If it contains in writing or cyphers proof of some facts it is a document, and the fact that a number of leaves happen to be bound together so as to take the appearance of a book cannot make any difference. If in fact it contains written proof of facts, it is a document.

It seems that neither South African courts[66] nor legal scholars are ad idem on what constitutes a "document".[67] The term "document" as defined in national legislation

---

60 [1908] 2 KB 333.
61 See *R v Daye* [1908] 333 on page 340 of judgment.
62 See Concise Oxford English Dictionary Twelfth Edition.
63 See CPR Rule 31.4 in the United Kingdom and Rule 26 and 34 of the Fed.R. Civ.P in the USA.
64 1919 TPD 270.
65 See *Seccombe v Attorney General* 1919 TPD 270 on page 277- 278 of the judgment.
66 See *S v Ramgobin* 19864 SA 117(N); *S v Baleka* 1986 4 SA 192(T) and *S Mpumlo* 1986 3 SA 485(E).
67 De Villiers (n 1 above) 565 and Hughes and Stander "eDiscovery in South Africa and the Challenge it Faces" 61 available at https://www.researchgate.net/publication/284173757_Ediscovery_in_South_Africa_and_the_Challenges_it_Faces.

differs from each other.[68] The lack of cohesiveness and parity between the CPA[69] and the CPEA[70] of what constitutes a "document" creates the impression that what is admissible as a document in civil proceedings differs from what is admissible as a document in criminal proceedings and creates much uncertainty amongst legal practitioners.[71] Section 221 of the CPA defines the term "document" as follows: "document includes any device by means of which information is recorded or stored". Section 33 of the CPEA defines a document as follows: "any book, map, plan, drawing or photograph". Although section 222 of the CPA transposed the application of section33 up until section 38 of the CPEA into criminal matters in South Africa, it seems that the disparity between the definitions of the term "document" in the CPA and the CPEA seems to suggest that electronic information may be excluded from discovery in civil matters but may be allowed as evidence in criminal matters.[72]

The ECTA[73] was specifically enacted to facilitate e-commerce and the exchange of electronic information between individuals and businesses in South Africa.[74] The ECTA transposed the doctrine of functional equivalence into South African law.[75] At the core of the principle is the doctrine of functional equivalence, which awards a "data message" the same legal, procedural and evidentiary status in civil matters as that of a paper document by establishing a statutory regulatory framework that provides for equal

---

68 See Schwikkard and Van der Merwe (n 35 above) 404 and Schwikkard and Van der Merwe (n 16 above) 431.

69 See (n 25 above).

70 See (n 24 above).

71 See Swales (n 44 above) 29.

72 See SALRC report (n 12 above) 81. See http://www.justice.gov.za/salrc/dpapers/dp131-prj126-ReviewLawOfEvidence.pdf (18-09- 2017). See Swales (n 44 above) 29.

73 See ECTA description (n 26 above).

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

75 The ECTA is modelled on the United Nations Commission on International Trade Law Model Law (hereinafter referred to Model Law) with Guide to Enactment 6-12-1996. According to UNCITRAL: "This instrument facilitates commerce and business conducted using electronic means and provide legislators in various countries with internationally acceptable rules to eliminate legal obstacles and increase electronic commerce. In particular, the limitations that emanates from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for enabling the use of paperless communication, thus fostering efficiency in international trade." See http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (last accessed on 14-10-2018).

treatment to users of paper-based documentation and users of electronic information.[76] Theophilopoulos stated:[77]

> In principle, the medium in which information is generated and stored, irrespective if it is paper or electronic, is irrelevant and does not affect the information's legal significance.

This means that information contained in the form of a "data message" is a document, but is not necessarily seen as documentary evidence. Various sections of the ECTA imply that electronic information is not different from paper documents. One of the core issues underlying the concept of functional equivalence is that it seeks to provide or facilitate an electronic equivalent for written, signed, and original paper documents.

The Magistrates' Court Rules, the Labour Court Rules, the Uniform Rules of Court, and ECTA refer to the term "document" but do not contain a definition of the term "document" in their respective definition clauses. It is uncertain if any of the current statutory definitions of the term "document" in the CPEA and CPA can be extended to include electronic information or a "data message" for purposes of discovery in legal disputes. The ECTA contains several references to the term "document"[78] but is silent on what constitutes a document or even transposes the definition in the CPA or CPEA into the ECTA.

In the United States, the issue of electronic information came to the fore in a series of decisions that considered the question of whether electronic information falls within the

---

76 See Theophilipoulos (n 19 above) 465. See Hofman (n 17 above) Careful consideration of various sections of the ECTA implies that electronic information is not different from paper documents. One of the core issues underlying the concept of functional equivalence is that it seeks to provide or facilitate for an electronic equivalent for written, signed and original paper documents.

77 Theophilopoulos (n 19 above) 464.

78 Sections 12, 17 and 19 of the ECTA is examples of this where reference are made to the term "document" in the ECTA.

definition of the term "document" or not.[79] In the matter of *Anti-Monopoly, Inc. v. Hasbro, Inc.*[80], No. 94 the court made the following observation:[81]

> [i]nclusive description of documents is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this may require the respondent to supply a printout of the data compilation.

The 2006 amendments to the Federal Rules of Civil Procedure (hereinafter referred to as Fed.R. Civ.P), by implication extended the definition of the term "document" to include electronically stored information as evidence that is discoverable in legal proceedings.[82]

The question of what constitutes a "document" also came under scrutiny in the United Kingdom. In the matter of *Derby & Co Ltd v Weldon* (No 9)[83] Justice Vinelott made the following observation:[84]

> [a]fter reading a considerable volume of evidence and hearing argument, I stated summarily the conclusion that I had reached, which was that the database, so far as it contains information capable of being retrieved and converted into readable form, is a document within the meaning of R.S.C., Ord. 24 of which discovery must be given.

This implies that electronic information that is capable of being stored and retrieved without tampering with the originality, integrity, and authenticity of that information falls

---

79 See *Rowe Entertainment v. William Morris Agency* 205 F.R.D. 421 (S.D.N.Y. 2002) and *Zubulake v UBS Warburg* LLC 217 F.R.D. 309 (S.D.N.Y 2003) hereinafter referred to as "*Zubulake I; Zubulake v UBS Warburg* LLC 230 F.R.D. 290 (S.D.N.Y 2003) hereinafter referred to as "*Zubulake II"*; *Zubulake v UBS Warburg* LLC 216 F.R.D. 280 (S.D.N.Y 2003) hereinafter referred to as "*Zubulake III"*; *Zubulake v UBS Warburg* LLC 220 F.R.D. 212 (S.D.N.Y 2003) hereinafter referred to as "*Zubulake IV* and *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) hereinafter referred to as "*Zubulake V*; *Mosaid Techs., Inc. v. Samsung Elecs. Co*., 348 F. Supp. 2d 332, 336 (D.N.J. 2004); *United States v. Philip Morris USA, Inc*., 2004 U.S. Dist. LEXIS 13580 (D.D.C., July 21, 2004); *Antioch Co. v. Scrapbook Borders Inc*., 210 F.R.D. 645 at 652 (D. Minn. 2002); *Simon Property Group L.P. v. Simon Inc*., 194 F.R.D. 639 at 640 (S.D. Ind. 2000)).

80 Civ. 2120, 1995 WL 649934, (S.D.N.Y. Nov. 3, 1995)

81 See *Anti-Monopoly, Inc. v. Hasbro, Inc.,* No. 94Civ. 2120, 1995 WL 649934, (S.D.N.Y. Nov. 3, 1995) at paragraph 4. In *Bills v. Kennecott Corp.,* 108 F.R.D. 459,463-64 (D. Utah 1985) the court said: "Information stored in computers should be as freely discoverable as information not stored in computers."

82 See Rule 34(a)(1)(A) of the Fed.R.Civ.P.

83 [1991] 1 WLR 652.

84 See *Derby & Co Ltd v Weldon* (No 9) [1991] 1 WLR 652 at paragraph 1.

within the ambit of the term "document". In the matter of *Kennedy v Information Commissioner and Another,*[85] the court once again considered the question of what constitutes a "document".[86] The Court had to determine if the definition in section 32(2) of the Freedom of Information Act, 2000 encompasses electronic documents as well as hard copy documents. The court held that the word "document" was not confined to hard copy documents. The court held that it included electronic documents. As recent as the year 2012, in the matter of *Phaestos v Ho*[87] the court still grappled with the question as to what constitutes a document. It seems from jurisprudence that there existed some uncertainty amongst legal practitioners in the United Kingdom whether particular evidence constitutes a "document" or not.[88]

Courts in the United Kingdom extended the definition of the term "document" to anything upon which information was recorded and stored. This included films, digital information on databases, backup systems, and servers.[89] The jurisprudential development of the term "document" by courts in the United Kingdom led to the amendment of the Civil Procedure Rules, 1998 (hereinafter referred to as CPR).[90] Legislative reform in the United Kingdom brought changes to the definition of the term "document" in the CPR.[91]

The CPR and Practice Directions in the United Kingdom currently define the term "document"[92] as well as for an electronic document.[93] Rule 31.4 reads as follows: "document means anything in which information of any description is recorded".

---

85 [2010] EWHC 475.

86 In *Kennedy v Information Commissioner and Another* the court considered the word document as defined the Freedom of Information Act, 2000.

87 [2012] EWHC 2756 (QB).

88 In *Victor Chandler International Ltd v Customs and Excise Commissioners and another* [2000] 1 All ER 160 the court said that: "information of itself cannot constitute a document, and the transmission of information of itself cannot constitute the transmission of a document."

89 See *Grant v South Western and County Properties* [1974] 2 All E.R. 465; *Derby v. Weldon (No.9)* [1991] 1 WLR 652 and *Alliance & Leicester Building Society v. Ghahremani* [1992] R.V.R 198.

90 Part 31 of the Civil Procedure Rules, 1998 was enacted 10 December 1998 came into operation on 26 April 1999 in the United Kingdom and are as amended from time to time. Prior to the 2004 amendments to the CPR it was referred to as discovery in the United Kingdom. Regular updates of the CPR are accessible and published on the Department of Justice website available at https://www.justice.gov.uk/courts/procedure-rules/civil/rules.The CPR took full effect in matters instituted from 26 April 1999, and replaced the Rules of the Supreme Court and the County Court Rules.

91 See Rule 31.4 and Practice Direction 31A paragraph 2A.1 of the CPR in the United Kingdom.

92 See Rule 31.4 and Practice Direction 31A paragraph 2A.1 of the CPR in the United Kingdom.

93 See Practice Direction 31B Paragraph 5(3).

Practice Direction 31B (hereinafter referred to as PD31B) paragraph 5(3) defines an electronic document:

> as any document held in electronic form. It includes, for example, email and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones. In addition to documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes metadata and other embedded data which is not typically visible on screen or a printout.

Practice Direction 31A Paragraph 2A.1 reads as follows:

> Rule 31.4 contains a broad definition of a document. This extends to electronic documents, including e-mail and other electronic communications, word-processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been 'deleted'. It also extends to additional information stored and associated with electronic documents known as metadata.

The aforementioned Practice Directions set out the scope and ambit of what constitutes a "document" in the United Kingdom and even go so far as to state that it includes electronic documents.

It seems that the United States of America and the United Kingdom are ad idem that electronic information falls within the ambit of a "document" irrespective of the form it takes. In the rules of court applicable in both the United States and the United Kingdom provisions are made for the discovery of electronic information.

## 2.2 DIFFERENCES BETWEEN PAPER DOCUMENTS AND ELECTRONIC INFORMATION

Various authors have covered the differences between electronic information and information recorded on paper, film, or other media that can be read without the aid of a computer.[94] In view of Theophilopoulos,[95] it is only the medium on which the information is generated, recorded, and stored that differs in the digital age. Theophilopoulos said we need to adapt the rules of evidence to accommodate electronic evidence in legal proceedings.[96]

The Sedona Conference Working Group on Electronic Document Production[97] identified six (6) differences between traditional paper documents and electronic information and divided these differences into six categories, namely: "(a) Metadata, (b) Volume and duplicability, (c) Persistence, (d) Dynamic, changeable content, (e) Environment dependence and obsolescence and (f) Dispersion and searchability."[98]

These differences identified above may significantly impact how the rules of evidence are applied in a jurisdiction where a party wishes to produce electronic information as evidence.[99] This will be addressed in paragraph 2.3 when I discuss the classification and admissibility of electronic information as evidence. Unlike paper documents, electronic information contains metadata, one of the prickly pears related to the

94 Herbstein & Van Winsen (n 2 above) 811, Schafer and Mason (n 13 above) 27 and Hughes and Stander (n 67 above) 61 and Burke et al (n 53 above) 155.

95 Theophilopoulos (n 19 above) 461-462.

96 Theophilopoulos (n 19 above) 461-462.

97 The Sedona Conference is a forum started in 1997 by Richard G. Braman as a non-profit, research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation and intellectual property rights. This forum promoted advanced dialogue to an open think-tank confronting some of the most challenging issues faced by litigants in the American legal system. In the United Kingdom a working party chaired by the Hon. Mr Justice Creswell was set up under the auspices of the Commercial Court Users' Committee to investigate, and make recommendations as to, the particular problems thrown up by the disclosure of emails and other electronic documents and how the current Civil Procedure Rules and Commercial Court Guide on disclosure apply to electronic documents. This working party released what became known as the Creswell report. In this report they refer to the differences between traditional paper documents and electronic documents as alluded to by the Sedona Conference.

98 See *Sedona Principles Best Practices Recommendations and Principles Addressing Electronic Document Production* (2nd ed: 2007) and *Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Production,* 19 Sedona Conf. J. 1, 93–96 (2018) [hereinafter *The Sedona Principles, Third Edition*]. Harvey *Collisions in the Digital Paradigm: Law and Rule Making in the internet Age* 25-35.

99 See the Sedona Principles, Third Edition: *Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 Sedona Conf. J. 1, 56–59 (2018).

identification, collection, preservation, and production of electronic information. Legal practitioners need to take heed of the differences between paper documents and electronic information to obtain useful insights into the preservation, retention, and discovery of electronic information. This approach will help legal practitioners to identify analogies between paper documents and electronic information and see if the current rules of discovery can be used to deal with electronic information in legal disputes.

In the United States, District Judge Scheindlin alluded to these differences between paper documents and electronic documents in the matter of *Zubulake v UBS Warburg LLC*.[100] The difference between electronic information and the printed version thereof may cause that evidence, including electronic information, is classified incorrectly and subjected to the rules of evidence that are not necessarily applicable to that evidence. This afore problem is further aggravated by the fact that rules of evidence are created around paper documents and do not always provide meaningful guidance in disputes involving electronic information.[101]

100 217 F.R.D. 309 (S.N.D.Y, 2003).
101 See Schmidt and Rademeyer (n 2 above) 12-3.

## 2.3 CLASSIFICATION OF EVIDENCE AND ADMISSIBILITY ISSUES RELATED TO ELECTRONIC INFORMATION

One should be mindful that there are three (3) classes of evidence namely: oral-[102], real-[103] and documentary evidence.[104] A document may be classified as real- or documentary evidence depending on the purpose and nature for which it was created or used.[105] As mentioned in chapter one above, the ECTA transposed the doctrine of functional equivalence into South African Law.[106] Theophilipoulos reiterated this point:[107]

> The ECTA reproduces the doctrine of functional equivalence in section 1 and chapter 3, Part I of the ECT Act when read together. Particularly section 3 "interpretation"; section 11 "legal recognition of data messages"; section 12 "writing"; section 13 "signature"; section 14 "original"; section 15 "admissibility and evidential weight of a data message"; section 16 "retention"; section 17 "production of document or information"; section 18 "notarisation, acknowledgment and certification"; and in section 19 "other requirements.

It is important to take cognisance of international standards to provide and facilitate an electronic equivalent for traditional paper documents giving due considerations to the inherent differences between printed evidence and evidence in electronic form. South African authors and Courts accepted this modern approach.[108] The courts extended their acceptance of this approach, on the basis that the ECTA is consistent with global law in that a traditional document is equated to a "data message".[109]

---

102 Schwikkard and Van der Merwe (n 16 above) 388-420.

103 Schwikkard and Van der Merwe (n 16 above) 431-436; Zeffert and Paizes *The South African Law of Evidence* (2017) 457 and Schwikkard and Van Der Merwe (n 16 above) 445-446. See *Makate v Vodacom* (n 45 above) where Spilg J held that a data message is a document for purposes of rule 35 of the Uniform Rules of Court.

104 See *S v Mpumlo* 1986 4 All SA 197 (E) at par 201; Schwikkard and Van der Merwe (n 16 above) 421-430; 431-436 and Papadoulos and Snail (n 39 above) 317.

105 Zeffert and Paizes (n 103 above) 457 and De Villiers (n 1 above) 568. According to Schmidt and Rademeyer (n 2 above) 12-11: "the arrival of electronic evidence has blurred the lines between documentary evidence and real evidence." See *S v M* 2002 2 SACR 411 (SCA) 431 the court accepted a letter as evidence to proof that the letter was transmitted by the appellant to a witness and the contents of the letter was held to be irrelevant in the case.

106 See Theophilopoulos (n 19 above) 465.

107 See Theophilopoulos (n 19 above) 465.

108 See *Spring Forest Trading 599 CC v Wilberry (Pty Ltd t/a Ecowash and Combined Motor Holdings Limited t/a Green Machine Firstrand Bank Limited v Venter* [2012] JOL 29436 (SCA); Brown (n 46 above); *Jafta v Ezemvelo KZN Wildlife* (2009) 30 ILJ 131 and *Sihlali v South African Broadcasting Corporation Ltd* (2010) 31 ILJ 1477 (LC).

109 See *Jafta v Ezemvelo KZN Wildlife* (n 108 above) paragraphs 62 -99.

The ECTA defines "data" as: "electronic representations of information in any form" and if stored or disseminated it is a "data message". The ECTA defines a "data message" as:

> means data generated, sent, received, or stored by electronic means and includes-
> (a) voice, where the voice is used in an automated transaction; and
> (b) a stored record;"[110].

On the contrary, the Cybercrimes Act also defines a "data message":

> "data message means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form".[111]

This brought about that two definitions of a "data message" exist in the South African context. This is not desirable and may lead to different interpretations as to what qualifies as evidence based on the current applicable evidentiary rules.

As recent as 2017, courts in South Africa were still preoccupied with the issue of classification of electronic information as real- or documentary evidence.[112] Electronic representations of information can be classified as real- or documentary evidence depending on its origin.[113] In instances where a "data message" is classified as documentary evidence, it still needs to meet the three requirements of relevance; authenticity and the original must be produced later as required in section 34 of the CPEA. In the matter of *S v Ndiki* Van Zyl J echoed Hofman's view and made the following remark:[114]

> A preferable point of departure in my view is to rather closely examine the evidence in the issue and to determine what kind of evidence it is that one dealing with and what the requirements for its admissibility are.

110 See section 1 of the ECTA.
111 See section 1 of Cybercrimes Act 19 of 2020.
112 See *S v Meyer* 2017 JDR 1728 (GJ) at paragraph 296 until 300.
113 In *S v Brown* Bozalek J stated that electronic evidence can be treated as real or documentary evidence depending on its nature. The court further held that in the event that: "electronic evidence is classified as documentary evidence the ordinary rules of law of evidence is applicable to determine admissibility of this evidence." Hofman (n 17 above) 263. In *Ndlovu v Minister of Correctional Services and Another* (n 24 above) 172.
114 *S v Ndiki* 2008 (n 18 above) at paragraph 53.

Currently, the law of evidence is not codified in a single statute in South Africa.[115] The Constitution, various pieces of legislation,[116] the common law, and South African jurisprudence must be considered to determine if electronic information is real- or documentary evidence[117] and thereafter if it is admissible as evidence or not.[118] The South African procedural law and evidentiary rules applicable to real- and documentary evidence were developed around traditional paper documents.[119]

Documentary– and real evidence bear some similarities, but each type of evidence has its own requirements to be admissible in legal proceedings.[120] The divergence of opinions in case law[121] and literature on whether to classify electronic information as real- of documentary evidence is an issue that creates uncertainty amongst judicial officers and legal practitioners in regards to which evidentiary rules must be applied to determine the admissibility of electronic information in legal disputes.[122]

115 Schwikkard and Van der Merwe (n 35 above) 24-31, De Villiers (n 1 above) 559 and Swales (n 44 above) 26.

116 See (n 25 above); (n 26 above) & (n 27 above).

117 See Schwikkard and Van der Merwe (n 16 above) 287.

118 See De Villiers (n1 above) 568; Schwikkard and Van der Merwe (n 16 above) 26-27 and Swales (n 44 above) 7.

119 See Schmidt and Rademeyer (n 2 above) 12-3.

120 Zeffert and Paizes (n 103 above) 967.

121 See *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ) where a full bench stated at paragraph 12 that "The "data messages" relied upon in this case are not only real evidence but include hearsay"; See *Ndiki* (n24 above) at paragraph 20 and paragraph 33 where the court concluded that a "data message" can be either real or documentary evidence, depending on its purpose and nature; but then commented further, obiter, that to avoid a difficult distinction between what would constitute hearsay evidence and what real evidence, computer generated evidence should always be treated as hearsay. This obiter statement is not supported and should be avoided to ensure South Africa remains consistent with its common law, and with international best practice – see a sample of the international legal position discussed below in chapter 3 at para 3.6. See also *S v Brown* 2 ( n 47 above) at paragraph 20, where Bozalek J made the following remark: "Given the potential mutability and transient nature of images such as the images in this matter which are generated, stored and transmitted by an electronic device, I consider that they are more appropriately dealt with as documentary evidence rather than "real evidence". I associate myself, furthermore, with the approach followed in the *Ndiki* matter where Van Zyl J expressed the view that the first step in considering the admissibility of documentary evidence is to examine the nature of the evidence in issue in order to determine what kind of evidence one is dealing with and what the requirements for its admissibility are."

122 See the cases of *Ndiki* and *Ndlovu* (n 24 above) and *Brown* (n 46 above) where Bozalek J made this remark: "I agree with the observation of Gautschi AJ in *Ndlovu* case that sec 15(1)(a) does not render a data message admissible without further ado. The provisions of sec 15 certainly do not exclude our common law of evidence. This being the case the admissibility of an electronic communication will depend, to no small extent, on whether it is treated as an object (real evidence) or as a document." Hughes and Stander (n 67 above) 61.

De Villiers refers to a five-stage approach to evaluate whether evidence is documentary or not.[123] In the first stage, one must determine whether a potential exhibit is real- or documentary evidence. In this stage, one looks at whether the object is the evidence or is it the content of that object that is the evidence. The evidence must speak for itself. If the evidence is found to be a document, then the next stage becomes operative. During step two, the so-called purpose test should be utilised to determine whether a document is presented as a physical object or whether the content of the object is evidence. In step three one needs to determine whether the common law of evidence or statutory law applies to the evidence in question. During step four, the evidence must be weighed up against the evidentiary rules applicable to the evidence about admissibility. Only once the evidence is admitted, step five becomes operative, in which the evidence as a whole is evaluated and the weight of the evidence in question is determined.

Once one has established whether the evidence at hand is real- or documentary evidence, one needs to determine whether the evidence is relevant to the facts of a matter. Thereafter, one needs to turn to the common law rules of evidence and the statutory rules of evidence to determine if the information can be adduced as evidence in legal proceedings.[124]

In the event that evidence, including electronic information, is classified as documentary evidence, it must meet the criteria set out in section 34 of the CPEA to be admissible legal proceedings. Section 34 of the CPEA states:

> (1) In any civil proceedings where direct oral evidence of a fact would be admissible, any statement made by a person in a document and tending to establish that fact shall on the production of the original document be admissible as evidence of that fact, provided-
> (a) the person who made the statement either-
> (i) had personal knowledge of the matters dealt with in the statement; or
> (ii) where the document in question is or forms part of a record purporting to be a continuous record, made the statement (in so far as the matters dealt with therein are not within his personal knowledge) in the performance of a duty to record information supplied to him by a person who had or might reasonably have been supposed to have personal knowledge of those matters; and

123 De Villiers (n 1 above) 569.
124 See Swales (n 44 above) 6 and Bouwer (n 17 above) 161 and De Villiers (n 2 above) 724.

(b) the person who made the statement is called as a witness in the proceedings unless he is dead or unfit by reason of his bodily or mental condition to attend as a witness or is outside the Republic, and it is not reasonably practicable to secure his attendance or all reasonable efforts to find him have been made without success.

(2) The person presiding at the proceedings may, if having regard to all the circumstances of the case he is satisfied that undue delay or expense would otherwise be caused, admit such a statement as is referred to in subsection (1) as evidence in those proceedings-

(a) notwithstanding that the person who made the statement is available but is not called as a witness;

(b) notwithstanding that the original document is not produced, if in lieu thereof there is produced a copy of the original document or of the material part thereof proved to be a true copy.

(3) Nothing in this section shall render admissible as evidence any statement made by a person interested at a time when proceedings were pending or anticipated involving a dispute as to any fact which the statement might tend to establish.

(4) A statement in a document shall not for the purposes of this section be deemed to have been made by a person unless the document or the material part thereof was written, made or produced by him with his own hand, or was signed or initialled by him or otherwise recognized by him in writing as one for the accuracy of which he is responsible.

(5) For the purpose of deciding whether or not a statement is admissible as evidence by virtue of the provisions of this section, any reasonable inference may be drawn from the form or contents of the document in which the statement is contained or from any other circumstances, and a certificate of a registered medical practitioner may be acted upon in deciding whether or not a person is fit to attend as a witness.

In the matter of S *v Ndiki* Van Zyl J said:[125]

> [t]hat the definition of a data message in section 1 of the ECTA appears to be sufficiently wide to not only include real evidence but also hearsay evidence in the form of a data message.

In so far as electronic information contained in a "data message" is concerned, it can also be classified as hearsay evidence.[126] Hearsay evidence is defined in section 4 of the LEAA:

> "evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence".

125 See *S v Ndiki* (n 18 above) at paragraph 8.
126 See Swales (n 44 above) 33-67.

If electronic information in the form of a "data message" is classified as hearsay evidence, it needs to pass the requirements in section 3 of the Law of Evidence Amendment Act (hereinafter referred to as the LEAA)[127]:

> (1) Subject to the provisions of any other law, hearsay evidence shall not be admitted as evidence at criminal or civil proceedings, unless-
> (a) each party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings;
> (b) the person upon whose credibility the probative value of such evidence depends, himself testifies at such proceedings; or
> (c) the court, having regard to-
> (i) the nature of the proceedings;
> (ii) the nature of the evidence;
> (iii) the purpose for which the evidence is tendered;
> (iv) the probative value of the evidence;
> (v) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends;
> (vi) any prejudice to a party which the admission of such evidence might entail; and
> vii) any other factor which should in the opinion of the court be taken into account, is of the opinion that such evidence should be admitted in the interests of justice.
> (2) The provisions of subsection (1) shall not render admissible any evidence which is inadmissible on any ground other than that such evidence is hearsay evidence.
> (3) Hearsay evidence may be provisionally admitted in terms of subsection (1) (b) if the court is informed that the person upon whose credibility the probative value of such evidence depends, will himself testify in such proceedings: Provided that if such person does not later testify in such proceedings, the hearsay evidence shall be left out of account unless the hearsay evidence is admitted in terms of paragraph (a) of subsection (1) or is admitted by the court in terms of paragraph (c) of that subsection.

So contrary to section 15 of the ECTA, if the probative value of the evidence, including electronic information, relies on the credibility of a person other than the person giving evidence, that evidence must be evaluated according to the requirements in section 3 of of the LEAA, to determine its admissibility.[128]

---

127 Act 45 of 1988. This Act was assented to on 15 April 1988 and became effective on 3 October 1988. See Zeffert and Paizes (n 103 above) 457 and *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider In re: MTN Service Provider v LA Consortium & Vending CC t/a LA Enterprises* (n 121 above) 12.

128 De Villiers (n 1 above) 567 said that: "this speaks to the accuracy of the document and does not mean that the content of the document is true."

Section 15 of the ECTA deals with the admissibility of data messages as evidence in legal proceedings and states as follows:

> (1)In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message in evidence
> (a) on the mere grounds that it is constituted by a data message; or
> (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
> (2) Information in the form of a data message must be given due evidential weight.
> (3) In assessing the evidential weight of a data message, regard must be had to (a) the reliability of the manner in which the data message was generated, stored (b) the reliability of the manner in which the integrity of the data message was (c) the manner in which its originator *(d)* any other relevant factor.
> (4) A data message made by a person in the ordinary course of business or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law. admissible in evidence against any person and (5) rebuttable proof of the facts contained in such record, copy, printout or extract.

Does this imply that section 15 of the ECTA overrides the provisions of section 3 of the LEAA if the evidence is in the form of a "data message"? Van Zyl J mentioned in the *Ndiki* case, that there is nothing specifically in the ECTA that stipulates that it does not override the provision of section 3 of LEAA. However, in the earlier *Ndlovu* case, Gautschi AJ stated:[129] [t]here is no reason to suppose that section15 (1) seeks to override the normal rules applying to hearsay. In the matter of *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* the court stated[130]:

> "any hearsay contained in a data message must pass the criteria set out in s 3 of the Law of Evidence Amendment Act 45 of 1988."

In the *LA Consortium* case, the court confirmed what was said in the *Ndlovu* case. However, it seems that judicial officers have a wide discretion to admit hearsay evidence and may create a disparity in applying their discretion between jurisdictions. It is of

129 See *Ndlovu v Minister of Correctional Services and Another* (n 24 above) on page 173.
130 See *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* (n 121 above) at paragraph 13.

utmost importance to determine the purpose for which the evidence was created and what it will be used for.[131]

Relevance is one of the first factors that is considered to determine the admissibility of evidence, including electronic evidence but is not the sole test for admissibility.[132] Evidence that is relevant and authentic can be excluded if it is privileged or its admissibility is otherwise restricted by the rules of evidence, such as confidentiality and privilege and the parol evidence rule.[133] Evidence, including electronic information, which is material or relevant, must also be competent to be admissible, i.e., it is not excluded by the evidentiary rules, common law, and statutory prerequisites of admissibility. For example, the testimony of an eyewitness may be material, but it may be inadmissible under marital privilege. Evidence, including electronic information, is relevant if it tends to determine to a reasonable extent the probability or improbability of a fact in dispute. The relevance of evidence, including electronic information, is determined by asserting a logical link to a fact in dispute in a matter. It is therefore advisable that parties define and discuss the relevance of evidence, including electronic information to ensure that it is preserved and later produced in its original form or the best evidence available. This will assist parties to specify grounds for objection in advance in terms of the rules of court or the law.

To determine whether evidence, including electronic evidence, is relevant and admissible can become problematic if that evidence is tendered as hearsay evidence; or as evidence to support the admissibility of other evidence, because there will be competing interests that must be weighed against each other. The current exclusionary rules that are found in common law and statute might be sufficient when considering admitting evidence, including electronic information in the short to medium term, but the exclusionary rules should develop to streamline with the digital age.[134]

131 De Villiers (n 1 above) 567.

132 See Swales (n 44 above) 102. For example, the best evidence rule cannot be applied is there is different version or copies available of the evidence in question. Bozalek J in *S v Brown* (n 47 above) stated as follows: "… the admissibility of an electronic communication will depend, to no small extent, on whether it is treated as an object (real evidence) or as a document."

133 See Zeffert and Paizes (n 103 above) 361-474.

134 See Swales (n 44 above) 117 and SALRC report (n 12 above) 20-29.

Authentication is a pre-condition to allow parties to introduce evidence in legal proceedings.[135] Electronic information can be altered easily[136] and this raises admissibility issues.[137] The Fed.R.Evid contains the evidentiary rules applicable to all forms of evidence that are adduced in legal proceedings in the United States.[138] The Fed.R.Evid provides a safeguard against tampering with evidence, including electronic information to ensure the authenticity and reliability of electronic information when adduced as evidence. Article IX of the Fed.R. Evid governs the authentication of evidence, including electronic information. Courts have a broad authority to determine the admissibility of evidence.[139] Rule 901(a) of the Fed. R Evid under Article IX and reads as follows:

> (a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

Rule 901(a) of the Federal Rules of Civil Procedure sets out the requirements for authentication of electronically stored evidence. Rule 901 of the Fed.R. Evid is silent on the process that one needs to follow to authenticate evidence.[140] It provides examples of how authentication can be achieved.[141] These examples include authentication through processes or systems that require evidence describing the process or system used to produce a result and showing that the process or system

---

135 In *United States v Vayner*, F.3d, 2014 WL 4942227 (2d Cir. Oct. 3, 2014), the court held that: "the court below had abused its discretion in admitting the web page that had been printed off from a Russian social networking site, akin to Facebook, holding that the document had not been properly authenticated under *Federal Rules of Evidence* (US) r 901. The court held there was not a sufficient basis on which to conclude that the printout was what it claimed it to be, that is, Mr Zhyltsou's profile page; therefore, there was insufficient evidence to authenticate the page and permit its consideration by the jury. Although information about Mr Zhyltsou appeared on the web page: his name, photograph, and some details about his life consistent with a witness' testimony about him, there was no evidence that Zhyltsou himself had created the page or was responsible for its contents. Interestingly the court went on to say that 'Had the government sought to introduce, for instance, a flyer found on the street that contained Zhyltsou's Skype address and was purportedly written or authorized by him, the district court surely would have required some evidence that the flyer did, in fact, emanate from Zhyltsou. Otherwise, how could the statements in the flyer be attributed to him?"

136 Cohen and Lender (n 3 above) 6-3.

137 Cohen and Lender (n 3 above) 6-3 and Schwikkard and Van der Merwe (n 35 above) 411.

138 See Fed.R. Evid in the United States.

139 In *United States v Sanders,* (1984) 749 F.2d 195, 197 (5th Cir. 1984).

140 Grimm, Bergstrom and O'Toole-Loureiro "Authentication of social media evidence". *Am. J. Trial Advoc.* 36(3), 433-472.

141 Stanfield "The Authentication of Electronic Evidence" (PhD thesis Queensland University of Technology 2016) 4-5.

produced an accurate result. Rule 901(b) (7) of the Fed.R. Evid deems public records and reports with their metadata stored on servers or computers to be authentic. In terms of this rule, parties do not have to provide any evidence, to show that the computer system producing the public records was reliable or the records accurate.[142] In contrast, Rule 901(b) (9) of the Fed.R. Evid deals with scenarios where the accuracy of the public record or report is dependent upon a computer processor system that produces it.[143] A litigant that adduces evidence must describe the process or system used to produce a result and illustrate that the process or system produces an accurate result.[144]

One needs to bear in mind the Fed.R. Evid was not amended or modified to fit in with technological advances. Judicial officers had to adapt their approach when dealing with electronic information as evidence to meet the requirements of relevance, authenticity, and admissibility in the United States.[145] In addition, the parties need to also discuss issues related to privilege under Fed.R. Evid 502.

Evidence, including electronic information, can only be admitted into evidence if it is shown to be accurate or trustworthy.[146] Contrary, to this, is section 11 of the ECTA that states:

> (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.
>
> (2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.
>
> (3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is (a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and(b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

---

142 See Fed.R. Evid

143 See rule 901 that reads as follows: “Authenticating or Identifying Evidence
(a) IN GENERAL. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.
(b) EXAMPLES. The following are examples only—not a complete list—of evidence that satisfies the requirement-… (9) *Evidence About a Process or System.* Evidence describing a process or system and showing that it produces an accurate result.”

144 Stanfield “The Authentication of Electronic Evidence” (n 141 above) 190.

145 Grimm “Authenticating digital evidence” *GP Solo* 31(5) 47.

146 De Villiers (n 2 above) 725 “genuine and authentic basically speaks to the character and nature of the document and does not touch on the issue whether the content is true or not.” So the accuracy and reliability of the evidence still needs to be considered.

Proper gathering, recording, management, and production of electronic information as evidence can aid the process of authentication and ensure that the integrity and reliability of the evidence, including electronic information, is not compromised.[147] This issue came to the fore, where electronic information was retrieved from mobile devices and later used in legal proceedings.[148]

The authenticity of evidence, including electronic information, can be brought into question in the event the evidence is not validated as what it purports to be.[149] This also applies to a "data message" based on the doctrine of functional equivalence.

As far as the originality of a "data message" is concerned, the ECTA[150] states that a "data message" is seen as original:

> (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if-
> (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2);
> (b) and that information is capable of being displayed or produced to the person to whom it is to be presented.
> (2) For the purposes of subsection 1 (a), the integrity must be assessed-
> (a) 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;
> (b) in the light of the purpose for which the information was generated; and (c) having regard to all other relevant circumstances.

However, section 15 (1) (b) of the ECTA dilutes the common law rule of originality and even go as far as to say that the test for integrity and reliability of "data message" in

147 See Mason, Sheldon and Dries "Proof: the technical collection and examination of electronic evidence" in Mason and Seng *Electronic Evidence* 4th ed 291-330. In *United States v Jackson*, 2007 WL 1381772 (D. Neb. May 8, 2007), an undercover police officer conducting the chat room conversation would cut-and-paste the entire conversation into a word document for later review. A computer forensics expert testified that this cut-and-paste method created several errors and that several portions of the defendant's conversations were omitted. The defendant argued the omitted portions of the transcript contained evidence relating directly to his intent and should not be admitted as evidence. The court found that the cut-and-paste document was not admissible evidence at trial because it was not authentic under the Federal Rules of Evidence.

148 See *Pistorius* (n 28 above) and *S v Brown* (n 47 above).

149 See Theophilopoulos (n 19 above) 467-470.

150 See section 14 of the ECTA.

section 14(2) of the ECTA can be sidestepped if the original "data message" is not produced. This places a bigger emphasis on the fact that courts can no longer exclude electronic information in legal proceedings merely on the basis that it is in a digital form.[151]

Section 15(1) (a) of the ECTA reinforces what is stipulated in section 11 of the ECTA and section 15(1) (b) of the ECTA goes further in that it creates a statutory exception that will allow a "data message" to be admissible without further ado. The exception in section 15(1) (b) will automatically mean if the evidence, including electronic information, is contained in a "data message" and is the best information available, it is exempted from the requirements in section 34 of the CPEA and section 3 of the LEAA irrespective of the fact that a "data message" is the equivalent of traditional paper documents.

Metadata can be used to assist in the process of authentication of evidence, including electronic information.[152] Electronic information is susceptible to intentional or unintentional alteration that cannot be view on the screen of laptops or computers. This may have a severe impact on the accuracy and trustworthiness of the evidence, including electronic information. Metadata can assist litigants to place the best evidence, including electronic information before a court. It can also afford parties the opportunity to test or place circumstantial evidence before a Court, to prove that a person did author a document, or to prove the accuracy of the content of the evidence, including electronic information.[153]

## 2.4 CONCLUSION

151 Hofman and De Jager "South Africa" in Mason *Electronic Evidence* 3rd ed 762 and section 15(1) (a) of the ECTA.
In *Ndlovu v Minister of Correctional Services and Another* (n 24 above), Gautschi J said: "that the ECT Act does not render data messages admissible without further ado. The act prohibits the exclusion from evidence of a data message on the mere grounds that it was generated by a computer and not a natural person." This view was echoed in *CMC Woodworking Machinery v Pieter Odendaal Kitchens* 2012 5 SA 604 (KZD) 2 where the court held that: "changes in the technology of communication have increased exponentially and it is therefore not unreasonable to expect the law to recognise such changes and accommodate it."

152 See Stanfield (n 141 above) 67 and Swales (n 44 above) 163.

153 In the matter of *Liverpool Victoria Insurance Co v Khan* [2016] EWHC 704 (QB) the Court relied on metadata. In casu, there were allegations that the third defendant requested his doctor to amend his initial report to state that his patient would need extensive treatment.

The definition of the term "document" in the CPA and CPEA is too narrow given the technological advancements and should be amended and the broader definition is included in the rules of court.[154] Classification of electronic information as either real- or documentary evidence is important to determine which evidentiary rules apply to the evidence in question.[155] Given the divergence in case law, it is my view that, in the short term, the courts may be able to address the admissibility of electronic information, but in the long-term reform is needed.[156]

The next chapter will discuss the preservation of evidence, including electronic information, concerning the discovery thereof, in the United States, the United Kingdom, and South Africa.

## CHAPTER 3

## PRESERVATION AND RETENTION OF ELECTRONIC INFORMATION

154 See SALRC report ( n 12 above) at paragraph 4.139 81.

155 Fourie "Using Social Media as Evidence in South African Courts" (unpublished LLM Dissertation May 2016) 16 and According to Swales (n 44 above) "there is a further nuance in that electronic evidence can be real and documentary at the same time or, at the very least, exhibit characteristics of both real and documentary evidence." See SALRC Issue Paper ( 59 above).

156 See *S v Brown* (n 47 above) at paragraph 18.

## 3.1 INTRODUCTION

In this chapter, I will discuss procedural and evidentiary issues related to the preservation of evidence, including electronic information. This chapter will focus on the following in regard to the duty to preserve evidence, including electronic information: (i) what is the duty to preserve, when it applies, what must be preserved, and if there are any implications if the duty is not met. This chapter also discusses the challenges posed by electronic information, and how document retention policies and legal hold notices can be used to aid with the collection, preservation, and management of evidence, including electronic information.

Firstly, the duty to preserve evidence, including electronic information, can describe as a duty to prevent that relevant and admissible evidence is not destroyed or altered when legal proceedings are anticipated or pending. Secondly one needs to identify what triggers the duty to preserve relevant and admissible evidence, including electronic information, and take reasonable steps to avoid destruction or tampering. Lastly, for litigants to meet the above duty, a party must identify, locate, preserve, manage, and retain electronic information in its original state that is relevant and admissible to the anticipated or pending legal proceedings.[157] It is important that legal practitioners and their clients preserve all relevant information when legal proceedings are anticipated or foreseeable.

Electronic information is the currency of the digital world and at the core of legal disputes in the modern day. The bulk of the information upon which businesses and persons rely on to function in their day-to-day operations is created and stored in digital form on computer systems, laptops, portable storage devices, backup systems, and cloud servers and is never reduced to paper.[158] One of the pertinent issues surrounding the preservation of evidence, including electronic information that is admissible and relevant, is the collection, retention, and management thereof in its original form. Electronic information must be stored and preserved in such a manner to maintain its veracity and integrity to admit it as evidence later in legal proceedings if the need

---

157 Scheindlin (n 15 above) 28. See https://www.edrm.net for the discussion of preservation of evidence.

158 See De Villiers (n 2 above) 723.

arises.[159]There is no common law duty on parties to retain evidence, including electronic information in South Africa. However, section 16 of the ECTA, the Companies Act[160] and the Income Tax Act[161] create a statutory duty on parties to retain information in its original state and fore a specified period. The obligation to preserve and retain relevant evidence, including electronic information, demands from litigants to identify, locate, collect and manage the evidence, including electronic information under their control but also consider what steps might be appropriate to ensure the preservation of evidence, including electronic information under the control of the opposing party for use in anticipation of legal disputes.[162]

Electronic evidence is usually recycled or destroyed in the ordinary course of business, as a result of corporate document retention and destruction policies or practices.[163] When litigants reasonably anticipate the threat of legal proceedings or there is pending litigation, they have a duty to ensure that relevant and admissible evidence, including electronic information, is preserved by taking reasonable and good faith actions.[164] This duty arises as soon as litigation is reasonably anticipated by a party. Legal practitioners and their clients need to be cognisant of what information needs to be retained and preserved in a readable format for foreseeable or pending litigation.

The flow of evidence, including electronic information, across borders, and the storage thereof on portable devices, cloud servers, and backup systems have given rise to multiple questions about who is in "possession" and "control" of the electronic

159 See Sedona Principles 3, 5 and 6 developed by the Sedona Working Group.
160 See section 15 of ECTA and the regulations of Act 61 of 1973 (as amended).
161 See section 73 of Act 58 of 1972(as amended).
162 Danna "Weathering the Evolving Landscapes of Electronic Discovery" (2017) 29 *Singapore Academy of Law Journal* (*SAcLJ)* 347.
163 See Cohen and Lender (n 3 above) 2-7. Litigants have a duty to ensure that they notify all relevant persons to ensure that potentially relevant electronically stored information in the event litigation is foreseen or pending is not destroyed due to regular computer operations.
164 See Cohen and Lender (n 3 above) 2-8 and Mason" in Mason *Electronic Evidence* 3rd ed (n 3 above) supports the view that the duty to preserve attaches as soon as litigation becomes likely. However, one should be mindful that more and more businesses outsource data management systems to information technology companies and they might not always be aware of any pending litigation or foresee the possibility of a future dispute that their clients face. Lawyers should be alert to this point of practice to ensure that they comply with a discovery request. Legal practitioner has ethical and other responsibilities to ensure that their clients preserve and produce electronically stored information that complies with the applicable requirements. While it is generally sufficient for counsel to furnish advice to clients and rely upon them to meet their obligations, courts have suggested that counsel has independent duties of supervision and, in some cases, of participation in the preservation and production process.

information that is subject to preservation and production during legal proceedings. As a result, thereof, practical problems linked to the preservation and production of electronic information as part of the discovery process have multiplied in situations where a party is not directly in "control" or "possession" of the information.

In the common law jurisdictions that I refer to in this study, guidelines and rules were developed to make provision for the manner in which electronic information is to be recorded, collected, preserved, managed and produced, during pre-trial stages and trials.[165] A group of legal practitioners in the United States took it upon themselves to develop standards for best practices, to address the challenges posed by electronic information, and to assist legal practitioners with the new and unusual challenges brought about by electronic information during the discovery process.[166] These standards and best practices have become known as the Sedona Principles.

This chapter will examine the positions in the United States and the United Kingdom in paragraphs 3.2 -3.3 below. I will also look at how these jurisdictions have amended and or supplemented their respective procedural- and evidentiary rules to deal with the preservation issues that parties faced when seeking discovery of evidence, including electronic information and the practices followed in these jurisdictions to avoid spoliation sanctions. It will be used as a tool to identify a suitable approach for the preservation, retention, and discovery of electronic information in South Africa.

165 See, for example, the EDRM model available at https://www.edrm.net/frameworks-and-standards/edrm-model/ that legal practitioners and judicial officers in the United States and United Kingdom consult as part of the e-discovery process.

166 See https://thesedonaconference.org/publication/The_Sedona_Principles.

## 3.2 PRESERVATION AND RETENTION OF INFORMATION IN THE UNITED STATES OF AMERICA

The duty to preserve relevant evidence, including electronic information in the United States, arises from common law.[167] In the United States, there is a common-law duty to preserve evidence, including electronic information, even before proceedings are commenced.[168] Litigants are obligated to preserve relevant and admissible evidence in their possession, custody, or control. If a party seeks a preservation order, that party must first demonstrate a real danger that the evidence might be destroyed and that there is no other remedy at its disposal to prevent the destruction of the relevant evidence.[169] In the matter of *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities*[170], District Judge Scheindlin said:[171]

> The common law duty to preserve evidence relevant to litigation is well recognized. The case law makes crystal clear that the breach of the duty to preserve . . . may result in the imposition of sanctions by a court because the court has the obligation to ensure that the judicial process is not abused. It is well established that the duty to preserve evidence arises when a party reasonably anticipates litigation. Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a `litigation hold' to ensure the preservation of relevant documents. A plaintiff's duty is more often triggered before litigation commences, in large part because plaintiffs control the timing of litigation.

The common law duty to preserve evidence, including electronic information, is supplemented by statutory powers encapsulated in rules 16(b)(3)(B),[172] rule 26(f)[173],

---

167 See *Silvestri v. General Motors Corp 271 F.3d 583, 591 (4th Cir.2001)* and advisory committee note on rule 37(f) of the Fed.R. Civ.P that states a preservation obligation may arise from many sources including common law statutes regulations or a court order. See also *Kronisch v United States*, 150F. 3d 112, 126-127 (2dCir.1998).

168 See Cohen and Lender (n 3 above) 3-5.

169 See Cohen and Lender (n 3 above) 3-5.

170 See *Pension Committee of University of Montreal Pension Plan v. Banc of Am. Sec*., 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010).

171 See *Pension Committee of University of Montreal Pension Plan v. Banc of Am. Sec*., 685 F. Supp. 2d 456 (n 170 above) at part 2 paragraph B.

172 Since December 2015, the Federal Rules of Civil Procedure Rule permits courts to include in their scheduling orders steps on how litigants must retain and preserve electronically stored information. Attorneys have a duty to notify their clients of the need to preserve electronically stored information. The information to be preserved includes electronically generated information and electronically stored information that would otherwise be deleted by a routine document destruction and retention policy or otherwise deleted in the ordinary course of business. The duty to preserve electronically stored information only requires a party to take reasonable steps to preserve potentially relevant information, which can be achieved through a litigation hold.

173 A judge or magistrate can make any order about any issue in regard to the discovery of electronically stored information at the scheduling conference. Rule 26(f) directs the parties to

and rule 37(f)[174] of the Fed.R.Civ.P.[175] This pre-litigation common law duty to preserve and retain electronic information is derived from the inherent powers of Federal Courts.[176] There is no rule in the Fed.R.Civ.P that deals exclusively with the duty to preserve evidence before litigation is filed, threatened, or reasonably foreseeable unless the duty is assumed or imposed by a statute, regulations, or court order.[177]

The digital explosion and processing of huge quantities of electronic information in the United States led to the development of the Sedona Principles[178] to guide legal practitioners on issues such as preservation, retention, management, and eventual discovery of electronically stored information.[179] The genesis of the Sedona Principles dates back to 2002 and influenced the development of the law governing electronic discovery in the United States.[180]

Principles 1,3,5,6 and 7 of the Sedona Principles specifically make provision for the preservation and retention of electronic information and can aid litigants to meet their preservation obligations.

Principle 1 reads as follows:

---

discuss any issues regarding the preservation of discoverable information during their conference as they develop a discovery plan. When a case involves discovery of electronically stored information, the issues to be addressed during the rule 26(f) conference depend on the nature and extent of the contemplated discovery and the parties' information systems. It may be important for the parties to discuss those systems and, accordingly, important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems. In appropriate cases, identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful.

174 Hedges *Discovery of Electronically Stored Information: Surveying the Legal Landscape* (2007) 86-91.

175 See Fed.R. Civ.P 26(f) (3) (C) stipulate that a discovery plan must include issues about the disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.

176 Koppel "Federal Common Law and the Courts' Regulation of Pre-Litigation Preservation" *Stanford Journal of Complex Litigation* Vol1 (1) 102.

177 See Koppel (n 176 above) 102; Schwerha; Bagby and Esler (n 3 above) 807 and Allman "Rule 37(f) Meets Its Critics: The Justification for A Limited Safe Harbor for ESI" *Nw. J. Tech. & Intell. Prop.* 1 (2006).

178 Sedona Principles, Third Edition: *Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 Sedona Conf. J. 1, 56–59 (2018). This is the project of the Sedona Conference Working Group on Electronic Document Retention and Production (WG1).

179 Sedona Principles, Third Edition: *Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 Sedona Conf. J. 1, 56–59 (2018). This is the project of the Sedona Conference Working Group on Electronic Document Retention and Production (WG1).

180 In this discussion writer will only focus on federal laws as point of reference and not state law.

> Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34, or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.

Principle 3 states:

> Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

Principle 5 states as follows:

> The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.

Principle 6 states:

> Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents.

Principle 7 reads as follows:

> The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.

The Sedona Principles are not law but were developed to aid legal practitioners, magistrates, and judges in federal and state courts to ensure that preservation obligations are met and to create a framework for preservation procedures in the United States. Litigants can assess their preservation duties' and obligations with the aid of the Sedona Principles, and these duties and obligations must be determined on a case-by-case basis.[181] The scope and ambit of parties' duties to preserve and retain electronic information will vary depending upon the fact whether the electronic information, is relevant and admissible in the dispute at hand.[182] The Sedona Principles are used as a yardstick to detect "lackluster" behaviour of legal practitioners and their

---

181 See *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1320 (Fed. Cir. 2011) and Schwerha; Bagby and Esler (n 3 above) 808.

182 See Sedona principles 1,5, 7 and 14.

clients who disregard procedures and processes in managing information systems and document retention policies, to limit the loss of relevant and admissible electronic information due to "routine, good faith" document destruction operations.[183]

Courts in the United States were tasked with the question to determine when the duty to preserve evidence in electronic form is triggered.[184] This lacuna in the federal laws applicable at that time in the United States was first dealt with in the matter of *Silvestri v. General Motors Corp*[185] prior to the development of the Sedona Principles and the 2006 amendments of the Fed.R.Civ.P. In *Silvestri v. General Motors Corp* decision, Circuit Judge Niemeyer stated:[186]

> The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.

In *Zubulake IV* the court dealt with this pre-litigation duty and further developed the test of when the duty to preserve evidence, including electronic information, is triggered.[187] In the *Zubulake IV*, the court set out the parameters that parties can follow to identify when the duty to preserve relevant and admissible evidence, including electronic information, arises.[188] Scheindlin J stated:[189]

> [a]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary. " While a litigant is under no duty to keep or retain every document in its possession … it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

---

183 Normally companies or businesses have automatic systems that delete electronic information and metadata to create space, to store more recent electronic information and metadata.
184 See Zubulake cases (n 79 above).
185 See *Silvestri v. General Motors Corp* (n 167 above) at part 2B.
186 See *Silvestri v. General Motors Corp* (n 167 above) at part 2B.
187 See paragraphs 8-12 of the *Zubulake IV* decision (n 79 above). In the matter of *Fujitsu Ltd. v. Fed. Express Corp.* the Court of Appeals for the Second Circuit echoed the view in *Silvestri* case and stated: [t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."
188 See *Zubulake IV* (n 79 above) on page 217.
189 See *Zubulake IV* (n 79 above) on page 217.

The aforementioned approach of the court is somehow vague in that a party or an anticipated party may argue that they did not anticipate or foresee any future litigation. District Judge Scheindlin also summarised the pre-litigation preservation obligations of parties in legal skirmishes involving electronic information as follows:[190]

> Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.

The court also examined how far that duty stretched to preserve and retain evidence, including electronic information, when litigation is anticipated or pending.[191] Scheindlin J stated:[192]

> What is the scope of the duty to preserve? Must a corporation, upon recognising the threat of litigation preserves every shred of paper, every e-mail or electronic document, and every back-up tape? The answer is clearly, "no". Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation. As a general rule, then, a party need not preserve all back-up tapes even when it reasonably anticipates litigation.

In *Zubulake I,* the court developed standards and guidelines to assist with the preservation and retention of electronic information in anticipation of a lawsuit or when legal proceedings are pending.[193] Challenges related to preservation, retention, and eventual discovery of electronic information were further amplified in the *Zubulake* decisions[194] that set the benchmark on various issues related to the discovery of electronic information in the United States.

---

190 See *Zubulake IV* (n 79 above) on page 218 at Part III (A) 2(iii).

191 See Schwerha; Bagby and Esler (n 3 above) 811. In the *Zubulake I* case the court developed a seven factor test applicable to inaccessible electronic information that can lead to sanctions if information was intentionally destroyed or deleted; See (n 360 above) above for the seven (7) factors that Scheindlin J developed to determine who would bear the cost of discovery.

192 See *Zubulake IV* (n 79 above) on page 217at Part III (A) 2.

193 See *Zubulake IV* (n 79 above) on page 217at Part III (A) 2.

194 In the matter of *Zubulake I* (n 79 above) decision, the Court made reference to a three-step approach in resolving the scope and cost of discovery when electronic information is involved as follows: "First, it is necessary to thoroughly understand the responding party's computer system, both with respect to active and stored data. For data that is kept in an accessible format, the usual rules of discovery apply: the responding party should pay the costs of producing responsive data.

In *Zubulake IV*, the court recognised that there must be some restrictions on the scope and ambit of its scheduling orders to preserve and retain evidence, including electronic information.[195] In this case, the court looked at two related questions: (i) when does the duty to preserve evidence, including electronic information attach? and (ii) what evidence, including electronic information must be preserved?

The first leg of the inquiry remains the same for traditional documents and electronic information, although the need to recognise when the duty arises may be important in light of the nature of electronic documents or information. The second leg of the inquiry is more complex because electronic information contains metadata that might be relevant to the dispute at hand. The duty above to preserve relevant and admissible evidence, including electronic information, requires that the responding party takes reasonable steps to identify and to ensure that the relevant and admissible information is readily available to the requesting party.[196] The *Zubulake IV* decision highlighted the need for legislative reform in regard to the preservation, retention, management, and discovery of electronic information in the United States. Although the Fed.R. Civ.P only becomes operative after legal proceedings are initiated, case law and the Fed.R.Evid supplements the Fed.R.Civ.P in regards to the duty to preserve electronic information when litigation is reasonably anticipated.

---

A court should consider cost-shifting only when electronic data is relatively inaccessible, such as in backup tapes. Second, because the cost-shifting analysis is so fact-intensive, it is necessary to determine what data may be found on the inaccessible media. Requiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases. Third, and finally, in conducting the cost-shifting analysis, the following factors should be considered, weighted more-or-less in the following order:1. The extent to which the request is specifically tailored to discover relevant information;2. The availability of such information from other sources;3. The total cost of production, compared to the amount in controversy;4. The total cost of production, compared to the resources available to each party;5. The relative ability of each party to control costs and its incentive to do so;6. The importance of the issues at stake in the litigation; and 7. The relative benefits to the parties of obtaining the information."

195 See *Zubulake IV* (n 79 above); Advisory committee note to Rule 37(f) of the Fed.R. Civ.P observes that [w]hen a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a litigation hold. The leading case, *Zubulake IV*, is actually part of a series of five (5) rulings handed down over many months related to the same case but addresses nearly the full gamut of issues that arise relating to e-disclosure. In *Zubulake IV* the court held that the duty to preserve electronically stored information attached as soon as plaintiff's supervisors became reasonably aware of the possibility of litigation, rather than when EEOC complaint was filed several months later.

196 See Principle 6 of the Sedona Working Group.

As soon as the duty to preserve evidence, including electronic information, is triggered, legal practitioners and their clients must issue a formal written notice,[197] referred to as "legal hold" or a "litigation hold",[198] to all appropriate persons that are likely to be in "possession" or "control" of relevant and admissible electronic information.[199] The Sedona Conference Working Group define a legal hold as:[200]

> [t]he processes by which an organization seeks to satisfy an obligation to preserve, initially by issuing a communication designed to suspend the normal disposition of records pursuant to a policy or through automated functions of certain systems. The term "legal hold notice" is used when referring to the actual communication.

In the United States of America, the reach of this notice, includes audits, government investigations, or any other such matter that suspends the normal disposition or processing of records.[201] The scope of legal holds or litigation holds is well articulated by Judge Scheindlin's 2003 decision referred to as *Zubulake IV*.[202] Scheindlin J restricted the scope of litigation holds. Scheindlin J stated:[203]

> As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy.

The written notice referred to above needs to address the following aspects:

(i) details of the dispute, dates, and criteria that define relevant and admissible information to be preserved;

(ii) that relevant and admissible electronic information and documentary evidence must be preserved;

---

197 In some instances, the legal hold notice might be ill-advised because it may lead to the deliberate destruction of relevant information. The above notice should: (i)describe the subject matter of the litigation, dates, and other criteria defining the information to be preserved; (ii) include a statement that relevant electronically stored information and paper documents must be preserved; (iii) identify likely locations of relevant information; (iv)provide steps that can be followed for preserving the information as may be appropriate; and (v) convey the significance of the obligation to the relevant recipients.

198 Sedona Conference *Commentary on Legal Holds, Second Edition: The Trigger & The Process* Sedona Conf. J. (2018 )1. The concepts of legal hold and litigation hold is used interchangeably and bears the same meaning in this text.

199 See Principle 5 and 6 of the Sedona Working Group.

200 See the Sedona Conference Glossary, Third Edition: *E-Discovery & Digital Information Management* (2010) Sedona Conf. J.

201 O'Shea et al "*Using legal holds for Discovery"* Wm. Mitchell L. Rev 464.

202 See *Zubulake IV* (n 79 above) on page 218.

203 See *Zubulake IV* (n 79 above) on page 218.

(iii) identify possible locations of relevant and admissible electronic information and documentary evidence;

(iv) set guidelines that can be followed for preserving the information as may be adequate; and

(v) inform relevant parties of the importance to preserve and retain information.[204]

Legal holds are the most common method of assuring the preservation and retention of relevant and admissible evidence, including electronic information when litigation is anticipated or pending.[205] The notice must inform a responding party of the scope or ambit of relevant and admissible evidence, including electronic information, to preserve and retain and the format in which to preserve the information.[206]

It is of paramount importance for the efficacy and efficiency of preservation, retention, and discovery of electronic information that litigants have early discussions to address issues related to the preservation, retention, and production of electronic information to avoid unnecessary delays and sanctions against the responding party.[207]

The 2006 and 2015 amendments to the Fed.R.Civ.P gave more emphasis to early discussions related to the preservation of evidence, including electronic information. Rule 26(f) of the Fed.R.Civ.P [208] requires litigants to meet and confer in regards to issues related to preservation, retention, and discovery of evidence, including electronic information, which parties intend to produce as evidence at trial.[209] Courts may give

---

204 Sedona Conference *Commentary on Legal Holds, Second Edition: The Trigger & The Process* (2010) 11 Sedona Conf. J. 280-284.

205 Sedona Conference Working Group on *Electronic Document Retention and Production*, (2010) 11 Sedona Conf. J. 265 267.

206 See Rule 37(e) of the Fed.R.Civ.P. The legal hold must take cognisance of the Fed.R.Civ.P, specifically Rule 34.

207 See Fed.R.Civ.P. 16(b)(5) and 26(f)(3). This rule requires that litigants to discuss the topic of electronically stored information at the initial meet and confer and draft a discovery plan.

208 At the "meet and confer", meeting the producing party should be prepared to present opposing counsel and the court with a reasonable plan for the preservation and production of relevant electronically stored information. According to Fed.R.Civ.P. 16(b)(5) read with16(b)(6) and best practices in the courts of the United States of America, parties should be prepared to discuss the sources of electronically stored information that have been identified as containing relevant information, as well as the steps that have been taken to search for, retrieve, and produce such information.

209 See Principle 5 of the Sedona Conference Working Group.

specific orders in terms of Rule 16 of the Fed.R.Civ.P in regards to preservation and retention of electronic information.[210]

As the position stands currently in the United States, rule 37(f) of the Fed.R.Civ.P,[211] read together with principle 3 of the Sedona Principles requires litigants to ensure that they take affirmative steps to prevent information systems from causing loss or destruction of discoverable information.[212] This rule is specifically designed to deal with destruction or tampering with evidence, including electronic information. Unlike the United Kingdom, the United States places a statutory duty on parties not to destroy evidence, including electronic evidence, when litigation is anticipated or pending. Fed.R.Civ.P 37(e) states:

> If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may: (A) presume that the lost information was unfavourable to the party; (B) instruct the jury that it may or must presume the information was unfavourable to the party; or (C) dismiss the action or enter a default judgment.

This rule was amended in 2015 to properly examine the culpable behaviour of parties who wilfully destroy evidence, including electronic evidence. This rule was brought in line with the Sedona Principles to ensure best practice in the United States.

The Fed.R.Civ.P in the United States are constantly interpreted by trial courts at pre-trial conferences and scheduling conferences where orders are made in terms of rule 16 of the Fed.R.Civ.P. These orders are published as official interpretations of the of the Fed.R.Civ.P and Federal Rules of Evidence ( hereinafter referred to as Fed.R.Evid).

---

210 See Fed.R.Civ.P. 26(f) (3).

211 See Fed.R.Civ.P. 37(f), which reads as follows: "Failure to Participate in Framing a Discovery Plan. If a party or its attorney fails to participate in good faith in developing and submitting a proposed discovery plan as required by Rule 26(f), the court may, after giving an opportunity to be heard, require that party or attorney to pay to any other party the reasonable expenses, including attorney's fees, caused by the failure."

212 See Principle 3 of the Sedona Conference Working Group and *Zubulake IV* decision where the court found that UBS Warburg failed to preserve backup tapes and various individuals' e-mails between the period that the duty attached and the date the plaintiff filed her complaint.

These decisions have become an enormous body of case law, as well as official commentary to the rules that legal practitioners and judicial officers can consult and refer to during the process of discovery of electronic information.

The duty to preserve evidence was developed through jurisprudence, judicial commentary, and legislative intervention.[213]

Rule 37 of the Fed.R.Civ.P was amended to deal with the uncertainty around sanctions in the event a party fails to preserve relevant evidence, including electronic evidence. However, there are unanswered questions and may lead to over-preservation or loss of relevant and admissible evidence, including electronic information in the United States.[214] For example, there is a disparity in how various circuit courts in the United States interpret what constitutes “possession”, “control”, and “custody”.[215] Further, the amended rule 37 of the Fed.R.Civ.P did not alter state laws in regards to sanctions for spoliation, hence litigants over preserve information to avoid penalties. Rule 37(e) also gives courts discretion as to why and when to impose sanctions, in the event the court finds that a party destroyed or failed to preserve relevant information.

213 See Harvey (n 98 above) 362.
214 See Danna (n 162 above) 347.
215 See Danna (n 162 above) 349.

## 3.3 PRESERVATION AND RETENTION OF ELECTRONIC INFORMATION IN THE UNITED KINGDOM (ENGLAND AND WALES)

Under the common law in the United Kingdom, there is no general duty to preserve and manage evidence, including electronic information that might be produced as evidence in legal disputes between parties.[216] In the matter of *Earles v Barclays Bank* the court stated:[217]

> However, in this jurisdiction as in Australia, there is no duty to preserve documents prior to the commencement of proceedings: British American Tobacco Australia Services Limited v. Cowell [2002] V.S.C.A. 197, a decision approved in this country by Morritt V.C. in Douglas v. Hello [2003] EWHC 55 at [86].

This is contrary to the position in the United States where the duty to preserve evidence, including electronic information, emerges as soon as a party reasonably anticipates litigation.[218] As early as 1968 English courts grappled with the question of when the duty to preserve evidence arose? In the matter of *Rockwell Machine v. EP Barrus*[219] Megarry J made the following remark:[220]

> [i]t seems to me necessary for solicitors to take positive steps to ensure that their clients appreciate at an early stage of the litigation, promptly after writ issued, not only the duty of discovery and its width, but also the importance of not destroying documents which might by possibility have to be disclosed. This burden extends, in my judgment, to taking steps to ensure that in any corporate organisation knowledge of this burden is passed on to any who may be affected by it.

The court took the view that an obligation to preserve and retain relevant evidence arose not earlier than when the legal proceedings are commenced. Although uncertainty exists in the United Kingdom as to when the obligation arises for litigants to preserve and retain potentially relevant evidence, including electronic information, it is the experience and general practice of solicitors practising in the Commercial Court to

---

216 See *Earles v Barclays Bank Plc* [2009] EWHC 2500 (Mercantile); Hibbert *The Electronic Evidence and Disclosure Handbook* ( 2016) 192; Wheater and Raffin (n 2 above) 111 and Burke et al (n 53 above) 160.
217 See *Earles v Barclays Bank Plc* ( n 216 above) at paragraph 28.
218 See *Zubulake IV* (n 79 above).
219 [1968] 1 W.L.R. 693.
220 See *Rockwell Machine v EP Barrus* [1968] 1 W.L.R. 693 on page 694.

advise their clients to preserve documents and electronic information that may be relevant once litigation is contemplated.[221] Paragraph 9 of PD31B stipulates:

> The parties and their legal representatives must also, before the first case management conference, discuss the disclosure of Electronic Documents. In some cases, (for example heavy and complex cases) it may be appropriate to begin discussions before proceedings are commenced.

Prior to supplementing the CPR with the Practice Directions 31A and 31B, there was uncertainty in the United Kingdom as to when the duty arose to preserve, manage and retain evidence, including electronic information and the metadata associated therewith.[222] This gap was bridged by supplementing the CPR with PD31A[223] and later PD31B[224]. Legislative intervention in the form of PD31B provides some guidance as to when the duty to preserve documents is triggered. Paragraph 7 of PD31B states:

> As soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include electronic documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business.

It seems that the wording of paragraph 7 places the duty to preserve evidence, including electronic information, on solicitors and not their clients *per se*.[225] It further complicates the issue as to when the duty arises to preserve evidence, including electronic information, that might be disclosable as evidence in legal proceedings. Similar to the position in the United States, this is a question of fact in each case, and cases must be considered individually.[226]

Upon careful consideration of the wording of paragraph 7 read together with paragraph 9 of PD31B, it becomes apparent that this duty may arise when legal proceedings are probable at best and not yet instituted. This may lead to abuse of process by parties in that the wording of paragraph 7 of PD 31B is open for interpretation. Further, it places

221 See *Goodman v Paxair Services* (2009) 632 F Supp 2d 494.
222 See Hibbert (n 216 above) 192.
223 See rule 31.4 of the CPR.
224 See paragraph 7 of PD 31B.
225 See *Rockwell Machine v. EP Barrus* (n 220 above) 693.
226 Wheater and Raffin (n 2 above) 113.

a duty on the legal practitioners and not clients to ensure that relevant information is preserved and retained in the original form.[227]

The duty articulated in paragraph 7, read together with paragraph 9 of CPR PD31B, is not a new duty but a pre-existing duty that litigants must guard against the deletion or destruction of evidence, including electronic information.[228] Litigants may conduct business as usual if there is no reason to believe that litigation is reasonably contemplated.[229] This may lead to the destruction of documents that parties might need in future to prove their own case. In the event that evidence, including electronic information, was destroyed as a result of routine document destruction policies, it must still appear in the disclosure list as evidence that was formerly under that litigant's "control" or "possession".

In addition to the issue of when the duty to preserve and retain evidence, including electronic information, are the issue of destruction of evidence, including electronic information. According to English common law, there is a duty on litigants not to destroy documents intentionally to pervert the course of justice.[230] The scope of the duty not to destroy evidence, including electronic information, is extended to solicitors, who in turn have a duty to advise their clients on the issue of preservation and retention of evidence, including electronic information, when requested to do so.

Solicitors must thus ensure that clients understand the duty to preserve evidence, including electronic information, and produce the evidence, including electronic information when requested to do so. In *Myers v Elman*[231] Lord Atkin described a solicitor's duty to his client as follows :[232]

> The duty owed to the Court to conduct litigation before it with due propriety is owed by the solicitors for the respective parties whether they be carrying on the profession alone or as a firm. They cannot evade the consequences of a breach of duty by showing that the performance of the particular duty of which breach is alleged was delegated by them [to

227 PD 31B paragraph 7.
228 See Hibbert (n 216 above) 196.
229 Hollander *Documentary Evidence* (2015) 183- 184.
230 See *British American Tobacco Australia Services Ltd v Cowell and McCabe* [2002] VSCA197 and Hibbert (n 216 above) 193.
231 [1940] A.C 282.
232 See *Myers v Elman* ( n 231 above) 302.

> another] …. If the Court is deceived or the litigant is improperly delayed or put to unnecessary expense, the solicitor on the record will be held responsible and will be admonished or visited with such pecuniary penalty as the Court thinks necessary in the circumstances of the cases.

The obligation to preserve evidence, including electronic information, extends to standard disclosure in the United Kingdom.[233] It is the ethical duty of legal practitioners to advise their clients as soon as litigation is contemplated, to preserve all material evidence, including electronic information, and it is associated metadata that might be subject to an order for specific disclosure in legal proceedings.

In the matter of *Alliance & Leicester Building Society v. Ghahremani*, the court held that the intentional destruction of documents by Mr. Chopra that was stored on his computer amounted to contempt of court and he was subsequently fine a thousand pounds. In *Douglas & Ors v Hello! Ltd.& Ors*[234] the court also dealt with the destruction of documents and accepted the principle laid down in *British American Tobacco Australia Services Ltd v Cowell*.[235] In the matter of British *American Tobacco Australia Services Ltd v Cowell* the court made the following observation:[236]

> [w]e turn to the critical question, whether there is any obligation on the defendant, before the commencement of proceedings, not to destroy documents which might well be relevant in future litigation when such litigation can reasonably be anticipated

In the United Kingdom, divergence exists in practice as to document retention policies and the implementation of these policies. Some organisations retain records of all documents generated in electronic form, whereas some organisations have routine document destruction policies in place.[237] There is no provision in the CPR and Practice

---

233 See Danna (n 162 above) 350. See rule 31.6 of the CPR that states that standard disclosure requires a party to disclose only–
(a) the documents on which he relies; and
(b) the documents which –
(i) adversely affect his own case;
(ii) adversely affect another party's case; or
(iii) support another party's case; and
(c) the documents which he is required to disclose by a relevant practice direction.

234 [2003] EWHC 55 (Ch).

235 [2002] V.S.C.A. 197.

236 *British American Tobacco Australia Services Ltd v Cowell* (n 230 above) at paragraph 142.

237 See the comment of Scheindlin J in *Zubulake IV* (n 79 above).

Directions to prevent litigants from routinely destroying information unless there is a statutory duty on parties to preserve and retain certain information.[238] This is based on the old Latin doctrine "omnia praesumuntur contra spoliatem."[239] In the matter of *Douglas v Hello*[240] the Court also dealt with the destruction of documentary evidence and relied on the principle laid down *British American Tobacco Australia Services Ltd v Cowell and McCabe* matters. In *Douglas v Hello,* the court distinguished between evidence destroyed before the institution of legal proceedings, and the destruction of documents after legal proceedings commenced. The court said:[241]

> Part B of the schedule to the application contains the details with regard to the allegations concerning the destruction or disposal of documents. As I have already recorded in paragraph 36 above the details are not in dispute. There is, however a distinction to be drawn between those which were destroyed or disposed of before these proceedings were commenced and those which were destroyed or disposed of thereafter. With regard to the former category it is established in the very recent decision of the Court of Appeal for the State of Victoria in *British American Tobacco Australia Services Ltd v Cowell and McCabe* [2002] VSCA 197 paragraphs 173 and 175 that the criterion for the Court's intervention of the type sought on this application is whether that destruction or disposal amounts to an attempt to pervert the course of justice. There being no English authority on this point I propose to apply that principle, not only because the decision of the Court of Appeal for the State of Victoria is persuasive authority but because I respectfully consider it to be right.

In *Earles v Barclays Bank Plc*[242] the court also dealt with the issue of spoliation of evidence to obstruct a fair trial before the trial commence. Brown J held that evidence must be presented, to demonstrate the culpable behaviour of a spoliating party for a court to make an adverse finding against for spoliation of evidence:[243]

> [t]here would have to be some clear evidence of deliberate spoliation in anticipation of litigation before one could legitimately draw evidential adverse inferences in those circumstances. There is no such evidential basis in this case.

238 See Hibbert (n 216 above) 193 and Hollander (n 229 above) 183-184.
239 This implies that all things are against the despoiler.
240 [2003] EWHC 55 (Ch).
241 See *Douglas & Ors v Hello! Ltd.& Ors* [2003] EWHC 55 (Ch) at paragraph 86.
242 See *Earles v Barclays Bank Plc* ( n 216 above).
243 See *Earles v Barclays Bank Plc* ( n 216 above) at paragraph 28.

In the above matter, the judge set it out in the starkest terms that electronic disclosure forms part of the CPR, and solicitors practicing in the civil courts in the United Kingdom are expected to know the CPR and practice in accordance with the CPR. Brown J stated that failure to do so amounts to gross incompetence and costs consequences can flow from a failure to comply.

Brown J relied on the principle from the *British American Tobacco Australia Services Ltd v Cowell and McCabe* in finding that there is a duty on litigants not to destroy documents. If they fail to meet their preservation obligations, the court has the discretion to sanction a party for destroying evidence. In both matters, the courts seem to suggest that if the destruction of evidence did not prejudice the innocent party or the party who destroyed the evidence did not secure an evidential advantage, the court will not easily sanction the destroying party.

As soon as a disclosure order has been made in the United Kingdom not to destroy documents or delete information held in electronic form, parties must preserve and retain all relevant evidence, including electronic information. A somewhat similar mechanism, albeit a more draconian one, is available to litigants in the United States. This is commonly known as a litigation hold.[244] However, it seems that it is the duty of solicitors in the United Kingdom to send hold notices to their clients or face sanctions if they failed to do so.

[244] See discussion above at paragraph 3.2 and Burke et al (n 53 above) 160. See https://searchstorage.techtarget.com/definition/litigation-hold.

## 3.4 PRESERVATION AND RETENTION OF ELECTRONIC INFORMATION IN SOUTH AFRICA

In South Africa, unlike the United States and the United Kingdom, there is no common law obligation to preserve and retain information in its original form. The ECTA was specifically promulgated to facilitate and regulate the admissibility of electronic communications and transactions in legal proceedings in South Africa.[245] The ECTA is the only statutory instrument that deals with the retention of evidence in the form of "data messages". However, the ECTA does not provide any guidance to three (3) very important questions: (i) when does the duty to preserve evidence, including electronic information arise? ; (ii) what triggers the duty to preserve evidence, including electronic information and (iii) what is the scope of the duty to preserve evidence, including electronic information?

Some statutes set requirements for how certain records must be managed and preserved in the original form.[246] In the event that a statutory duty exists to retain certain records, it can be done electronically if the requirements of section 16 of the Electronic Communications and Transaction Act are met. Section 16 stipulates as follows :

> (1)Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if —
> (a) the information contained in the data message is accessible so as to be usable for subsequent reference;
> (b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
> (c) the origin and destination of that data message and the date and time it was sent or received can be determined.
> 2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Although section 16 of the ECTA makes provision for the retention of information in electronic form, one still needs to keep in mind that the term "document" and a "data

245 See the preamble of the ECTA (n 26 above).
246 See section 15 of Act 61 of 1973 also known as the Companies Act of South Africa as well as section 73A of Act 58 0f 1972 also known as the Income Tax Act in South Africa.

message" are not synonymous in terms of the prevailing legislation mentioned in Chapter 2 of this study. The term "document" is defined in the CPA and CPEA and the definitions in the aforementioned acts are far removed from that of a "data message". Section 17 of the ECTA further complicates the issue by implying that the term "document" and "data message" can be used interchangeably.[247] The ECTA fails to deal with the issues of when the duty to preserve arise, what triggers the duty, and the scope of the duty to preserve.

The Magistrates' Court Rules and the Uniform Rules of Court do not contain a provision for the automatic preservation and retention of evidence, including electronic information, for purposes of discovery in anticipated or pending legal proceedings. [248] The South African procedural framework requires litigants to approach a court to ensure relevant evidence, including electronic information, is not destroyed intentionally or unintentionally.[249] The High Court can order that all routine document destruction policies of a responding party be suspended to ensure that relevant evidence, including electronic information is preserved and made available to a requesting party. This remedy is borrowed from English law. This remedy is commonly referred to as an Anton Pillar order.[250] In the matter of *Viziya Corporation v Collaborit Holdings (Pty) Ltd & Others*[251] Mathopo J stated:[252]

> An Anton Piller order is directed at preserving evidence that would otherwise be lost or destroyed. It is not a form of early discovery, nor is it a mechanism for a plaintiff to ascertain whether it may have a cause of action. The cause of action must already exist and the preserved evidence must be identified.

---

247 See *Viziya Corporation v Collaborit Holdings (Pty) Ltd* and Others SA 173 (SCA).

248 See Hughes (n 2 above) 24 as well as the comments of Hughes in the SALRC report (n 12 above) 81.

249 Litigants can approach court to obtain an order for the preservation of documents and related material or things that is relevant to pending proceedings. This remedy is borrowed from English law. See Taylor "Outdrawn by a USB: The Sheriff and Technology in *Anton Pillar Orders*" (2009) 24 SA *Public Law* 668. An applicant who fears that information might disappear or be destroyed brings this type of application ex parte. For example, where organisations has routine document destruction polices in place.

250 See the matter of *Anton Pillar KG v Manufacturing Processes Ltd* [1976] 1 ALL ER 779 (CA). In casu, the applicant brought an application for the preservation of evidence that was in danger of being destroyed, concealed or removed outside the Court's jurisdiction to defeat the claim. In *Rath v Rees* 2007 (1) SA 99 (C) the Court held that this type of order infringes upon a respondent's rights to privacy. As result of the nature of this remedy, litigants can easily challenge its constitutionality.

251 See *Viziya Corporation v Collaborit Holdings (Pty) Ltd* and Others (n 247 above).

252 See *Viziya Corporation v Collaborit Holdings (*Pty) Ltd and Others ( n 247 above) at paragraph 23.

As a result of the draconian nature of these types of orders, litigants need to be mindful that a court will only grant this type of order under exceptional circumstances.[253]

Parties must approach the High Court for an order that all parties in "possession" or under whose, "control" relevant evidence, including electronic information is kept, to preserve and retain it in its original form.[254] In practice, this might prove to be more problematic because of a lack of guideposts on issues relating to proportionality, search methodologies, and cooperation between parties. This can be aggravated as a result of issues relating to the identification of information, what information must be preserved, the locations of information, methods to search for responsive information, and the form in which information must be produced.

### 3.5 CONCLUSION

Preservation of evidence, including electronic information, is part of modern litigation and has become a common aspect of litigation globally. Although legislative reform in the United States and the United Kingdom is much more advanced, it seems that certain areas of their respective legislation may still need some form of an amendment. In South Africa, the ECTA strives to facilitate e-commerce but failed to take cognisance of the procedural rules and requirements to avoid lackluster preservation and retention of evidence, including electronic information. In South Africa, it seems that relevant evidence, including electronic information, and associated metadata, can easily be destroyed before proceedings are instituted if a requesting party fails to obtain an Anton Pillar order against a responding party. This calls for legislative reform in South Africa in this digital age.

253 *Non-Detonating Solutions (Pty) Ltd v Durie* [2015] ZASCA154.
254 See www.golegal.co.za/anton-piller-evidence-preservation/ accessed 18 May 2020.

# CHAPTER FOUR

## 4. THE IMPACT OF THE BILL OF RIGHTS ON PRIVACY, CONFIDENTIALITY AND PRIVILEGE ARISING DURING THE DISCOVERY OF ELECTRONICALLY GENERATED AND OR ELECTRONICALLY STORED INFORMATION IN PRE-TRIAL STAGES AND TRIAL

### 4.1 INTRODUCTION

This chapter will examine the right to privacy, confidentiality, and privilege in regards to the preservation, management, and discovery of evidence, including electronic information and its metadata. Privilege is no longer seen, merely as an evidentiary rule, but a fundamental right captured in the right to privacy and enshrined in the Bill of Rights.[255] The principle of privilege cannot be considered in isolation but must be considered comprehensively with confidentiality, privacy, and some of the rights enshrined in the Bill of Rights.[256]

No in-depth study will be conducted about ethics, but I will illustrate how attorneys should deal with evidence, including electronic information when legal proceedings are pending or have been commenced. Litigants need to take their ethical duties in the e-discovery process seriously to avoid any prejudicial consequences that might follow.[257] Consideration will also be given to the role of legal practitioners to ensure that information between litigants is accessible and that trials are conducted fairly.[258]

In this era of technology, most information is generated and stored on electronic devices, such as desktops, laptops, hard drives, and various platforms. Technology brings with it the inherent risk that private and confidential information that is generated and stored on digital devices and in applications such as “Dropbox”, “Huawei Cloud”,

255 The Bill of Rights is included in the Constitution, 1996. See section 14 of the CPEA and sections 203, 217 and 219A of the CPA.
256 See Bill of Rights in chapter 2 of the Constitution.
257 Harvey (n 98 above) 182.
258 See section 35 of the Constitution. This is generally applicable to criminal matters.

"MySpace", "ICloud" and "Google Drive" platforms, become known to third parties or adversaries as a result of impropriety or inadvertent disclosure.[259]

The preservation, retention, and management of private and confidential information on digital devices or platforms render the information vulnerable to cyber-hacking or acts of impropriety.[260] For instance, when a person sends an unsecured email, this may cause the information to end up in the wrong hands, and it may even be seen as a form of a waiver of privilege to that information.

In the United States, the American Bar Association's Bar Model Rules (hereinafter referred to as the ABA Rules) were amended to address the issues associated with technology, confidentiality, impropriety, and inadvertent production of electronic information and its metadata. In the United Kingdom, legal practitioners are guided by the Bar Standards Board Handbook (hereinafter referred to as BSB handbook)[261] and the Solicitors Regulation Authority Code of Conduct 2011, (Version 19) (hereinafter referred to as the SRA Code of Conduct).[262]

Prior to the enactment of the South African Constitution, courts did not pay much attention to the manner in which evidence was acquired.[263] The court's approach under common law was that relevant evidence was admissible. Courts did not concern themselves with how it was obtained.[264] Judicial officers had the discretion to exclude otherwise improperly obtained evidence if its prejudicial effect exceeded its probative value.[265] In the matter of *Motor Industry Fund Administrators* Myburgh J made the

---

259 Mupangavanhu "Electronic signatures and non-variation clauses in the modern digital world: The case of South Africa" 2016 SALJ 854; *Diners Club SA (Pty) Ltd v Singh and Another* 2004(SA) 630(D) at 673 and Basdeo (n 11 above) 195.

260 See S v Brown (47 above) and *Harvey v Niland and Others* 2016(2) SA 436 (ECG); The Department of Communications drafted a proposed cybersecurity framework for South Africa in 2010 (Electronic Communications Act 36 of 2005: Notice of intention to make South African national cybersecurity policy' GN 118 *GG* 32963 of 19 February 2010). The introductory section makes mention of the fact that the legal provisions for cybersecurity in South Africa do not adequately address the challenges faced in effectively dealing with cybercrime.

261 See version 19 of the Handbook that was published on 1 October 2017 available at https://www.sra.org.uk/solicitors/handbook/code/content.page.

262 See https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-solicitors/ last accessed on 08 February 2020.

263 See *S v Makhanya* 2002 3 SA 201 (N) and *S v Singh* 2016 2 SACR 443 (SCA).

264 Currie and De Waal *The Bill of Rights Handbook* 6th ed 308.

265 See *Motor Industry Fund Administrators v Janit* 1994 3 SA 56 (W) at paragraph 64A-B.

following observation to emphasise the importance of exercising judicial discretion with regard to tainted evidence:[266]

> Modern technology enables a litigant to obtain access to the most private and confidential discussions of his opponent: his telephones can be tapped, a listening device can be planted in the boardroom (or bedroom) of the opponent, documents can be photostatted, tape recordings of meetings stolen.

In civil matters, if any of the parties resorted to illegal or unconstitutional methods to obtain evidence, such conduct may render that evidence inadmissible.[267] Such evidence may be excluded on the basis that its admission would lead to an unfair trial or bring the administration of justice into disrepute.[268] In the event that the court is confronted with such a scenario, it should also consider the conduct of the party who objects to the admission of the tainted evidence.[269]

Issues related to improperly obtained evidence gained judicial prominence with the advent of the interim Constitution[270] and eventually the Constitution of South Africa.[271] Courts have the discretion to admit evidence including electronic information, obtained through the infringement of certain rights in the Bill of rights. Recently in the *Harvey* matter[272], the court held that section 86(1) of the ECTA was silent on the admissibility of unlawfully intercepted data, therefore the evidence could not automatically be excluded.[273] The admissibility of evidence depends on the discretion of the presiding officer in a specific matter.

In the United States of America, constitutional protection is granted against self-incrimination under the Fifth Amendment.[274]

---

266 See *Motor Industry Fund Administrators v Janit* 1994 3 SA 56 (W) at paragraph 63H.
267 Schwikkard and Van der Merwe ( n 35 above) 128.
268 Section 34 of the Constitution.
269 De Vos "Illegally or unconstitutionally obtained evidence: a South African perspective" TSAR (2011) 268 280.
270 Act No. 200 of 1993 also known as the Interim Constitution of South Africa was the fundamental law from 27 April 1994 until it was superseded by the final constitution on 4 February 1997.
271 De Vos (n 269 above) 268.
272 See *Harvey v Niland and Others* ( n 260 above).
273 See *Harvey v Niland and Others* ( n 260 above).
274 See *Miranda v Arizona* 384 US 438(1966).

The advent of the Constitution changed the landscape of privacy, confidentiality, and privilege.[275] In the *Lotter* case, Bertelsmann J explained why courts must adhere to the Constitution:[276]

> Since the advent of the Constitution, the Court is obliged to uphold its principles and foundational values. The citizen has a right to protection against violation of his or her fundamental rights. As a matter of public policy and in upholding the constitutional rights of the respondents, this Court must set its face against the unwarranted intrusion into the private sphere of individuals. … This Court has the discretion to exclude evidence in civil matters which has been obtained in violation of the Constitution or '… by a criminal act or otherwise improperly

In South Africa, the Bill of Rights protects certain rights that are fundamental to our constitutional dispensation. Parties may approach the Constitutional Court to enforce any of these rights. Section 14 stipulates:[277]

> Everyone has the right to privacy, which includes the right not to have the privacy of his or her communications infringed.

The use and production of electronic information as evidence in legal proceedings must accord with the right to privacy, confidentiality, and privilege. In addition, evidence must also be relevant, authentic, and reliable. Evidence that is relevant and authentic might nevertheless be inadmissible in legal proceedings.[278]

The issue in regard to the admissibility of improperly obtained evidence had surfaced in the pre-constitutional era and continued into the post-constitutional dispensation. As will be shown, a violation of the right to privacy often means that the evidence was unlawfully obtained and should trigger an inquiry as to whether or not to exclude the evidence in question.[279] There seem to be three principles that a court can follow to determine if improperly obtained evidence should be excluded or not:[280]

---

275 See *Lotter v Arlow* 2002 6 SA 60 (T).
276 See *Lotter v Arlow* ( n 275 above) at paragraph 63J-64B.
277 See section 14(d) of the Constitution.
278 Schwikkard (n 35 above) 417.
279 See *S v Brown* (n 47 above) *and S v Pistorius* (n 20 above) where electronic information on accused's phones were adduced as evidence in criminal proceedings.
280 Zeffert DT & Paizes AP *The South Africa Law of Evidence* 2nd ed (2008) 712.

> The reliability principle: This principle places the quest for truth at the center of the fact-finding process and argues that if the improperly obtained evidence is reliable – as it will be in the ordinary course – it should be received since it is not the function of the rules of evidence to deter or to punish impropriety on the part of law enforcement officers. This is not to condone the impropriety; merely to recognise that it is the province of other disciplinary rules or measures.
>
> The disciplinary principle: This principle acknowledges the role of deterrence and punishment as a function of the rules of evidence. It accepts the limitations of other civil measures for addressing the impropriety and places the responsibility on the court hearing the (for the most part) criminal matter to ensure that those guilty of the impropriety do not benefit by having the ensuing evidence received against the accused and that others are deterred from acting in a similar way. It accepts, too, that the courts should not associate themselves or the legal system they serve with misconduct, but should enforce procedural safeguards so that they do not become meaningless.
>
> The protective principle: This principle stresses the need to protect the beneficiary of legally recognised rights against the abuse of those rights by functionaries of the state. It maintains that the exclusion of the tainted evidence is the appropriate way to prevent prejudice or disadvantage being suffered by the holder of that right.

Courts in South Africa should give due consideration to instances where evidence was unconstitutionally obtained.[281] In the matter of *Key v Attorney-General, Cape Provincial Division and Another.*[282] Kriegler J touched on the issue of improperly obtained evidence:[283]

> What the Constitution demands is that the accused be given a fair trial. Ultimately, as was held in Ferreira v Levin, fairness is an issue which has to be decided upon the facts of each case, and the trial judge is the person best placed to take that decision. At times fairness might require that evidence unconstitutionally obtained be excluded. But there will also be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted

281 See *Fedics Group (Pty) Ltd v Matus* 1998(2) SA 617 (C).
282 1996 2 SACR 113 (CC).
283 See *Key v Attorney-General, Cape Provincial Division and Another* (n 282 above) at paragraph 13.

In general, improperly obtained evidence is inadmissible, although it might be relevant.[284] In the *Fedics* case, the applicants were a group of companies that rendered catering services to government entities, such as the defence force. *In casu*, the applicants sought to interdict five of their former employees from unlawfully competing with them in the catering market.

According to the applicants, the respondents, while still in the employ of one of the divisions of the applicants, set up two business entities that directly competed with the applicants in the same market. Applicants obtained information that M intended to hide the information that proved the applicants' claims. The applicant's attorney, accompanied by four other persons involved in the investigation, proceeded to the site where M was doing business and searched her home and office where they found documents to support the applicants' case. Applicants sought to introduce these documents in evidence, and the respondents objected to the admission of this evidence on the basis that it was unlawfully obtained, and violated M's constitutional right to privacy, and that its admission would render the trial unfair. Brand J declined to deal with the issue of trial fairness and preferred to deal with the issue of judicial discretion to exclude illegally or improperly obtained evidence in civil proceedings. The court allowed the applicants to introduce the tainted documents in evidence.[285]

Brand J stated:[286]

> On the one hand, the litigant who seeks to introduce evidence, which was obtained through a deliberate violation of constitutional rights, will have to explain why he could not achieve justice by following the ordinary procedure, including the Anton Piller procedure, available to him. On the other hand, the Court will, in the exercise of its discretion, have regard to the type of evidence, which was in fact obtained. Is it the type of evidence which could never be lawfully obtained and/or introduced without the opponent's co-operation, such as privileged communications, or the recording of a tapped telephone conversation, or is it the type of evidence involved in this case, namely documents and information which the litigant would or should eventually have obtained through lawful means? In the latter case, the Court should, I think, be more inclined to exercise its discretion in favour of the litigant who seeks to introduce the evidence than it would be in the case of the former. It goes without

284 See Hofman and De Jager,(n 151 above) 761; Whitear-Nel "Illegally or unconstitutionally obtained evidence" 2016 SACJ 81 and *S v Masoka* 2015 (2) SACR 268 (ECP).
285 See *Fedics Group (Pty) Ltd v Matus* ( n 281 above) at paragraph 68.
286 See *Fedics Group (Pty) Ltd v Matus* (n 281 above) at paragraph 640C-E.

> saying that the Court will, in any event, have regard to all the other circumstances of the particular case

In essence, the decision was based on two considerations. Brand J referred to the fact that the respondents, who were now objecting to the admission of the improperly obtained evidence, were themselves engaged in unlawful conduct. The court held that the right to a fair trial and the broader concept of the repute of the administration of justice constitute a sound basis in favour of the admissibility of the impugned information.

In the matter of *S v Jwara*[287] the court also dealt with the admissibility of information gathered via the interception and monitoring of cellphone communications in terms of the Interception and Monitoring Prohibition Act 127 of 1992.[288] In this matter, the state failed to obtain the requisite authorisation to monitor and intercept the communications of the accused. The SCA found that the evidence was admissible and had been properly admitted by the court *a quo*. In *casu,* the court said if other investigative tools were employed it would have jeopardised the investigation. The court held that the exercise of the discretion by the court *a quo* was proper and correct and, under the circumstances, to have excluded that evidence would have been detrimental to the administration of justice. The court further held that section 35(5) cannot be used as a shield to exclude evidence that was obtained according to the directions of the Interception and Monitoring Prohibition Act and the admission of the evidence by the court below cannot be impugned. The court held that the monitoring of the telephonic conversations was the only means to investigate criminal offences since the suspects were all members of the SAPS.

In 2016, the issue of unlawfully obtained evidence was again under the spotlight in the matter of *Harvey v Niland and Others* (ECG).[289] *In casu*, Plasket J gave a detailed explanation of the circumstances under which evidence obtained unlawfully may be

---

287 2015(2) SACR 525 (SCA).

288 It should be noted that the Regulation of Interception of Communications and Provision of Communication Related Act 70 of 2002 have since repealed this act.

289 See Harvey v Niland (n 260 above).

allowed in legal proceedings as evidence.[290] Plasket J made the following observation:[291]

> At common law, all relevant evidence which was not rendered inadmissible by an exclusionary rule was admissible in a civil court irrespective of how it was obtained.

In the *Harvey* case, Plasket J allowed the applicant to adduce electronic evidence obtained from the respondent's Facebook communications. The applicant gained access to the Respondents' Facebook communication without his consent or knowledge. *In casu,* the court held that the ECTA is silent on whether evidence including electronic information, obtained in contravention of s 86(1) is admissible or not. The court stated the fact that ECTA, by its silence on the issue, allows for the admission of unlawfully obtained evidence subject to the discretion of the court to exclude evidence that will render the trial unfair. The admissibility of evidence depends on the discretion of the presiding officer in a specific matter. In the Harvey matter similar to the *Fedics* case the court exercised its judicial discretion in weighing up against each other the prejudicial effect to a fair trial against the administration of justice in this matter. The manner in which the courts dealt with the admission of improperly obtained evidence in the *Fedics* and *Harvey* cases indicate consistency in their approach when considering admitting tainted evidence.

The gathering of electronic evidence should be done in a forensically sound manner and with due observance of the Constitution to be admissible in legal proceedings.[292] The collection, preservation, and management of evidence, including electronic information, should be done in a way that preserves the integrity, accuracy, and reliability of the information.[293] If legal practitioners or their clients tamper with original

290 See *Harvey v Niland* (n 260 above) at paragraphs 41-47.

291 See *Harvey v Niland* (n 260 above) at paragraph 38.

292 See McKemmish, "IFIP International Federation for Information Processing" (2008) 285 *Advances in Digital Forensics IV 3* and Schwikkard (n 34 above) 417. The most reliable manner to preserve digital evidence in a forensically sound way is to engage a qualified IT specialist because no one is better equipped to prevent problems or resolve them should they arise. Schwikkard and Van der Merwe (n 35 above) 417. See Bouwer (n 17 above) 156. See *S v Brown* (n 47 above) where information was retrieved from an accused person cellular phone without his consent and presented as evidence.

293 Proper management of electronic evidence will ensure that meaning and interpretation of the electronic evidence has been unaffected by the computer forensic process. To ensure evidence is reliable all errors must be reasonably identified and satisfactorily explained to eliminate possible evidentiary issues in regards to the evidence. Collection of evidence must be transparent so that process can be independently examined and verified.

electronic evidence, this will alter the metadata that attaches to that information, and it may render the information inadmissible in legal proceedings. It becomes the responsibility of the responding party to adduce evidence to prove the integrity, accuracy, reliability, and relevance of evidence if the evidence is called into question by the requesting party.

Legal practitioners must advise their clients on the preservation and management of evidence, including electronic information, regardless of the form or medium on which it is stored.[294] Paper-based discovery differs from the discovery of electronic information in that the latter contains embedded information referred to as metadata.[295]

294 See Cohen and Lender (n 3 above) 1-3; *Format Communications v ITT (United Kingdom) Ltd* [1983] FSR473 CA. This is normally the safest rule of thumb if you have to weigh it up against the undue burden to retrieve the information and potential costs to retrieve the information.

295 See Schafer and Mason (n 13 above) 35; See Cohen and Lender (n 3 above) 2-37; Wheater and Raffin (n 2 above) 41; Smith (n 3 above) 122 138; Burke et al (n 53 above) 156. Metadata can include information such as the history of file, the purported author of the file, the purported dates of creation and revision of the file that the relevant software program attaches to the file, recipients, changes and modification dates, file names, tracking, to whom the file was addressed and the management of an electronic document. In the United Kingdom, the legislature inserted a provision in the rules that deals with metadata. Practice Direction 31B defines metadata as follows: "Metadata' is data about data. In the case of an Electronic Document, metadata is typically embedded information about the document, which is not readily accessible once the Native Electronic Document has been converted into an Electronic Image or paper document. It may include (for example) the date and time of creation or modification of a word-processing file, or the author and the date and time of sending an email. Metadata may be created automatically by a computer system or manually by a user".

## 4.2 PRIVACY, CONFIDENTIALITY AND PRIVILEGE OF ELECTRONIC INFORMATION IN THE DISCOVERY PROCESS

Privilege is a common law principle[296] that attaches to a client and is independent of the legal practitioner in whose "possession" or under whose "control" that information is.[297] Legal practitioners must ensure that they do not disclose a client's privileged information in response to a discovery request.[298] The court set this position out as follows:

> [a]s, by reason of the complexity and difficulty of our law, litigation can only be conducted by professional men, it is absolutely necessary that a man, in order to prosecute his rights or to defend himself from an improper claim, should have recourse to the assistance of professional lawyers, and it being so absolutely necessary, it is equally necessary, to use a vulgar phrase, that he should be able to make a clean breast of it to the gentleman whom he consults with a view to the prosecution of his claim, or the substantiating his defence against the claims of others; that he should be able to place unrestricted and unbounded confidence in the professional agent, and that the communications he so makes to him should be kept secret, unless with his consent (for it is his privilege, and not the privilege of the confidential agent), that he should be enabled properly to conduct his litigation. That is the meaning of the rule.[299]

This right was strengthened with the advent of the Constitution. The principle of privilege was introduced to avoid the abuse of information that was obtained through the process of discovery.[300] Privilege[301] forms part of the substantive law, rather than the procedural

---

296 The Appellate Division recognised the right in *R v Camane* 1925 AD 570 575. See Burke et al (n 53 above) 150.

297 Hofman and De Jager (n 151 above) 783 and Wheater and Raffin (n 2 above) 165.

298 Scheindlin (n 15 above) 391.

299 See *Anderson v Bank of Columbia* (1876) 2 Ch D on page 649.

300 According to Hofman the South African law relating to privilege is founded in common law. He further mentions that communications between attorney and client are privileged under South African law and cannot be used at trial. See George (n 55 above) 288.

301 Theophilopoulos "Electronic documents, encryption, cloud storage and the privilege against selfincrimination"2015 SALJ 596 is of the view that the principle of privilege and confidentiality is intertwined. If a party waives privilege to certain information, confidentiality is lost with it. Lord Hoffman described legal professional privilege as a fundamental human right in *R v Special Commissioner of Income Tax* [2003] 1 A.C. 563.

law.[302] In *Thint (Pty) Ltd v National Director of Public Prosecutions; Zuma v National Director of Public Prosecutions*[303] Langa CJ stated :[304]

> [t}he right to legal professional privilege is a general rule of our common law which states that communications between a legal advisor and his or her client are protected from disclosure, provided that certain requirements are met. The rationale of this right has changed over time. It is now generally accepted that these communications should be protected in order to facilitate the proper functioning of an adversarial system of justice, because it encourages full and frank disclosure between advisors and clients. This, in turn, promotes fairness in litigation.

Privilege can be described as a personal right to refuse to discover relevant and admissible evidence.[305] In the matter of *R v Camane and Others*,[306] Innes CJ analysed the right to self-incrimination:

> Now it is an established principle of our law that no one can be compelled to give evidence incriminating himself. He cannot be forced to do that either before the trial, or during the trial. The principle comes to us through the English law, and its roots go far back in history. Wigmore, in his book on Evidence (vol IV, section 2250)18 traces very accurately the genesis, and indicates the limits of the privilege. And he shows that, however important the doctrine may be, it is necessary to confine it within its proper limits. What the rule forbids is compelling a man to give evidence which incriminates himself. "It is not merely compulsion" says Wigmore (section 2263)19 "that is the kernel of the privilege, but testimonial compulsion." It is important to bear this in mind, because a man may be compelled, when in Court, to do what he would rather not. His features may be of importance, and he may be made to show them; his complexion, his stature,

---

302 The theoretical foundations of the privilege are explored by Paizes (1989) 106 *SALJ* 109–46. Hollander (n 229 above) supports this view at paragraph 12-01. In this respect the judgment of Botha JA in *S v Safatsa* 1988 (1) SA 868 (A) is of seminal significance. See Hoffmann & Zeffertt *Evidence* at 247. See also *Bogoshi v Van Vuuren* 1993 (3) SA 953 (T) at 958H–961G; *Blue Chip Consultants (Pty) Ltd v Shamrock* 2002 (3) SA 231 (W) at 235H–I; *A Company v Commissioner, South African Revenue Service* 2014 (4) SA 549 (WCC) at 552E–553F; *South African Airways Soc v BDFM Publishers (Pty)* (n 309 above) at 576F–582D; Zeffert *Evidence* 640–642; See the Human Rights Act 1998 in the United Kingdom (hereinafter referred to as HRA) read with article 6 of the European Convention on Human Rights (hereinafter referred to as the ECHR). This notion does not, in my view, contradict the dictum by Botha JA in *S v Safatsa* 1988 (1) SA 868 (AD) at 886G in which he expressed agreement with the perspective expressed by Dawson J in Baker v Campbell (1983) 49 ALR 385 that the rule about privilege is not a mere rule of evidence, but rather, by implication, a substantive law rule. The central idea is that it is a rule which underpins the legal system and is not merely a procedural aid.

303 2009 (1) SA 1 (CC).

304 See *Thint (Pty) Ltd v National Director of Public Prosecutions; Zuma v National Director of Public Prosecutions* ( n 303 above) at paragraph 78E–F.

305 Van Loggenberg *Commentary on the Magistrates' Court Rules* Vol. 2 10th edition; Schwikkard and Van der Merwe (n 35 above) 124. This is also encapsulated in rule 23(2)(a)(ii) of the Magistrate Court Rules and rule 35(2)(b) of the Uniform Rules of Court.

306 1925 AD 570.

> mutilations, or marks on his body, may be relevant points, and he may be compelled to show them to the Court. That is what Wigmore calls autoptic evidence (vol II, section 1150)20 which is perceived by the Court itself, and which it has a right to see. In such cases the man is really passive. But he cannot be forced to go further and to give evidence against himself.

In a 1941 Appellate Division in the case of *Ex parte Minister of Justice: In re R v Matemba*[307] Watermeyer JA, revisited this issue of privilege against self-incrimination and made the following remark:[308]

> It follows that the production of documents or chattels by a person (whether ordinary witness or party witness) in response to a subpoena, or to a motion to order production, or to other form of process treating him as a witness (*i.e.* as a person appearing before the tribunal to furnish testimony on his moral responsibility for truth telling), may be refused under the protection of the privilege; and this is universally conceded. For though the disclosure thus sought be not oral in form, and though the documents or chattels be already in existence and not desired to be first written and created by a testimonial act or utterance of the person in response to the process, still no line can be drawn short of any process which treats him as a witness; because in virtue of it he would be at any time liable to make oath to the identity or authenticity or origin of the articles produced.

By contrast, in *South African Airways Soc v BDFM Publishers (Pty) Ltd*[309] the court held that that the mere fact that information is private and confidential does not mean it cannot be introduced as evidence. Sutherland J stated:[310]

> [t]he 'privilege' cannot reside in the information anyway, because it only becomes the subject matter of the claim of privilege *when that right not to disclose it is claimed, and not before*. At most, the information *per se*, can never be more than *eligible* to be the subject matter of legal advice privilege; ie, if it satisfies the test of being (1) legal advice, (2) given by a legal advisor (3) in confidence to a client and (4) is claimed.16 If privilege is not claimed the information about the legal advice can be adduced in legal proceedings because then, to use the shorthand, it is not 'privileged

To locate, identify and protect privileged documents, including electronic information, an exposition of the law of privilege is required.[311] In this instance we need to be specific

307 1941 AD 75 1 35.
308 See *Ex parte Minister of Justice: In re R v Matemba* 1941 AD 75 1 35 on page 82.
309 2016 (2) SA 561 (GJ).
310 See *South African Airways Soc v BDFM Publishers* (n 309 above) at paragraph 46.3.
311 See Hibbert (n 216 above) 363.

what documents, including electronic information, may be seen as privileged and how one avoids waiving that privilege that attaches to specific evidence, including electronic information? Litigants must avoid practices of abusing the claim of privilege for evidence, including electronic information that is not privileged, or erroneously waiving privilege that attaches to evidence, including electronic information.[312] Litigants, who receive a notice to discover evidence, including electronic information, may object to producing information that they deem to be protected by privilege.[313] However, litigants must be cognisant that abuse of the right to claim privilege will not be entertained lightly by courts. In the matter of *Midi Television v Director of Public Prosecutions (Western Cape)* Nugent JA stated:[314]

> [t]hat there must be a "demonstrable and substantial … real risk that prejudice will occur. … Mere conjecture and speculation that prejudice might occur will not be enough".

Nugent JA's comments illustrate that claims of potential harm or prejudice by responding parties if disclosure occurs would be thoroughly evaluated by courts.

The overarching principles that underlie privilege are similar worldwide, and therefore I will not distinguish between different jurisdictions.[315] The protection of personal interests of persons or the public is at the core of the principle of privilege.[316]

The principle of privilege brings with it the right to privacy and confidentiality that attach to certain information.[317] In the United States and the United Kingdom, litigants also enjoy some protection when the information was disclosed in error or information becomes known to adversaries by impropriety.[318] However, in the South African common law, no rule forbids the use of evidence disclosed in error. It seems that if the evidence is inadvertently disclosed or made available to third parties, confidentiality is

---

312 The Sedona Conference *"Commentary on Protection of Privileged ESI"* The Sedona Conference Journal (2016) Vol 17 108-109.
313 For example, rule 35 of Uniform Rules of Court and rule 23 of the Magistrates' Court Rules in South Africa.
314 See *Midi Television v Director of Public Prosecutions (Western Cape)* 2007 5 SA 540 (SCA) at paragraphs 16-17.
315 See Van Heerden (n 24 above) 32.
316 Du Toit et al *Commentary on the Criminal Procedure Act* Juta (2015) Volume II, 23-48.
317 Theophilopoulos (n 301 above) 596.
318 See Rule 26(b) (2) (5) of the Fed.R.Civ.P.

lost. In *SABC v Avusa*[319] Willis J dealt with a demand by the SABC to return to it a confidential document revealing various irregularities that had fallen into the hands of the *Sunday Times*. The court affirmed a right to the protection of a person's confidential information, distinguishing it from privacy rights. Willis J remarked that:[320]

> …. [c]onfidentiality was lost when the copy of the report was handed over to the Sunday Times, and handing it back will not restore the confidentiality which has been lost'. The absence of any duty of confidentiality by the reporters of the Sunday Times to the SABC, unlike the duties of persons who stood in some form of relationship to the SABC from which such a duty could derive, like employees, meant that possession and dissemination of the information by the newspaper could not attract a liability to desist.

In *South African Airways Soc v BDFM Publishers (Pty) Ltd*, the court explained the operation and effect of confidentiality:[321]

> But if the confidentiality is lost, and the world comes to know of the information, there is no remedy in law to restrain publication by strangers who learn of it. This is because what the law gives to the client is a 'privilege' to refuse to disclose, not a right to suppress publication if the confidentiality is breached. A client must take steps to secure the confidentiality, and if these steps prove ineffective, the quality or attribute of confidentiality in the legal advice is dissipated. The concept of legal advice privilege does not exist to secure confidentiality against misappropriation; it exists solely to legitimise a client in proceedings refusing to divulge the subject matter of communications with a legal advisor, received in confidence. This vulnerability to loss of the confidentiality of the information over which a claim of privilege can and is made flows from the nature of the right itself. The proposition about the consequences of loss of confidentiality is endorsed by the authorities.

A court may draw an inference that the producing party waived privilege to that evidence, including electronic information, that became public as a result of an error or impropriety.[322] However, in South Africa, various statutes operate contrary to this general principle.[323] The possibility that third parties can gain access to a person's

---

319 2010 (1) SA 280 (GSJ).
320 See *SABC v Avusa* ( n 219 above) at paragraph 26.
321 See *South African Airways Soc v BDFM Publishers (Pty) Ltd* (n 309 above) at paragraph 49.
322 Hofman and De Jager "(n 151 above) 783.
323 Section 19 of the Legal Aid Act, 39 of 2014 that reads as follows:
(1) A private legal practitioner who has been instructed by Legal Aid South Africa, to represent a person who qualifies for legal aid under this Act must, when requested by Legal Aid South Africa, grant access to the information and documents contained in the file relating to the person

private and confidential information without that person's consent or knowledge in this digital revolution is a real threat and an inherent risk of the digital paradigm we find ourselves in.[324]

As mentioned earlier in this text, privilege is a personal right and can be categorised into two (2) broad categories namely: legal advice privilege and litigation privilege.[325]

Legal professional privilege is limited to evidence, including electronic information that is private and confidential. However, if information that would otherwise be privileged is known to one's adversaries or in the hands of third parties, legal professional privilege will be lost. Legal professional privilege affords a litigant the right to refuse to disclose certain information, but it does not allow a litigant to suppress information.[326]

The rise of e-commerce and electronic communication gave rise to large volumes of electronic information, which are the subject of e-discovery requests in legal proceedings. The volumes of electronic information have skyrocketed and made producing parties' ability to review electronic information for privilege and confidentiality more complex.[327] Parties must be extra vigilant during the review process to identify privileged information and exclude it from the information that will be produced for inspection.[328]

---

in question for the sole purpose of conducting a quality assessment of the work done by the legal practitioner.

(2) The information and documents referred to in subsection (1) remain privileged information against any other party as information between attorney and client, despite having been made available to Legal Aid South Africa.

324 See *Brown* (n 46 above); *Diners Club SA (Pty) Ltd v Singh and Another* 2004 (3) SA 630(D), *Harvey v Niland*( n 260 above) and Hofman and De Jager (n 151 above) 783.

325 Hollander (n 229 above) 215; Wheater and Raffin (n 2 above) 165 and Zeffert and Paizes (n 103 above) 625 – 671 furnishes an historical account of the conceptualisation of legal professional privilege.

326 See *South African Airways Soc v BDFM Publishers (Pty) Ltd* (n 309 above) at paragraph 49.

327 Scheindlin (n 15 above) 391.

328 This myriad of information creates the possibility that errors is inevitable and it may happen that privileged documents will sometimes be produced inadvertently.

### 4.2.1 UNITED STATES

In the United States, rule 501 of the Fed.R. Evid. stipulates that privilege is governed by common law:[329]

> The common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of the following provides otherwise: the United States Constitution; a federal statute; or rules prescribed by the Supreme Court. But in a civil case, state law governs privilege regarding a claim or defense for which state law supplies the rule of decision.

However, in civil state cases, state law governs privilege, regarding a claim or defence for which state law supplies the rule of decision.

The sheer volume of electronic information that is at the core of e-discovery requests in the United States, has often led to privileged information being disclosed in error. This has necessitated intervention from courts.[330] The legislature also introduced legislative reforms to address the shortcomings of the Fed.R.Civ.P.[331] In addition, the Fed.R.Evid supplements the Fed.R.Civ.P in the United States in instances where evidence including electronic information, is disclosed in error.[332] Rule 26(1) (b) (5) (A) of the Fed.R. Civ.P set out the procedure a litigant must follow to claim privilege:

> Claiming Privilege or Protecting Trial-Preparation Materials.
> (A) Information Withheld. When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must:
> (i) expressly make the claim; and
> (ii) describe the nature of the documents, communications, or tangible things not produced or disclosed— and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.

329 See Rule 501 of the Fed.R.Evid in USA.
330 Fed.R.Evid 502 was enacted to regulate and facilitate the issues of waiver where electronically stored information was disclosed inadvertently.
331 See Rule 26(b)(5)(A) of the Fed.R.Civ.P.
332 See Rule 502(b) of the Fed.R.Evid.

Inadvertent disclosure of privileged information, during the electronic discovery process, is a difficult and sometimes unavoidable question, as a result of the voluminous nature of electronic information.[333] In instances, where information is disclosed in error, Rule 26(b)(1)(5)(B) afford litigants the opportunity to remedy discovery mistakes, to request the return of information disclosed in error:[334]

> Information Produced. If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.

Rule 26(1)(b)(5)(B) and Rule 26(f)(3)(D) of the Fed.R.Civ.P. guides litigants on the procedure to follow to bar adversaries and third parties from using and disseminating information disclosed in error in the United States.

This is aggravated by the amount of time and cost required to screen these large quantities of electronic information for legal professional privilege and other related privileges.[335] As a starting point, one needs to be well versed in the law and procedure in regards to privilege when evidence including electronic information, is inadvertently disclosed, and how one can plan and strategically draft non-waiver agreements to counter inadvertent disclosure.[336] The courts[337] in the United States have also developed a five-factor test to determine whether privilege is waived:

(1) the reasonableness of the precautions taken to prevent inadvertent disclosure in light of the extent of document production;
(2) the number of inadvertent disclosures;

---

333 In some civil disputes, the sheer volume of relevant electronically stored information increases the possibility that a large volume of privileged information may be included among that information.
334 See Rule 26(b)(5)(B) of the Fed.R.Civ.P.
335 See Schwerha; Bagby and Esler (n 3 above) 812.
336 Hibbert (n 216 above) 363.
337 See *Hydraflow, Inc. v. Enidine, Inc.*, 145 F.R.D. 626, 637 (W.D.N.Y. 1993) and *Int'l Brominated Solvents Ass'n v. American Conference of Governmental Indus. Hygienists, Inc.*, No. 5:04-cv-394, 2007 U.S. Dist. LEXIS 47430.

(3) the extent of the disclosures;
(4) the promptness of measures taken to remedy the problem; and
(5) whether justice is served by relieving the party of its error.

Congress amended[338] the Fed.R.Civ.P. to address and eliminate the risks associated with the discovery of electronic information disclosed in error. Specific provisions were inserted into Fed.R.Civ.P.,[339] and the Fed.R. Evid,[340] to ensure that the fundamental rights of persons were protected during legal proceedings.[341]

Rule 26(f)(1) of the Fed.R. Civ.P requires the parties to confer before the pre-trial conference about e-discovery issues and include it in a discovery plan.[342] Parties may conclude an agreement to provide for the preservation and disclosure of evidence including electronic information. Parties must confer on the issue of retrieving privileged information that is disclosed in error.[343]

If privilege is not claimed, the information on which the legal advice is based can be adduced in legal proceedings because it is not protected by the holder's claim. If information is disclosed in error that contains the same subject matter as privileged information, it may be seen as a waiver of privilege. However, this position cannot be accurate. Rule 502(a) of the Fed.R.Evid establish a rebuttable position in regards to subject matter waiver of undisclosed information:

> When the disclosure is made in a federal proceeding or to a federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a federal or state proceeding only if: (1) the waiver is intentional; (2) the disclosed and undisclosed communications or information concern the same subject matter; and (3) they ought in fairness to be considered together.

338 The Fed.R.Civ.P was amended on 01 December 2017 and the F.R.E was amended in October 2010 to include provisions dealing with inadvertent disclosure.
339 See Rule 26(b)(5)(B) in Chapter 2 above.
340 See F.R.E 502(b) that reads as follows:
(b) Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:
(1) the disclosure is inadvertent;
(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).
341 See Fed.R.Civ.P. 26(b)(5)(B) deals with information that is subject to privilege or some protection.
342 Scheindlin (n 15 above) 108-110.
343 Scheindlin (n 15 above) 105 and 397.

On the other hand, Rule 502(b) of the Fed.R.Evid states that information that was disclosed in error in federal proceedings or to a federal office or agency do not constitute waiver:[344]

> When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:
> (1) the disclosure is inadvertent;
> (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
> (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26 (b)(5)(B).

Parties may enter into clawback agreements to retrieve privileged information that was disclosed in error.[345] Agreements may be made an order of court:

> A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.

A clawback is an agreement that the attorney-client privilege and work-product protection are not waived by disclosure. However, clawback agreements are not a solution for all difficult issues that emanate from inadvertent disclosure.[346] The most standard agreement between the parties is that the other side will return any inadvertently disclosed documents. Rule 16(b) specifically permits courts to include provisions in scheduling orders regarding clawback agreements.

Nevertheless, in instances where a party discloses information in a different matter that is unrelated, to the first matter where a Rule 502(d) order was entered, constitutes a waiver of privilege.[347] One needs to be cognisant of the fact that these agreements are binding between parties to the agreement but unenforceable against nonparties.

344 See Rule 26(b)(5)(B) of the Fed.R.Civ.P.
345 Scheindlin (n 15 above) 105.
346 See Hibbert (n 216 above) 369.
347 Scheindlin (n 15 above) 396-397.

### 4.2.2 UNITED KINGDOM

In the United Kingdom, privilege is recognised as a substantive legal right of the client at common law and protected in the CPR.[348] This affords protection to a client's private and confidential information under the following circumstances:

(i) between a lawyer and his or her client;

(ii) where the lawyer is acting within the course of their professional relationship and the scope of his or her professional duties; and

(iii) for the dominant purposes of seeking or giving legal advice and assistance in a relevant legal context.

Privacy has been transposed into the domestic law of England and Wales under the European Convention on Human Rights (hereinafter called ECHR);[349] by the Human Rights Act 1998,[350] Data Protection Act 1998, and the General Data Protection Regulation (hereinafter referred to as the GDPR) that replaced the EC Data Protection Directive. The European Union Parliament approved the GDPR on 14 April 2016 and regulates the flow of personal data around the European Union.[351] Although the ECHR and the GDPR are seen as non-state law, are widely accepted in the European Union and followed in the United Kingdom.

The CPR affords a party the right or duty to withhold privileged documents[352] and sets out the procedure to object to disclosing evidence including electronic information, from inspection by an opponent in litigation or by the court.[353] In practice, privileged documents are mentioned in lists of relevant documents exchanged between the

348 Hibbert (n 216 above) 352.

349 See articles 8 and 10 of the ECHR available at https://www.echr.coe.int/Documents/Convention_ENG.pdf accessed on 18 July 2018.

350 The European Convention on Human Rights incorporates privilege into domestic English law by the Human Rights Act 1998. See http://www.wipo.int/wipolex/en/text.jsp?file_id=313007 accessed on 16 July 2018.

351 The General Data Protection Regulation (GDPR) was published in the Official Journal of the European Union (OJEU) on 4 May 2016. Its provisions are directly applicable and fully enforceable in European Union (EU) Member States (Member States) from 25 May 2018. Any person or organisation that handles personal data must comply with these core principles. Due to the extended territorial scope and a wider definition of personal data, more organisations will be subject to European data protection regulation than before. Territorial scope is addressed in Article 3 of the GDPR, which extends the reach of the European Economic Area (EEA) data protection regime.

352 See Rule 13.3(b) of the CPR.

353 See Rule 13.19 of the CPR.

parties, subject to a claim of confidentiality and right to withhold the privileged documents.[354]

Rule 31.10(4) (a) read in conjunction with Rule 31.19 set out the procedure a litigant must follow, to claim privilege to information.[355] This is not an application to the court. However, a party may approach the court to decide if the claim made under Rule 31.19(1) of the CPR is sound in law:

> A party may apply to the court to decide whether a claim made under paragraph (3) should be upheld.

The courts in the United Kingdom will allow litigants to use and adduce evidence that was disclosed in error.[356] CPR rule 31.20 states:

> Where a party inadvertently allows a privileged document to be inspected, the party who has inspected the document may use it or its contents only with the permission of the court.

A party who disclosed the evidence in error must seek injunctive relief from the court to prohibit the use of that evidence, including electronic information.[357] It seems as if this allowance gives the requesting party an unexpected and unfair advantage over its

354 Usually parties will not need to detail every document covered by privilege individually, but it is helpful to indicate the nature or classes of documents over which privilege is claimed and the factual basis of the grounds giving rise to privilege.

355 See Hibbert (n 216 above) 201 and Wheater and Raffin (n 2 above) 68.

356 See *Rawlinson and Hunter Trustees S.A. & Ors v Director of the Serious Fraud Office* [2014] EWCA Civ 1129 at paragraph 15.

357 See *Rawlinson and Hunter Trustees S.A. & Ors v Director of the Serious Fraud Office* (n 356 above) at paragraph 15.

adversary. However, it seems that CPR rule 31.20, article 6[358] , and article 8[359] of the ECHR[360] are in contrast to each other on the issue of inadvertent disclosure of evidence, including electronic information. In the matter of *Rawlinson and Hunter Trustees S.A. & Ors v Director of the Serious Fraud Office (No 2)*,[361] the court alluded to this contrast in its judgment on information disclosed in error:[362]

> Although discovery is an inherently intrusive process, it is not intended that it be allowed to affect a person's entitlement to maintain the confidentiality of documents where the law allows. It follows that where a privileged document is inadvertently disclosed, the court should ordinarily permit the correction of that mistake and then order the return of the document, if the party receiving the document refuses to do so.

The manner, in which CPR rule 31.20 is worded, requires litigants to enter into clawback agreements because nowadays all discovery in the United Kingdom is in electronic form.[363] The inherent risks associated with e-discovery in the United Kingdom require litigants to enter into pre-Case Management Conference (hereinafter referred to as the CMC) negotiations, to conclude clawback agreements that specifically deal with the discovery of evidence, including electronic information before the first CMC.[364]

---

358 In the determination of civil rights and obligations or of any criminal charge against a person, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly, but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice. 2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law. 3. Everyone charged with a criminal offence has the following minimum rights: (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him; (b) to have adequate time and facilities for the preparation of his defence; (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require; (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him; (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

359 Right to respect for private and family life 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

360 Although the ECHR is non state law instrument, this convention is an instrument which is binding on member states of the European Union (hereinafter referred to as the EU).

361 [2014] EWCA Civ 1129.

362 See *Rawlinson and Hunter Trustees S.A. & Ors v Director of the Serious Fraud Office* (n 356 above) at paragraph 50.

363 See Hollander (n 229 above) 155.

364 See CPR PD31B paragraph 9.

The adverse effect of CPR rule 31.20 and the frequent occurrence of inadvertent disclosure in the United Kingdom requires that litigants draft clawback agreements with ingenuity and innovation, to counter discovery mistakes. The clawback agreements must specify how adversaries need to act when privileged information is disclosed in error.[365] Barristers and solicitors in the United Kingdom can also draw from the BSB handbook as well as the SRA Code of Conduct, to guide them in situations where evidence, including electronic information, was inadvertently discovered in the e-discovery process. Barristers have a duty, stipulated in Rule C5, Rule C15.5, and Core Duty 6 of the BSB Handbook that requires them to preserve the privacy and confidentiality of their clients' information. Similarly, solicitor's duties are set out in Chapter 4, SRA Code of Conduct 2011(Version 19) that protects private and confidential information of their clients. A solicitor's duty is extended even after the mandate is terminated to keep the client's information private and confidential. All members of the lawyer's staff, including support staff, owe the duty. The information must be kept private and confidential unless the law requires disclosure, or the client consents thereto.

365 See Hibbert (n 216 above) 368.

### 4.2.3 SOUTH AFRICA

South African courts have adopted the English practice that a document is privileged, and need not be discovered, if it is part of the evidence that supports the case of the party in whose possession the document is, or if it does not support his adversary's case, or if it contains nothing that makes the holder's case suspicious.[366]

The rules of confidentiality and privacy underlie privilege and must be developed to take cognisance of the growing electronic world.[367] Privileged evidence, including electronic information, which has been inadvertently produced is another issue with particular resonance in electronic discovery. Legal practitioners must ensure that they have a good understanding of their clients' computer operations from the outset of litigation.[368]

The Magistrate Court Rules[369] and the Uniform Rules of Court[370] make provision for litigants to request that evidence be discovered and produced. In the matter of Independent *Newspapers (Pty) Ltd v Minister for Intelligence Services: In re Masethla v President of the Republic of South Africa* the court held:[371]

> Ordinarily courts would look favourably on a claim of litigants to gain access to documents or other information reasonably required to assert or protect a threatened right or to advance a cause of action. This is so because courts take seriously the valid interest of a litigant to be placed in a position to present its case fully during the course of litigation.

A producing party is entitled to object to producing and making available for inspection certain information that is private and confidential on the ground of privilege[372] in terms of rule 35 of Uniform Rules[373] and rule 23 of the Magistrates' Court Rules.[374] However, the producing party needs to raise an objection and must demonstrate that the

366 In other words, the party that calls for disclosure is not entitled to see documents that do not help or harm his case of the disclosing party is it is not relevant to the issues in dispute. A document is not privileged if it was obtained for another goal and not for legal advice.
367 See Theophilopoulos (n 19 above) 477.
368 See Theophilopoulos (n 19 above) 477.
369 See Rule 23(1) of the Magistrates' Court Rules.
370 See Rule 35(1) of the Uniform Rules of Court.
371 See *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services: In re Masethla v President of the Republic of South Africa* [2008] ZACC 6 at paragraph 25.
372 Hollander (n 229 above) 201.
373 See Rule 35(2)(b) of the Uniform Rules of Court.
374 See Rule 23(2(a)(ii) of the Magistrates Court Rules.

documents or their contents are exempted from production and discovery. The holder of this right must exercise his or her right in claiming privilege.[375] In *Thint (Pty) Ltd v National Director of Public Prosecutions and Others* Langa CJ (as he was known at the time) stated:[376]

> Accordingly, privileged materials may not be admitted as evidence without consent. Nor may they be seized under a search warrant. They need not be disclosed during the discovery process. The person in whom the right vests may not be obliged to testify about the content of the privileged material. It should, however, be emphasised that the common-law right to legal professional privilege must be claimed by the right-holder or by the right-holder's legal representative.

The abovementioned view in the *Thint* case is the default position in South Africa regardless of whether the information is electronic or traditional documents.[377] This implies that the holder making a claim thereto triggers privilege.

In South Africa, multiple statutes deal with issues such as privacy and confidentiality that relates to privilege.[378] For example, the Promotion of Access to Information Act, Act 2 of 2000 (hereinafter referred to as PAIA) was enacted to regulate the right of access to information,[379] held by the State and any information held by a third party, that is required for the exercise or protection of any rights, and to provide for matters incidental to it. This applies to records of public and private bodies, regardless of when the records came into existence.[380] In instances, where individuals or organisations

---

375 See *South African Airways Soc v BDFM Publishers (Pty) Ltd* (n 309 above) at paragraph 46.

376 See *Thint (Pty) Ltd v National Director of Public Prosecutions and Others* (n 303 above) at paragraph 185.

377 See *Thint (Pty) Ltd v National Director of Public Prosecutions* ( n 303 above ) at paragraphs 183-185.

378 For example, the Constitution, the Promotion of Access to Information Act, Act 2 of 2000 (hereinafter referred to as PAIA), the Protection of Personal Information Act, (hereinafter referred to as POPIA) and the Regulation of Interception of Communications and Provision of Communication-Related Information Act (hereinafter referred to the RICA), Act 70 of 2002.

379 Act 2 of 2002. See section 9(a)(ii);

380 Section 34 reads as follows: PAIA only allows requestors access to “records”. A record is defined as follows in Section 1of PAIA:
‘record ‘of, or in relation to, a public or private body, means any recorded information-
(a) regardless of form or medium;
(b) in the possession or under the control of that public or private body, respectively; and
(c) whether or not it was created by that public or private body, respectively;”. It seems that the definition of record includes electronic evidence, but the right is limited to recorded information.

seek access to information, to which an objection is raised based on public policy,[381] the matter can be referred to court for adjudication.[382]

In terms of section 40 of PAIA, a public body may object to produce and make available for inspection information that it deems privileged in terms of public policy. Section 7 of PAIA further restricts the right to access to information:

> (1) This Act does not apply to a record of a public body or a private body if-
> (a) that record is requested for the purpose of criminal or civil proceedings;
> (b) so requested after the commencement of such criminal or civil proceedings, as the case may be; and
> (c) the production of or access to that record for the purpose referred to in paragraph (a) is provided for in any other law.

This aforementioned section is a mechanism to discourage litigants to abuse PAIA, to gain access to information in possession of a public or private body, where other legislation provide for the production and inspection of evidence, including electronic information.[383]

On the contrary, section 46 mandates that a public body disclose information:

> Despite any other provision in this chapter [ie including section 40] the information officer of a public body must grant a request for access to a record of the body contemplated in [various sections of the chapter] if (a) The disclosure of the record would reveal evidence of (i) a substantial contravention of or a failure to comply with the law, or (ii) An imminent and serious threat to safety or environmental risk; and (b) The public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question.

Some other examples are the Protection of Personal Information Act, (hereinafter referred to as POPIA)[384] and the ECTA. POPIA aims to balance the right to privacy

---

381 See the National Credit Act 34 of 2005, RICA , sections 50 and 51 of the ECTA and the Protection of Personal Information Act, Act 4 of 2013.

382 *My Vote Counts NPC v President of the Republic of South Africa and Others* 2017 (6) SA 501 (WCC).

383 Section 29(3) of the ECTA is a clear example of this. According to section 29(3) a cryptography provider does not need to disclose to the Director General of the Department of Communications confidential information about its cryptographic products when applying to have its products registered in South Africa.

384 The POPIA was signed into law by Former President Zuma on 19 November 2013 and published in the Government Gazette Notice 37067 on 26 November 2013. The aim of POPI is to ensure that

against other constitutionally protected rights and public policy. POPIA is only applicable where personal information is processed i.e : gathered, preserved, and disseminated by organisations or persons. Although POPIA takes cognisance of the principle of privilege, the protection afforded to individuals and organisations can be limited by the law of general application.[385] POPIA creates a legal framework to protect personal information and outlines the rights and duties of data handlers.[386] POPIA do not provide fast and hard rules for gathering, preservation, and dissemination of personal information. POPIA aims to balance the legitimate needs of organisations, to collect and use personal information for specific organisational purposes, against the right of a person to have his or her personal information kept private and confidential with his or her consent. POPIA applies to both public and private bodies.

POPIA restricts adversaries from gaining access to any information, irrespective of form the information is kept, from opponents without their consent even, if the information might not be privileged.

POPIA and the ECTA also aim to guard against the unlawful gathering, preservation, and use of personal information of any person by any data handler, organisation, person, and private or public bodies.[387] Similar to POPIA, the ECTA lists nine principles to which data controllers should adhere when processing personal information:[388]

(1) the express written consent of the data subject should be obtained, before the data controller may collect, collate, process or disclose personal information of the subject, unless required by law to do so;
(2) the data must be necessary for lawful purposes;
(3) that data controller must disclose in writing to the subject the purpose which the personal information will serve;
(4) the data controller may not use the information other than that for which it has been agreed upon with the subject;
(5) the data controller should keep a record of the personal information;

---

the state meets its constitutional obligation and give effect to the right to privacy enshrined in section 14 of the Constitution.

385 See limitation clause in the Constitution.
386 See chapter 3 of POPIA.
387 See section 51 of the ECTA.
388 See section 51 of the ECTA.

(6) the data controller unless required by law, may not disclose the personal information to a third party;

(7) if personal information is legally disclosed, the data controller must keep a record thereof;

(8) the data controller should delete all personal information which has become obsolete; and

(9) the data controller may use the personal information to compile profiles for statistical purposes and to trade freely with such profiles and statistics, as long as a third party cannot link the profiles or statistical data to a data subject[389]

The ECTA regulates the production, retention, and admission of data messages in legal proceedings as evidence in South Africa.[390] Sections 11 to 20 of the ECTA make provision for the production of "data messages" in legal proceedings. However, the ECTA does not deal with the procedural and evidentiary aspects related to the impropriety and inadvertent discovery of electronic information in legal proceedings. This is one of the shortfalls of the ECTA and reform is needed.

389 Section 51 of the ECTA.
390 Papadoulos and Snail (n 39 above) 317.

## 4.3 CLAW BACK AGREEMENTS

Litigants must operate ethically and sensitively to resolve issues that emanate from evidentiary management mistakes. These mistakes are more prevalent in cases that involve electronically generated and electronically stored information because a responding party can have thousands of electronic documents in their possession that are relevant to a dispute.[391]

Parties in the United States and the United Kingdom have developed a useful tool referred to as clawback agreements to counter discovery errors. Clawback agreements have their origins in the United States.[392] The use of clawback agreements has gained more traction in the United States, with the explosive growth of electronic information and the large volumes of electronic information, that has become the subject of production and inspection in the e-discovery process.

The United States has responded to the risk of inadvertent discovery of privileged information with clawback agreements, or non-waiver of agreements. Clawback agreements allow parties to conduct a less intense privilege review before the electronic information is made available to opponents. In the event that privileged materials are produced, it can be reclaimed without any waiver imputed from the circumstances. These agreements may provide that materials or information disclosed in error shall not impute waiver of any applicable privilege. The party claiming privilege must assert his or her right within a reasonable time after the inadvertent production became known

This form of agreement is regulated by Fed.R.Evid,[393] which specifically deals with inadvertent disclosure.[394] Clawback agreements are enforceable *inter partes*, but not against third parties.[395] The Fed.R.Civ.P works in tandem with the Fed.R.Evid,[396] to

391 Hibbert (n 216 above) 363.
392 Since the 2006 amendments to the Federal Rules of Civil Procedure in the United States parties can conclude such agreements.
393 See Fed.R.Civ.P 26(b)(5)(B).
394 See Fed.R. Evid 502(d).
395 See article dated January 5, 2008 on "The 2006 F.R.C.P. E-discovery Amendments: A Look One Year Later" available at http://www.pepperlaw.com/uploads/files/e-discovery_shiekman01052008.pdf accessed on 12 May 2018.
396 *Federal Rules of Evidence* (USA) Article V. Privileges, r 502.

address issues in regards to inadvertent discovery and the remedial steps a party may take to notify the requesting party of the error.

In the matter of *Brookfield Asset Management, Inc. v. AIG Financial Products Corp,*[397] the court illustrated the benefits of clawback agreements during the discovery process. The court considered the reach and ambit of Fed.R.Evid 502(d), which reads as follows:[398]

> A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court — in which event the disclosure is also not a waiver in any other federal or state proceeding.

In the *Brookfield Asset Management* matter, the court dealt with the discovery of AIG Board Minutes. The question before the court was whether the minutes were privileged and whether it was disclosed in error. Although AIG disclosed a redacted version of the minutes and it was censored before the minutes were made available, the embedded privileged information was still visible to the plaintiffs on review of metadata. The court held that the minutes contained privileged information and AIG has the right to claim the return of the redacted minutes, irrespective of the circumstances that gave rise to the disclosure of the minutes.

The court ruled that this advertent discovery did not amount to waiver, but emphasised the fact that litigants must keep a watchful eye over their vendors employed to assist with privilege reviews. Maas J noted that even if the defendant's counsel had "dropped the ball"; the parties entered into a 502(d) agreement that contained this noticeable point: Production of any documents in this proceeding does not constitute a waiver of any applicable privilege concerning produced documents. Even if the censored portions of the minutes were of significance to the plaintiff's case or the court's warning to litigants to closely monitor its e-discovery vendor's work, the stipulation provided AIG with an undisputed right to clawback the information disclosed in error. The court directed the plaintiff to return all copies of the draft minutes to AIG. The court based its finding upon

397 S.D.N.Y. Jan. 7, 2013.
398 See Fed.R.Evid 502.

the "clear answer" provided by the parties' Rule 502(d) stipulation that had been entered as a court order.

In this case, two issues are highlighted that legal practitioners need to be aware of when negotiating clawback agreements. As a starting point, a duly drafted 502(d) agreement can mitigate the risk inherent to inadvertent disclosure of privileged information. Secondly, it draws attention to the importance of understanding the form in which electronic documents are made available to the requesting party, and in particular, the metadata associated with the electronic documents that are discovered.

In the *Brookfield Asset Management* Maas J stated:[399]

> That stipulation (ECF No. 57) contains one decretal paragraph, which provides that "Defendants' production of any documents in this proceeding shall not, for the purposes of this proceeding or any other proceeding in any other court, constitute a waiver by Defendants of any privilege applicable to those documents, including the attorney-client privilege ...." Accordingly, AIG has the right to claw back the minutes, no matter what the circumstances giving rise to their production were.

The court also suggested a guideline to litigants on how to deal with clawback agreements in the digital era. Firstly, parties need to exercise due diligence when negotiating a clawback agreement. As part of the Rule 16(f) conference[400] at the start of legal proceedings, parties must discuss issues related to e-discovery and conclude an agreement with their adversaries that will govern the inadvertent production of privileged information. The clawback agreement should then be tendered to the court for it to be made an order of Court. It is important to note that Fed.R. Evid 502(d) extends the reach and protection afforded to litigants by a clawback agreement. For example, when a litigant disclosed privileged information under the circumstances as envisaged in Fed.R. Evid 502(b) and 502(c) it does not operate as a waiver in federal or state proceedings.

---

399 See *Brookfield Asset Management, Inc. v. AIG Financial Products Corp* (n 397 above) at paragraph 3.

400 See Fed.R.Civ.P.

The second leg of this guideline is that litigants must continuously evaluate the work of e-discovery vendors. The court also made it clear that parties need to take cognisance of the work of third parties vendors. Maas J stated:

> [t]his emphasizes the need for counsel for a producing party to keep a watchful eye over their e-discovery vendors.[401]

The legal representative must ensure that he or she fulfills his or her responsibility towards his or her clients. It is pivotal that legal representatives review the work of e-discovery vendors who assist them to review information for privilege. Parties must develop a working relationship with e-discovery service providers that will indicate to the court that the producing party took reasonable precautions to ensure that protected documents are not inadvertently disclosed. Parties should also assess the providers' experience in protecting privileged documents and inquire about what quality assurance and controls are in place before responding to a production request. It is considered professional negligence or misconduct not to seek an order in terms of Fed.R. Evid 502 in the United States.

In the United Kingdom, parties conclude clawback agreements before the first CMC, to ensure that all evidence, including electronic information, exchanged between parties before the first CMC is also protected, to avoid post-disclosure skirmishes over inadvertently disclosed information. Clawback agreements is not a full-blown remedy for all difficulties associated with inadvertent disclosure of privileged evidence, including electronic information.[402]

On the one hand, a court can take the view that an error was not obvious, and hence privilege is waived.[403] On the other hand, a court can also take the view that as soon as evidence, including electronic information, lands in the hands of third parties or litigants that are later joined to an action after conclusion of the clawback agreement, that privileged was waived and that the evidence, including electronic information, is no longer private and confidential.[404]

401 *Brookfield Asset Management, Inc. v. AIG Financial Products Corp* (n 397 above) at paragraph 2.
402 See Hibbert (n 216 above) 369.
403 See Hibbert (n 216 above) 369.
404 See Hibbert (n 216 above) 369.

## 4.4 QUICK PEEK AGREEMENTS

Electronic disclosure has also led to the emergence of another type of agreement, called "quick peek" agreements. The use of quick peek agreements occurs where there are time and practical constraints to execute a document-by-document review of large volumes of information before production for privilege.[405] With quick peek agreements, there is little or no review on the side of the producing party of information made available to adversaries. This is very risky, and in the United States and the United Kingdom, this may open the door for professional misconduct inquiries.

At common law, circumstances may exist where a party cannot say that the privilege has not been waived.[406] The circumstances are determined by the conduct of the producing party. A waiver may be express or implied. It will be implied in instances where the particular conduct is inconsistent with the maintenance of the confidentiality that the privilege is intended to protect.

## 4.5 CONCLUSION

The South African law provides little guidance to legal practitioners when evidence, including electronic information, is disclosed inadvertently or unlawfully obtained. There is no provision in the Magistrates' Court Rules, the Uniform Rules of Court, and the Labour Court Rules, that address the inadvertent discovery of evidence, including electronic information. The problem is further aggravated because the statutes that deal with issues related to privacy, confidentiality, and privilege are fragmented and disjointed. This is one of the shortfalls of the procedural law in South Africa when dealing with evidence, including electronic information.

During the discovery process litigants and their legal representatives need to take cognisance of the right to access to information,[407] right to privacy,[408] and access to

405 See Hibbert (n 216 above) 371. See CPR r.31.5 (7) (f). These orders give the Court a wide discretion to make any other order in relation to disclosure that the court considers appropriate.

406 In these circumstances waiver is imputed due the circumstances under which the information was disclosed.

407 Section32 of the Constitution gives a person the right to access to information and section 16 of the Constitution allows a person to distribute information to others.

408 Section 14 of the Constitution of South Africa.

justice,[409] and how the discovery of evidence including electronic information, fits into the South African constitutional dispensation.

The ECTA was enacted to deal with the admissibility of electronic information in legal proceedings but is silent on issues of inadvertent disclosure, privilege, and confidentiality of electronic information.

409 See Scheindlin (n 15 above) 391.

## CHAPTER FIVE

# 5. RECENT DEVELOPMENT OF THE PROCEDURAL LAW BY COURTS IN SOUTH AFRICA ON THE USE OF TECHNOLOGY AND ADMISSIBILITY OF ELECTRONIC INFORMATION AS EVIDENCE AND PROPOSED BILLS

In this chapter I will give an overview of various judgments that dealt with this new form of evidence. Our judiciary has made some remarkable strides in the field of procedural law to shed some light on the admission of this new form of evidence in legal disputes. This evident from the so-called Facebook cases that were adjudicated upon by the High Court[410] and the Labour court.[411] This will illustrate how courts had to navigate the procedural law framework and the law of evidence in South Africa to address technological advances. This overview of case law will assist me to gauge if our procedural framework is adequate to deal with electronic information as evidence in legal disputes. Recently electronic communications have become the cause of disagreement from which various legal disputes arose in South Africa.[412]

The ECTA was enacted to facilitate e-commerce and electronic communications. However, it fails to set out clear guidelines for legal practitioners, judges, and magistrates when dealing with procedural aspects that may affect the admissibility of electronic information, and the use of technology in courtrooms. Although the ECTA is in place, electronic evidence is not yet freed from traditional procedural law requirements in South Africa.[413]

Professor Karthy Govender, a research fellow in law at the University of Kwazulu Natal, states that our justice system must embrace the digital revolution and these digital forms of communication can add value to the procedural framework:[414]

---

410 *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD).

411 *Media Workers Association of SA obo Mvemve v Kathorus Community Radio* (2010) 31 ILJ 2217 (CCMA) and *Sedick and Another v Krisray (Pty) Ltd* (2011) 8 BALR (CCMA).

412 See *Jafta v Ezemvelo KZN Wildlife* (n 108 above) and *Sihlali v South African Broadcasting Corporation Ltd* (2010) 31 ILJ 1477 (LC) judgments in this regard. Also see *Isparta v Richter and Another* 2013 (6) SA 529 (GNP).

413 Schwikkard and Van der Merwe (n 16 above) 446.

414 See https://www.pressreader.com/south-africa/the-witness/20180604/281681140564011 accessed on 05 June 2018.

> When we consider evidence for something like a loan defaulter, the key is 'has the message been sent', and is there proof of it being sent and the person receiving it. If we can satisfy that, then it would be foolhardy not to move with the times and embrace this. Digital messaging could leave a trail that would be easier to follow, and even act as more trustworthy proof than a letter being sent. It could streamline the cumbersome process of sending letters. Very often people in default say they did not get the correspondence or communication. The party instituting proceedings will need to prove that the letter was dispatched via the post office and provide a registered slip as proof of dispatch.

In *Le Roux and Others v Viana NO and Others* , Mlambo JJA made the following observation:[415]

> Furthermore, properly construed the reference to books and documents in s 69(3) has nothing to do with the form in which those books and documents are. The Concise Oxford English Dictionary (10th edition revised) defines a book as 'a set of records or accounts or the embodiment of a record of commercial transactions' and a document as 'a piece of written, printed or electronic matter that provides information or evidence or that serves as an official record'. That these definitions accord with what the section contemplates cannot be disputed. They also fit in with the context within which one must view the role and functions of a trustee in the scheme of the Insolvency Act. There is no dispute in this case that the books and documents stored on the hard drive and targeted by the warrant relate to the financial and business affairs of the companies in liquidation. That being the case those books and documents, irrespective of the form they are in, are clearly within the contemplation of s 69 and are susceptible to seizure under a warrant in terms of that section. It can hardly be suggested, as counsel for the appellants submitted, that we should not take judicial notice of the technological advancements regarding electronic data creation, recording and storage because this was unheard of in 1936 when the Insolvency Act was passed.1 For these reasons the warrant is beyond reproach.

In the above matter, the court expanded the meaning of the term "document" to include electronic material susceptible to seizure for later use in legal proceedings.

In the S v *Ndiki* matter, the court dealt with rules of admissibility and stated that the same rules can be utilised to admit electronic information into evidence. In the *Ndiki* matter, Van Zyl J observed that evidence in electronic form is admissible and should not be excluded based on its nature. The judge stated that we need to treat electronic information in the same way as traditional evidence.

---

415 See *Le Roux and Others v Viana NO and Others* 2008 (2) SA 173 (SCA) at paragraph 10.

In the matter of *S v Agliotti*,[416] a subpoena was needed to access the accused's cell phone records. The Regulation of Interception of Communications and Provision of Communication-Related Information Act[417] (more popularly known as RICA) has been put in place to specifically make it easier to connect a cell phone account with a specific individual, in an attempt to simplify the verification of the identity of cell phone owners. However, the Constitutional Court has declared certain sections of RICA unconstitutional.

In *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd*[418] the court echoed the views of Van Zyl J in the *Ndiki* matter. In the *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd* the court held that tapes on which the company backed up information are discoverable under the Uniform Rule of Court 35.[419] The court expanded the reach of rule 35(1) and held that electronic information stored on backup tapes is a document.

In the matter of *Makate v Vodacom (Pty) Ltd,*[420] the question arose whether an agreement between the parties be signed in the same manner that individuals sign their emails. Two emails contained signatures of two persons. One of the signatures with which the email communication was concluded read: "Kind regards, Greg" and the other signature read: "Nigel". The content of the emails and the signatures attached to the emails respectively was not in dispute. The issue that the court had to determine was whether the signatures that the parties attached to their respective emails should have been advanced electronic signatures. The court held that the exchange of electronic communication meets the requirement of "writing" as envisaged in the ECTA.[421] The court further concluded that the requirement of a "signature" is met when the identities

416 2011 (2) SACR 437 (GSJ).
417 Act 70 of 2002.
418 [2011] ZAWCHC 358.
419 See *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd* ( n 418 above) at paragraph 9.
420 2014 (1) SA 191 (GSJ) at 202I–204B. This view was supported by Judge in in *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd* (n 418 above).
421 Section 12 of the ECT Act reads: "A requirement in law that a document or information must be in writing is met if the document or information is-
*(a)*in the form of a data message; and
*(b)* accessible in a manner usable for subsequent reference." This section puts a 'document' and a 'data message' on equal footing in law".

of the originator and addressee are clear from the exchange of electronic communications.[422] Spilg J stated :[423]

> I am accordingly satisfied that an e-document, ie. electronic material whether it be in the form of a communication or stored data that is retrievable through a filtering process or a data search, is discoverable under rule 35 procedures. Even if it were not so it would be open to utilise the provisions of rule 35 (7) in order to ensure that the discovery process achieves its objective in the electronic age. The caution expressed earlier about the need to ensure that discovery remains within acceptable limits, having regard to the volume of data captured and retained by electronic means has received consideration in other jurisdictions in the form of specific discovery procedures for electronic material. I have attempted to be cognisant of these concerns. In the present case they do not arise.

This is a clear indication that Spilg J concurs with what Van Zyl in the *Ndiki* case that evidence, including electronic information, should not merely be excluded as a result of its nature.[424]

In the matter of *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association*, Spilg J stated:[425] "information technology and the use of the internet is now commonplace". The court further observed:[426]

> Email is perhaps the most convenient means of communicating whether for work related activities or socially. Its other attributes are low cost, mobility and speed of communication irrespective of where in the world the respective parties happen to be. In the result, unsolicited advertising material reduces the convenience of using emails and increases overall costs to the consumer. It is also significant that one of the biggest providers of email software programs, Microsoft discourages its users from "unsubscribing" (see Microsoft's "Outlook 2007 Help" webpage on spam and junk e-mail) as this would verify the recipient's address as being active and, as can be inferred from the papers before me, this information itself can be on-sold or used when the spammer moves to another website or adopts other means to evade anti-spam measures.

422 See (n 84).
423 See *Makate v Vodacom* (n 45 above) at paragraph 40.
424 See (n 18).
425 See *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association* 2014 (2) SA 569 (GSJ) at paragraph 19.
426 See *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association* (n 415 above) paragraph 28.

In the Supreme Court of Appeal, in *Spring Forest Trading 599 CC v Wilberry (Pty Ltd t/a Ecowash and Combined Motor Holdings Limited t/a Green Machine*[427] the court dealt with electronic signatures. Cachalia JA made an important observation:[428]

> The approach of the courts to signatures has therefore been pragmatic not formalistic. They look to whether the method of signature used fulfills the function of the signature – to authenticate the identity of the signatory – rather than to insist on the form of the signature used.

Cachalia JA further stated:[429]

> It is apparent that the Act distinguishes between instances where the law requires a signature and those in which the parties to a transaction impose this obligation upon themselves. Where a signature is required by law and the law does not specify the type of signature to be used, s 13(1) says that this requirement is met only if an 'advanced electronic signature' is used. Where, however, the parties to an electronic transaction require this but they have not specified the type of electronic signature to be used, the requirement is met if a method is used to identify the person and to indicate the person's approval of the information communicated (s 13(3)*(a)*); and having regard to the circumstances when the method was used, it was appropriately reliable for the purpose for which the information was communicated (s 13(3)*(b)*).

The ECTA makes a clear distinction between situations where the law requires a signature, or where parties impose the obligation upon themselves.[430] The court in this instance accepted that the electronic signatures are valid as per the ECTA.

In the matter of *Democratic Alliance v African National Congress and Another,*[431] the Court dealt with evidence in the form of a short message service (hereinafter referred to as an SMS). The question was around an SMS that the Democratic Alliance

---

427 [2014] ZASCA 178.

428 *Spring Forest Trading 599 CC v Wilberry (Pty Ltd t/a Ecowash and Combined Motor Holdings Limited t/a Green Machine* (n 108 above) at paragraph 26.

429 See *Spring Forest Trading 599 CC v Wilberry (Pty Ltd t/a Ecowash and Combined Motor Holdings Limited t/a Green Machine* (n 108 above) at paragraph 18.

430 Section 13(3) of the ECTA states: 'Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if-
(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and
(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.".

431 2015 (2) SA 232 (CC).

(hereinafter referred to as the DA) sent to more than 1.5 million voters in Gauteng before the 2014 general elections. The content in the SMS read as follows:

> The Nkandla report shows how Zuma stole your money to build his R246m home. Vote DA on 7 May to beat corruption. Together for change.

The South Gauteng High Court as court of first instance in this matter[432] found that the SMS amounted to fair comment and dismissed the application. The African National Congress ( hereinafter referred to as the ANC) appealed this decision and the Electoral Court[433] reversed the decision of the High Court. According to the Electoral Court, the SMS contained false and inaccurate information. The Electoral Court further held that the publication of the SMS violated the Electoral Act, 73 of 1998,[434] and the Electoral Code Conduct.[435] The DA appealed against the decision of the Electoral Court to the Constitutional Court. Van Der Westhuizen J held that the Electoral Code and Act must be interpreted in light of the right to freedom of expression. At the core of this dispute was an SMS that was sent to millions of South Africans and the court dealt with this evidence as documentary evidence. Although the parties did not raise the issue of originality and authenticity, the court was open to look at electronic content in the form of an SMS as evidence.

In the matter of *Cape Town City v South African National Roads Authority and Others,*[436] the Supreme Court of Appeal (hereinafter referred to as the SCA) interrogated the "implied undertaking rule" in regards to discovery and inspection of documents. In casu Ponnan JA investigated the origins of the "implied undertaking rule" and found that it is inconsistent with our constitutional values and hence not part of the South African law.[437]

---

432 2014 (3) SA 608 (GJ).

433 See *Electoral Court: African National Congress v Democratic Alliance and Another* 2014 (5) SA 44 (EC).

434 See Rules Regulating the Conduct of Proceedings of the Electoral Court in terms of the Electoral Court Act, 73 of 1998.

435 See https://www.elections.org.za/content/Parties/The-Electoral-Code-of-Conduct/ last accessed 07 February 2020.

436 2015(3) SA 386 (SCA).

437 The Court held that, holding that implied undertakings are not part of our law". Ponnan J warned other courts not to blindly adopt the implied undertaking rule. The learned judge concluded that Court must err on the save side and first do the necessary analysis under section 39(2) of the Constitution to determine if the rule is in line with the spirit and objects of the Bill of Rights. Although the Court possess inherent powers under section 173 of the Constitution to regulate their own processes one still needs to do the analysis in terms of section 39(2) of The Constitution.

In *Harvey v Niland and Others,*[438] the court dealt with the issues of privacy and confidentiality in regards to private communications on a social media platform. This application arose as a result of the unlawful hacking of Niland's Facebook communications by Harvey. In casu, the court held that section 86(1) of the ECTA was silent on the admissibility of unlawfully intercepted evidence, including electronic information in the form of a data message, and there was no automatic exclusion of the tainted evidence. It further held that the court should exercise its discretion in assessing the admissibility of tainted evidence. Madlanga J stated:[439]

> I accept for purposes of this matter that, in accessing Niland's Facebook communications, Harvey acted unlawfully. I accept too that this act, apart from probably constituting criminal conduct also constituted a violation of Niland's right to privacy.

Harvey and Niland's partnership came to an end that left a sour taste in the mouth of Harvey. The association agreement entered into by Harvey and Niland contained a restraint of trade clause. Harvey averred that shortly after Niland left the employ of Huntershill, he suspected that Niland breached his fiduciary duties to Huntershill. Harvey alleged that Niland was actively competing against the business activities of Huntershill by soliciting and diverting existing clients of Huntershill to Thaba Thala.

Plasket J stated:[440] [I]n these circumstances, I am of the view that annexure 'G' is admissible and the application to strike it out must fail." The court held that the right to privacy and confidentiality of information is not absolute.[441]

In the matter of *Gareth Cliff v Electronic Media Network (Pty) Ltd and Entertainment (Pty) Ltd* [442] a dispute arose between the litigants as to whether a valid contract was

---

438 See (n 281 above).
439 See *Harvey v Niland and Others* ( n 260 above).at paragraph 48.
440 See *Harvey v Niland and Others* ( n 260 above).at paragraph 53.
441 See paragraph 53 of the judgment that reads as follows: "In these circumstances, I am of the view that annexure 'G' is admissible and the application to strike it out must fail". See *Gaertner & Others v Minister of Finance& Others* 2014 (1) BCLR 38 (CC) where Madlanga J made the following remark: "Privacy, like other rights, is not absolute. As a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks. This diminished personal space does not mean that once people are involved in social interactions or business, they no longer have a right to privacy. What it means is that the right is attenuated, not obliterated. And the attenuation is more or less, depending on how far and into what one has strayed from the inner sanctum of the home."
442 *Cliff v Electronic Media Network (Pty) Ltd and Entertainment (Pty) Ltd* case no 1368/16 (SGH).

concluded between the parties to the dispute. Nicholls J ruled that emails exchanged between parties were admissible as evidence irrespective of its nature. The court did not deal with the admissibility issues such as originality, authenticity, etc. as neither party raised it.

In the matter of *Viziya Corporation v Collaborit Holdings (Pty) Ltd and Others,* the court dealt with the preservation of electronic information and Mathopo J made the stated:[443]

> The major flaw in Viziya's case was not so much the scope of the search, which would always need to be comprehensive, but the failure in its affidavits to identify or specify which vital information was in possession of Collaborit that needed to be preserved. As this court held in para 30 of Non Detonating Solutions, a blanket search for unspecified documents or evidence, which may or may not exist, is not permitted. Viziya was obliged to identify the documents it sought to preserve with the necessary degree of specificity, possibly by category as occurred in Non-Detonating Solutions.

In the Randburg Magistrate's Court, two seminal judgments were handed down about service of letters of demand as required by section 129 of the National Credit Act.[444] In these cases, the Magistrates accepted that letters of demand delivered via SMS were of similar status to the traditional registered post.[445] These judgments dealt with default loan repayments, where the final letter of demand was sent via SMS to the defaulters. The SMS notifications we delivered to the defaulter's cellular number via a registered SMS. In terms of the ECTA digital registered SMS or electronic mail meets the regulations in regards to the legality of electronic messages. A message delivered via electronic messaging or communication is, therefore, deemed a request made in writing.[446]

---

443 See *Viziya Corporation v Collaborit Holdings (Pty) Ltd and Others* SA ( n 247 above) at paragraph 32.

444 See Randburg Cases for March 2018 and May 2018 available at https://www.southafricanlawyer.co.za/article/2018/06/digital-letters-of-demand-the-way-forward/. These cases dealt with sections 12 and 19(4) of the Electronic Communications and Transactions Act, as well as section 129 of the National Credit Act.

445 Ignoring those SMSes that remind you to pay your debts could see you facing the might of the law.

446 See https://www.pressreader.com/south-africa/the-witness/20180604/281681140564011 accessed on 05 June 2018.

*Minister of Finance v Oakbay Investments and Others*[447] dealt with the relief sought by the then Minister of Finance that the Minister was not by law compelled to interfere in a private dispute between a financial institution and its client. The Director of Financial Intelligence Centre, at the request of the Minister of Finance, issued a certificate[448] setting out 72 suspicious transactions (hereinafter referred to as STR's) that were reported to the Financial Intelligence Centre by banks against several entities in the Oakbay Group and several associated individuals.

In a second application that ran parallel to the matter referred to above, namely *Oakbay Investments (Pty) Ltd and Others v Director of the Financial Intelligence Centre*,[449] several entities brought an application against the Director of the Financial Intelligence Centre to compel the Director to disclose electronic information that was reported and sent to the FIC by the applicants' erstwhile bankers.[450] The second application was premised on section 40 (1) (e) of the FIC Act.[451]

The application was dismissed with costs. The FIC application was withdrawn and the court held that the application was not necessary, although the FIC application was based on the FIC Act. The court held that the application related to access to information that was entrenched in the Constitution and was intended to enforce the applicant's constitutional right.

---

447 *Minister of Finance v Oakbay Investments (Pty) Ltd and Others; Oakbay Investments (Pty) Ltd and Others v Director of the Financial Intelligence Centre* 2018 (3) SA 515 (GP) (18 August 2017).

448 In terms of section 39 of the Financial Intelligence Centre Act 38 of 2001 the Director may issue a certificate that sets out certain transaction as stipulated in terms of sections 28, 29, 30 (2) or 31 of the FIC Act.

449 (80978/2016) [2017] ZAGPPHC 576.

450 See sections 28, 29, 30 (2) or 31 of the FIC act. The certificate listed 72 STRs sent to the FIC by the banks in regards to companies who formed the Oakbay Group and associated individuals.

451 This application is referred to as the FIC application. See section of the FIC Act 40 Access to information held by Centre:
(1) No person is entitled to information held by the Centre, except-
…
(e) in terms of an order of a court; Section 40 and 41 of the FIC Act must be read together. Section 41 reads as follows: No person may disclose confidential information held by or obtained from the Centre except- (a) within the scope of that person's powers and duties in terms of any legislation; (b) for the purpose of carrying out the provisions of this Act; (c) with the permission of the Centre; (d) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or (e) in terms of an order of court.

The SALRC also drafted the Law of Evidence Bill (hereinafter the LEB)[452] to address the issues related to electronic evidence. In this draft bill, the SALRC provides definitions of what constitutes a document[453] and an electronic document[454] respectively. This proposed bill aims to regulate the admissibility of electronic evidence but it seems that there is still a lack of cohesion between the CPA, CPEA, and the LEB on what constitutes a document.

The Protection of Personal Information Act was gazetted on 26 November 2013[455] but is not yet fully operational in South Africa. The legislation was enacted to ensure that the constitutional right to privacy is protected and it deals with the confidentiality of personal information.[456]

The Protection of State Information Bill (hereinafter referred to as POSI) was gazetted on 05 March 2010 and still awaits promulgation. In the event that this Bill is signed into law by the president, it will limit the scope of PAIA in regards to access to certain information.[457]

The legislature also introduced the Cybercrimes Act,[458] and it takes cognisance of the existence of evidence in electronic form.[459] The proposed bill deals with the protection of personal data and makes provision for the preservation and disclosure of electronic

---

452 See Discussion Paper 131 Project 126 "Review of the Law of Evidence" available at http://www.justice.gov.za/salrc/dpapers/dp131-prj126-ReviewLawOfEvidence.pdf accessed on 24 June 2018.

453 "Document" shall mean "anything in which information of any description is recorded and includes a copy". Available at http://www.lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf.

454 "Electronic document" shall mean "data that are recorded or stored on any medium in or by a computer system or other similar device, and includes a display, printout or other output of that data". Available http://www.lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf

455 See Government Gazette Vol 581 No. 37067.

456 Section 54 of POPI Act reads as follows: "A person acting on behalf or under the direction of the Regulator, must, both during or after his or her term of office or employment, treat as confidential the personal information which comes to his or her knowledge in the course of the performance of his or her official duties, except if the communication of such information is required by law or in the proper performance of his or her duties."

457 See section 49 of the Bill.

458 See https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000.

459 See preamble of the Cybercrimes Act (n 111 above).

evidence.[460] It also sets out the procedure that must be invoked to ensure that electronic evidence is preserved and disclosed. Although this draft bill is aimed at curbing cybercrime, it at least gives some guidance on the preservation of evidence in the form of a data message and the dissemination of electronic information.

## 5.2 CONCLUSION

It is clear from the judgments mentioned above, legislation, and proposed Bills that electronic evidence is here to stay and our procedural framework must be adapted to make provision for technological advancements.

460 See sections 39, 40 and 42 of the Cybercrimes Act (n 111 above). It is clear that the SALRC takes cognizance of the importance of electronic evidence, and we need to embrace it.

# CHAPTER 6

# DISCOVERY

## 6.1 BACKGROUND TO DISCOVERY

The chapter will examine the process of e-discovery in two Anglo-Saxon jurisdictions namely the United States and the United Kingdom respectively. Further, this chapter aims to determine if the South African procedural law in its current state is adequate to allow electronic information in pre-trial and trial preparation. This chapter will also examine if the current discovery process in South Africa can safeguard the integrity and reliability of electronic information when adduced as evidence.

> Discovery has been said to rank with cross-examinations one of the two mightiest engines for the exposure of the truth ever to have been devised in the Anglo-Saxon family of legal systems. Properly employed where its use is called for it can be, and often is, a devastating tool.[461]

The process of discovery is common to jurisdictions where the legal systems are based on the common law systems.[462] The process of discovery is referred to as disclosure in the United Kingdom. In this work, the term discovery will be used for the sake of consistency and clarity. In almost all types of civil disputes, there is oral-, documentary- and real evidence that have a bearing on the factual disputes of a case.[463] The rapid rise in electronic communication and e-commerce expanded the realm of discovery. As mentioned earlier electronic information can be classified as real- or documentary evidence. Electronic information can be created in one of three ways:

(a) content created by a person. Generally, this evidence would be hearsay without evidence from persons who inputted the data;

(b) electronic information created without any human intervention and would constitute real evidence. In the event that the evidence is generated by a

---

461 See *MV Urgup: Owners of the MV Urgup v Western Bulk Carriers (Australia) (Pty) Ltd and Others* 1999 (3) SA 500 (C) at paragraph 513G-513H.

462 Matthews and Malek *Disclosure* 5ed Sweet and Maxwell 10 and Hibbert (n 216 above) 444.

463 Van Heerden (n 24 above) 35; Cohen and Lender (n 3 above)1-1; George (n 55 above) 283 and Rockwood "Shifting the Burdens and Concealing Electronic Evidence: Discovery in the Digital Era" 2005-2006 *Richmond Journal of Law & Technology (Rich.J.L& Tech)* 19. See also *STT Sales v Fourie* 2010 (6) SA 272(GSJ) at par 276C-D. Discovery is a procedure that are to be used to identify factual issues once legal issues has been determined. According to Malan J discovery is a procedure whereby a party to an action may ascertain what documents and tape recordings relating to the matter in issue is in the possession of the opponent.

computer we assume that the computer was properly functioning at all times; and

(c) information that consists of electronic information and information compiled by human intervention.

The process of discovery deals with identifying, collecting, preserving, managing, and producing evidence that is relevant and admissible in legal proceedings.[464] The process of discovery should aid with the authentication of evidence and test the integrity of the evidence to determine its admissibility.[465]

The underlying purpose of the process of discovery is to give effect to the *audi alteram partem*-principle.[466] The process of discovery is the ideal mechanism with which to meet this need to obtain access to information for purposes of trial.[467] The rules of evidence applicable to the process of discovery exist to ensure that parties do not utilise the process to establish legal issues in their pre-trial skirmishes.[468] Thring J supported

---

464 Schwerha; Bagby and Esler (n 3 above) 810. This process is time consuming and the most expensive part in the whole litigation process.

465 Van Heerden (n 24 above) 35 and Stanfield (n 140 above) 190.

466 Van Heerden (n 24 above) 33; See Hughes and Stander (n 67 above) is helpful to litigants to ensure all the parties is aware of all the relevant documentary evidence available, to narrow down the issues in dispute in the matter and to prevent the element of surprise. The ordinary purpose of discovery is to give litigants access to documents in possession of their opponents and to determine in advance what documents will be relevant at trial. The aforementioned documents must be made available to the party who does not have access to the relevant documents to inspect and copy it.

467 In the matter of *Hickman v. Taylor*, 329 U.S. 495, 507 (1947) the court held as follow: "Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation. Thus the spirit of the rules is violated when advocates attempt to use discovery tools as tactical weapons rather than to expose the facts and illuminate the issues by overuse of discovery or unnecessary use of defensive weapons or evasive responses."

468 See Van Heerden (n 24 above) 33; Schwerha; Bagby and Esler (n 3 above) 797; *FirstRand Bank Ltd t/a Wesbank v Manhattan Operations* 2013 (5) SA 238 (GSJ) 243C-E*. Independent Newspapers v Minister for Intelligence Services* [2008] ZACC 6 39-43*; Bosasa Operations v Basson* 2013 (2) SA 570 (GSJ) 574B-D*; Bridon International GmbH v International Trade Administration Commission* 2013(3) SA197(SCA) 209I-210E*; Transnet v MV Alina 11* 2013 (6) SA 556 (WCC) 563H-564E*; Capalcor Manufacturing v GDC Hauliers* 2000 (3) SA 181 (W) 194A; *Santam Ltd v Segal* 2010(2) SA 160 (N) at 165D-G; *Makate v Vodacom* (n 45 above) at paragraph 197I-1198D. In the matter of *Playboy Enterprises Inc v Welles* 78 F. Supp. 2d 1066 (S.D. Cal. 1998) the Court ordered that a mirror image of the hard drive in possession of the producing party be made available to the requesting party. However, in *Fennell v First Step Designs Ltd* 83 F.3d 526, 532-33 (1st Cir. 1996) the Court deviated from the *Playboy Enterprises Inc v Welles* decision. In the latter case, the court was of the view that the protocol submitted by Fennell was vague and inadequate and will convert the discovery process of into a fishing expedition. In *Fennell v First Step Designs Ltd* 83 F.3d 526, 532-33 (1st Cir. 1996) the Court held that the protocol submitted by Fennell was held to be inadequate, making discovery too much of a 'fishing expedition'.

the view that discovery is a process to aid legal practitioners to minimise factual disputes. In the matter of *MV Urgup v Western Bulk Carriers* the judge stated:[469]

> Discovery must not be abused or called in aid lightly in situations for which it was not designed or will lose its edge or become debased.

However, in some instances, pre-action discovery is available to a requesting party if there is a need and an advantage to obtain access to the information.[470]

One of the features at the core of the process of discovery is that a party in whose possession or under whose control evidence is ought to know the nature thereof.[471] A party who is in control or possession of documentary or real evidence is obliged to arrange it chronologically for the benefit of his or her adversary and the court before setting the matter down for trial.[472]

Discovery enables parties to place before the court evidence that is relevant, genuine, accurate, and authentic to the factual disputes before the court.[473] The discovery process, however, also serves several other purposes, and there is extensive literature on its functions, especially in the United States where discovery consumes the largest share of the litigation process and has been described as a "self-contained universe".[474] Discovery of evidence must assist the court in discovering the truth and come to a just determination in a matter.[475] One of the benefits of the process of discovery is that it

---

469 See *MV Urgup v Western Bulk Carriers* 1999 (3) SA 500 (C) at paragraph.

470 See rule 31.16 of the CPR in United Kingdom, section 50 of PAIA in South Africa and Rule 37 of the Uniform Rules of Court.

471 See *Capalcor Manufacturing v GDC Hauliers* 2000 (3) SA 181 (W) 194I.

472 See Van Heerden (n 24 above) 33; Mason "England and Wales" in Mason *Electronic Evidence* 3rd ed 415; Hibbert (n 216 above) 250. See CPR PD 58 paragraph 10.8.

473 See Schmidt and Rademeyer (n 2 above) 11-21; *Church of Scientology of California v Department of Health and Social Security* [1979] 1 WLR 723 (CA) at paragraph 733C-E. In *STT Sales v Fourie* 2010 (6) SA 272(GSJ) the court held that: "as a general rule and order for discovery will only be made after the legal issues has been determined". *See also MV Urgup v Western Bulk Carriers* 1999 (3) SA 500 (C) 513I.

474 See Van Heerden (n 24 above) 35.

475 Hughes & Stander (n 65 above). In *Davies v Eli Lilly & Co.* Lord Donaldson made the following remark: "[L]itigation in this country is conducted 'cards face up on the table'. Some people from other lands regard this as incomprehensible. 'Why', they ask, 'should I be expected to provide my opponent with the means of defeating me?' The answer, of course, is that litigation is not a war or even a game. It is designed to do real justice between opposing parties and, if the court does not have all the relevant information, it cannot achieve this object."

can aid litigants to assess the merits of their case prior to the trial, to avoid lengthy and unnecessary trials and adverse cost orders.[476]

Herbstein & Van Winsen[477] describes the purpose of discovery as follows:

> The function of discovery is to provide the parties with the relevant documents or recorded material before the hearing so as to assist them in appraising the strength or weaknesses of their respective cases, and thus to provide the basis for a fair disposal of the proceedings before or at the hearing. Each party is therefore enabled to use before the hearing or to adduce in evidence at the hearing documents or recorded material to support or rebut the case made by or against him or her to eliminate surprise at or before the hearing relating to documents or recorded evidence and to reduce the costs of litigation.

The process of discovery in the three jurisdictions under consideration is regulated by a set of legal rules originating from various statutes and jurisprudence.[478] Each jurisdiction has additional rules or practice directives that it follows to facilitate the process of discovery.[479]

According to Moseneke DCJ discovery must ensure that litigants are afforded an adequate chance to prepare and present their respective cases.[480] The process of discovery enables parties to establish what evidence is in their opponents' possession or under their control that may advance or damage either party's case.[481] It is of utmost importance that attorneys and their clients cooperate with their adversaries to prepare and exchange all relevant information before the trial.[482]

---

476 Van Heerden (n 24 above) 35; Sharpe "Electronically Recorded Evidence" (1989) 53 and Mason (n 169 above) 391.

477 Herbstein and Van Winsen (n 2 above) 777.

478 See the CPEA; LEAA; ECTA; RICA and POPIA.

479 See the model applicable in federal districts and states in the United States of America.

480 See *Independent Newspapers v Minister for Intelligence Services* [2008] ZACC 6.

481 See *Capalcor Manufacturing v GDC Hauliers* 2000 (3) SA 181 (W); Parties are therefore under a duty to discover all documents which may *"either directly or indirectly enable the party requiring the affidavit either to advance his own case or to damage the case of his adversary*"; See *Swissborough Diamond Mines v Government of the Republic of South Africa* 1999 (2) SA 279 (T) at 316-317).

482 See *Capalcor Manufacturing (Pty) Ltd v GDC Hauliers (Pty) Ltd (formerly GDC Hauliers CC)* 2000 (3) SA 181 (W) 195B.

As part of this process, litigants must disclose all documentary evidence in their possession or under their control under oath in the form of an affidavit[483] to their opponents for inspection and trial purposes.[484]Attorneys should ensure that their clients fully comprehend the significance of the process of discovery and the contents of the affidavits parties execute to place evidence before the court.[485] Legal practitioners must ensure that affidavits drafted on behalf of clients must be crafted with precision and accuracy. This requires that parties need to be honest and frank in their discovery affidavits.

In the matter of *Natal Vermiculite v Clark* the court stated:[486]

> All attorneys should realise that it is their clear duty to ensure that their clients fully appreciate the significance and importance of a discovery affidavit before it is drawn up. No attorney should allow a client to make such an affidavit unless he is satisfied that his client understands what is required of him and appreciates that dire results may follow at the trial if an inaccurate discovery affidavit is made. Attorneys are responsible for the technical side of litigation and they have a duty to see that their clients understand the importance of complying with the Rules of Court.

The process of discovery has been revisited ample times to keep track of jurisprudential development as well as legislative reform of the procedural framework that facilitates discovery in the three jurisdictions considered in this work.[487] The process of discovery has evolved into a two-fold process. Firstly, it focuses on uncovering the truth to come

---

483 In the Magistrates' Court, this affidavit would take the form similar to that of Form 13 in the Magistrates' Court Rules whilst in the High Courts it will take the form similar to Form in the Uniform Rules of Court.

484 Schmidt and Rademeyer (n 2 above) 12-3.

485 See *Rellams (Pty) Ltd v James Brown and Hamer Ltd* 1983 (1) SA 556 (N) at paragraph 558E stated: "[g]reat weight … is given to these affidavits and they should not be drawn in so loose a manner as to leave any avenue of escape.". See *Natal Vermiculite v Clark* 1957 (2) SA 431(N) at paragraph 431F- 432A the court made the following remark "[A]n affidavit of discovery is a solemn document, not merely a scrap of paper, and it is the duty of every attorney to be satisfied that in drawing up a discovery affidavit, the client understands what is required and appreciates that dire results may follow at the trial if an inaccurate discovery is made. Full and honest disclosure should be made".

486 1957 (2) SA 431(N) 431H-432A.

487 The matter *Durbach v Fairway Hotel* 1949 (3) SA 1081 (SR) are seen as the locus classicus that laid the foundation for the modern-day discovery in South Africa.

to a just determination.[488] Secondly, one needs to bear in mind the costs associated with producing relevant and admissible evidence to prove the truth.[489]

It is essential to identify and protect confidential and privileged information of a producing party during the process of discovery. Litigants may employ traditional mechanisms at their disposal when requesting the discovery of electronic information.[490] However, one should be bear in mind that the procedural tools and evidentiary rules were developed when electronic information and metadata associated with the electronic information were unheard of in pre-trial preparation and litigation in general.[491] This implies that litigants must discover the documents together with the embedded information about that document.

488 See Transnet v MV Alina II 2013 (6) SA 556 (WCC) at 19; Air Canada v Secretary of State for Trade [1983] 2 AC 394 at 445 – 446 and Santam Ltd and Others v Segal 2010(2) SA 160 N at 162 E – F.

489 Burke et al (n 53 above) 150; and Schwerha; Bagby and Esler (n 3 above). The underlying principle of discovery is that it must assist court in reaching a just determination of the issues in dispute.

490 See Cohen and Lender (n 3 above) 2-3.

491 Withers "Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure" 4 NW.J. TECH.& INTELL.PROP.171 (2006) 212 and Grimm "Authenticating digital evidence" (n 145 above) 47-49.

## 6.2 ELECTRONIC DISCOVERY

One needs to ask the following question. What is electronic discovery? Electronic discovery is often distinguished from conventional discovery, which refers to the discovery of information recorded on paper, film, or other media, which can be read without the aid of a computer.[492] Of course, there is also the discovery of tangible things that usually refers to physical objects and property, which is real evidence.

Electronic documents and information consist of large volumes of data that is stored in multiple repositories with complex internal structures of collections of data and the relationships of one file to another are in different formats and coding schemes that may need to be converted into text to be reviewed; and subject to frequent changes in information technology.[493] Electronic discovery refers to the retrieval of electronic documents or information together with the embedded information that attaches to the electronic information that encompasses the identification, collection, processing, preservation, and production of electronic information in legal proceedings.[494] Electronic documents consist of anything that is stored on a digital device such as e-mail, web pages, word processing files, and computer databases. Electronic information is readily accessible on various platforms and devices such as desktop and laptop computers, network servers, cloud servers, and smartphones. Documents and data are electronic if they exist in a medium that can only be read with the aid of a digital device for example computer hard drives, DVDs, and CDs.[495]

The Sedona Conference has had several working groups dedicated to the development of guidelines and standards to assist legal practitioners and judicial officers with various issues related to electronic discovery in the United States. The first Working Group ( also known as WG1) met between 17-18 October 2002 and was dedicated to the development of guidelines for electronic document identification, collection, processing, preservation, and production. The Sedona conference defined electronic discovery:[496]

---

492 Hibbert (n 216 above) 3.
493 See Herbstein and Van Winsen (n 2 above) 811.
494 Harrison (n 20 above) 22.
495 Sharpe (n 158 above) and Hedges (n 172 above) 1.
496 See https://thesedonaconference.org/download-pub/3757 accessed on 02 October 2017. See https://www.edrm.net/frameworks-and-standards/edrm-model/ where the EDRM model conceptualizes the e-discovery process for litigants to assist them. Also see See Herbstein and Van Winsen (n 2 above) 811.

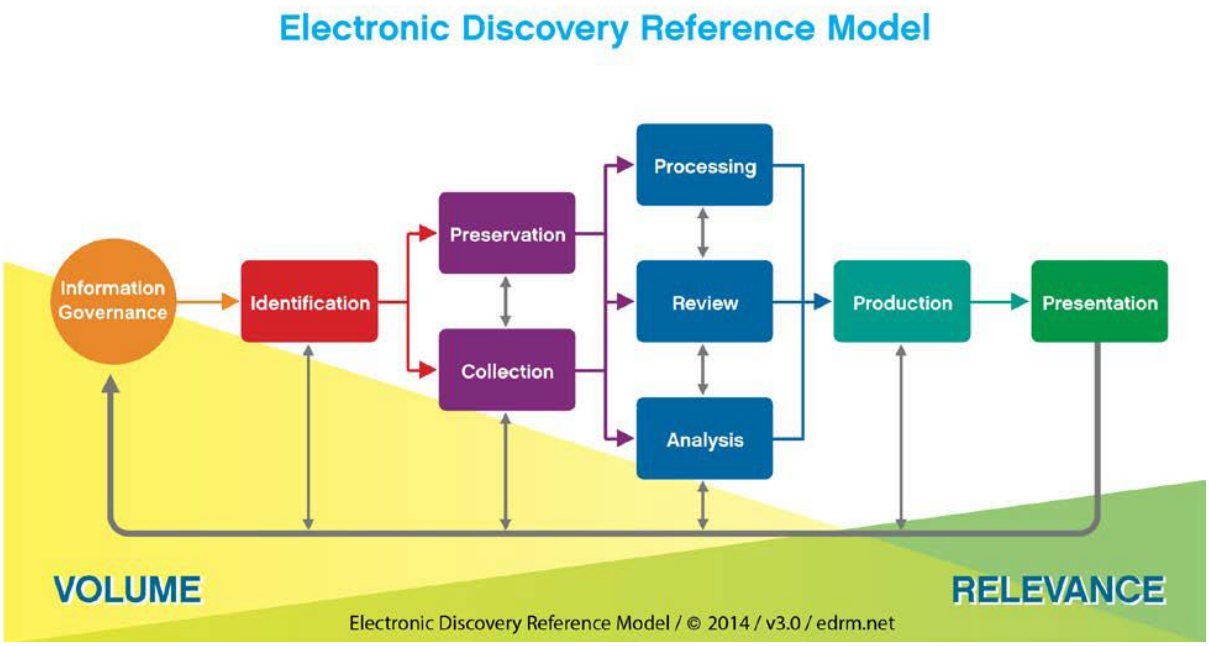
> the process of identifying, locating, preserving, collecting, preparing, reviewing, and producing electronically stored information in the context of the legal process.

The aforementioned definition is not the only available definition of electronic discovery.[497] Simply put it is the discovery of electronic information and metadata associated with that electronic information. One must bear in mind that although information is recorded and stored in digital form it can still be classified as either real- or documentary evidence.[498]

There is no uniform way to conduct the process of e-discovery.[499] The need for e-discovery standards came to the fore because of the proliferation of electronically generated information and electronically stored information, and the lack of guidelines to assist legal practitioners during the process of e-discovery in the United States and later in the United Kingdom.[500] This led to the development of a roadmap, also known as the Electronic Discovery Reference Model (hereinafter referred to as the EDRM).[501] The EDRM is based on e-discovery practices in the United States, and it seems that legal practitioners find it useful in the United Kingdom as a reference to consult during the discovery process.[502] This model consists of nine (9) phases that provide industry standards to assist legal practitioners during the process of discovery of electronic evidence.[503]

---

497 See Hibbert (n 216 above) 3.
498 See Schmidt and Rademeyer (n 2 above) 12-11. Admissibility of this evidence will be subject to the provisions of section 34 of the CPEA.
499 Wheater and Raffin (n 2 above) 21.
500 Hibbert (n 216 above) 5. See Infology "Comments and submissions in response to issue paper 27" http://www.infology.net/downloads/Infology%20Submission%20in%20response%20to%20Issue%20Paper%2027.doc.
501 Hibbert (n 216 above) 5. The EDRM was developed in 2005 by George Socha Jr., founder of St. Paul, Minn.-based Socha Consulting LLC, and Tom Gelbmann, managing director of Gelbmann & Associates in Roseville, Minnesota. See Figure 1 below available at https://www.edrm.net/frameworks-and-standards/edrm-model/.
502 Hibbert (n 216 above) 6 and Wheater and Raffin (n 2 above) 5.
503 See Figure 1.1 available in Hibbert (n 216 above) 7 and included in this text as illustration.




The EDRM is not the only model available to legal practitioners and litigants, However, it provides legal practitioners and litigants with a framework to consult during the process of discovery.

The availability of electronic information that is subject to discovery raises just as many questions as the solution it provides. One of the main issues is that this wealth of information brings with it technical electronic discovery issues.[504] Legal practitioners must have basic computer skills to understand technology in the electronic discovery process.[505] The fact that legal practitioners and Information technology professionals are aware of the myriad of information available on digital platforms but do not comprehend the technology behind the law and *vice versa.*[506]

504 Hibbert (n 216 above) 53.
505 Reavis (n 25 above) 275.
506 Cohen and Lender (n 3 above) 18-2; Hibbert (n 216 above) 53.

## 6.3 ELECTRONIC DISCOVERY IN THE UNITED STATES OF AMERICA

The United States is a common-law jurisdiction with separate court systems within each of its states.[507] The Fed.R.Civ.P prescribes the procedure for obtaining discovery, including e-discovery in the federal courts. Some of the states in the United States have their own set of rules applicable to discovery, which are modeled on the Fed.R.Civ.P.[508] In some instances these state rules are an exact mirror image of the Fed.R.Civ.P.[509] New Jersey is an example of e-discovery rules that govern the collection, production, and best practices in legal proceedings and mirrors the federal rules.[510]

The Sedona Conference played a pivotal role in the development of the process of e-discovery in the United States.[511] The Sedona Principles were at the pinnacle in the formulation of the so-called national standards for the discovery of electronic information in the United States.[512] The recommendations of the Sedona Conference were one of the catalysts that brought about the amendments to Fed.R.Civ.P in the United States that laid the foundation for the discovery of electronically stored information.

The Sedona Principles, jurisprudence, and the amendments to the Fed.R.Civ.P have significantly paved the way for the development of standards and guidelines for the process of e-discovery in the United States.[513] The amendments to the Fed.R.Civ.P.[514]

---

507 Cohen and Lender (n 3 above) 2-3 and 2-7and Schwerha; Bagby and Esler (n 3 above) 798.

508 For example, California has its own Electronic Discovery Act that regulates production and discovery of electronic information. However, its Electronic Discovery Act falls within the scope and ambit of federal laws in the United States. More than 50 percent of the states' and some local federal districts in United States have adopted special rules relating to electronic discovery including states like Texas and Virginia. Some federal districts like District of Wyoming, Eastern and Western Districts of Arkansas have embarked on addressing electronic discovery by varying their respective local rules. Furthermore, although these various states in the United States have their own set of rules applicable to discovery, its foundation is in the Fed.R. Civ.P.

509 See Mason (n 3 above) 703. There are fifty states within the United States, each with their own rules of evidence. It is not intended that the rules of evidence within each state be examined, rather only the rules of evidence within the federal jurisdictions.

510 Clare and Prentice "Collecting Electronically Stored Information" *New Jersey Law Journal* Vol. 208 - No 7__.

511 See https://thesedonaconference.org.

512 See https://www.edrm.net/frameworks-and-standards/edrm-model/edrm-stages-standards/ accessed on 03 July 2018.

513 See Zubulake cases (n 79 above).

514 According to Mason (n 3 above) rule 26 and 34 of the Fed.R.Civ.P was too restrictive to admit electronic evidence hence the amendments ensured that electronically stored information is admissible and discoverable.

were a direct result of the work done by the Sedona Conference working group.[515] The Sedona Conference Working Group 1 formulated 14 principles as guidelines for courts that judicial officers and legal practitioners may consult and it was specifically tailored to address the challenges posed by electronic information that is adduced as evidence in tribunals, forums, and courts.[516] The Sedona Principles[517] complements the Fed.R.Civ.P and the Fed.R.Evid in regards to the discovery of electronic information.[518]

The need to amend the Fed.R.Civ.P was further amplified by the series of *Zubulake* judgments[519] as well as the *Rowe* decision.[520] The Fed.R.Civ.P was amended on numerous occasions to ensure that electronic information is not excluded, lost, or abused as evidence in legal proceedings.[521]

The Fed.R.Civ.P facilitates the process of discovery of certain discoverable evidence in courts in the United States.[522] Rule 1 and rule 26 of the Fed.R.Civ.P sets out the parameters and scope of discovery in general.[523] Rule 34 of the Fed.R.Civ.P specifically deals with the discovery of electronically generated information and electronically stored information in civil litigation.[524] The inclusion of the term ESI in rule 34(a) places paper

---

515 This working group consisted of lawyers, jurists, academics and consultants and formed the Sedona Conference Working Group 1 on Electronic Document Production.

516 See https://thesedonaconference.org.

517 See Addendum E at the end of this dissertation.

518 See Harvey (n 98 above) 175.

519 See (n 102 above).

520 Harvey (n 98 above) 174.".

521 See http://www.uscourts.gov/rules.gov/rules/EDiscovery_w_Notes.pdf. The amendments affected rules 16, 26, 33, 34, 37, 45 and Form 35.

522 See Fed.R. Civ.P 1, 26-37 and 45. The rules changes were introduced to specifically deal with issues that arose with collection, preservation and production of electronic information. The Fed.R. Civ.P only regulates procedures in civil matters and the Federal Rules of Criminal Procedure govern criminal matters. For purposes of this dissertation, we will focus on the Fed.R. Civ.P and not on the Federal Rules of Criminal Procedure. The 2006 amendments to the Federal Rules of Civil Procedure addressing the discovery of electronically stored information became effective 01 December 2006. See http://www.uscourts.gov/rules.gov/rules/EDiscovery_w_Notes.pdf. The amendments above affected rules 16, 26, 33, 34, 37, 45 and Form 35.

523 The provisions of Rule 26 of the Fed.R. Civ.P applies mutatis mutandi to electronic discovery. However, Rule 34 was specifically inserted into the Fed.R.Civ.P to address the challenges posed by ESI; See Cohen and Lender (n 3 above) 2-54.2; Rockwood "Shifting the Burdens and Concealing Electronic Evidence: Discovery in the Digital Era" (n 463 above) 12.

524 The Fed.R.Civ.P only regulates procedures in civil matters; however, Federal Rules of Criminal Procedure govern criminal matters. For purposes of this study, writer will focus on the Fed.R.Civ.P and not on Federal Rules of Criminal Procedure. The 2006 amendments to the Federal Rules of Civil Procedure addressing the discovery of electronically stored information became effective 01 December 2006.

documents and electronic documents on equal footing.[525] Fed.R.Civ.P 26(a)(1)(i) and 26(a)(1)(ii) require a party to produce evidence even before a formal request is received.[526]

In general, parties will initially use rule 26 of the Fed.R.Civ.P to obtain production of discoverable evidence.[527] In circumstances where parties seek that electronic information under the control or in their possession of adversaries to be made available, rule 34 of the Fed.R.Civ.P is employed in conjunction with rule 26 of the Fed.R.Civ.P in the United States.[528]

Legislative intervention ensured that litigants have clarity on whether electronic information is subject to discovery and admissible as evidence in legal proceedings.[529] ESI is specifically included as one of the categories of information that is susceptible to discovery and inspection in the United States.[530]
In the United States, parties are required to attend a rule 26 (f) conference prior to the court's rule 16 conference to discuss preliminary issues in regards to the discovery and inspection of evidence, including electronic information and its metadata.[531] This requires that litigants discuss problems related to identification, collection, preservation,

---

525 Cohen and Lender (n 3 above) 2-5.
526 Cohen and Lender (n 3 above) 2-19.
527 Rule26 reads as follows: "(a) Required Disclosures.
(1) Initial Disclosure.
(A) In General. Except as exempted by Rule 26(a)(1)(B) or as otherwise stipulated or ordered by the court, a party must, without awaiting a discovery request, provide to the other parties:
(i) the name and, if known, the address and telephone number of each individual likely to have discoverable information—along with the subjects of that information—that the disclosing party may use to support its claims or defenses, unless the use would be solely for impeachment;
(ii) a copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment;
(iii) a computation of each category of damages claimed by the disclosing party—who must also make available for inspection and copying as under Rule 34 the documents or other evidentiary material, unless privileged or protected from disclosure, on which each computation is based, including materials bearing on the nature and extent of injuries suffered; and
(iv) for inspection and copying as under Rule 34, any insurance agreement under which an insurance business may be liable to satisfy all or part of a possible judgment in the action or to indemnify or reimburse for payments made to satisfy the judgment."
528 See Addendum A at the end of this dissertation.
529 See Rule 26(a)(1)(A)(ii) of the Fed.R.Civ.P.
530 See Rule 26(a)(1)(A)(ii) give a description of discoverable information: "copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defences." Rule 34(a) also supports the inclusion of electronic information.
531 See Scheindlin (n 15 above) 97.

and discovery of relevant evidence, including electronic information that must be preserved. However, rules 26 and 34 of the Fed.Civ.R.P does not stipulate that metadata must be preserved and produced but urge parties to discuss it.[532]

Parties involved in litigation need to specify the form in which they want evidence, including electronically stored information to be preserved and discovered. If a requesting party opts that information be produced in electronic form, the requesting party need to also indicate the format in which they want the information to be produced.[533] If parties fail to agree or the is no rule 16 order in place, the responding party can produce the ESI in the form it is ordinarily maintained in or in a reasonably useable form.[534] Rules 26 and 34 of the Fed.R.Civ.P set out in detail the processes and procedures to be followed to obtain discovery. The aforementioned rules go further to outline the scope and limitations of these rules with reference to the discovery of relevant and admissible evidence, including electronic information that is subject to privilege and confidentiality. Parties are required to agree on a protocol when the evidence, including electronic information, is inadvertently discovered.

As mentioned in chapter 3 of this research preservation in anticipation of the later discovery of evidence, including electronic information.

The process of discovery of electronic information in the United States is not without limits. In terms of rule 34 of the Fed.R.Civ.P, the courts have power under rules 26(b)(2)[535] and 26(c)[536] to limit the scope of discoverable information litigants may obtain from their adversaries.[537] Rule 34[538] allows a requesting party to search the responding party's databases and computer systems for ESI that is relevant to issues in dispute between parties. This provision is a two-edged sword. If the requesting party

532 See Scheindlin (n 15 above) 214-222.
533 For example, native format, TIFF or PDF. See Scheindlin (n 15 above) 105.
534 See Scheindlin (n 15 above) 201-209.
535 See Addendum A on the content of this rule.
536 See Addendum A on the content of this rule.
537 Rule 26(b)(2)(B) sets parameters for initial discovery of electronically stored information to information from reasonably accessible sources. The court in *Zubulake I* noted that consideration of cost shifting is appropriate where stored data is not in a "readily useable" format, such as backup tapes. The decision above is an example of how the Courts can utilise Rule 34 of the Fed.R. Civ.P to limit the scope of discovery.
538 See Rule 34 of the Fed.R.Civ.P. However, this rule makes provision that parties must agree on the form of production at the Rule 26(f) conference. If an agreement is reached between the parties, it may be embodied in a Rule 16(b) Scheduling Order.

is not familiar with the responding party's in-house recordkeeping, management systems, databases, hardware, and software applications they might struggle to find responsive material during searches. However, this may also allow the requesting party access to privileged information of the responding party.[539]

The procedure outlined in rule 34 of the Fed.R.Civ.P can be time-consuming and disruptive and might not bear any fruit at all. The manner in which this rule is worded and the operation thereof can obstruct the discovery process.[540] The rationale behind this is, in the event that a requesting party fails to specify in which form or format production must occur, the producing party may produce the requested information in its native format or any form that is inaccessible to the requesting party.[541] This will render the request by the requesting party who has no knowledge of the responding party's computer systems futile.

If a requesting party is allowed to search the producing party's servers and databases for response material, it may lead to several problems. For instance, if the requesting party does not have the technical expertise to conduct searches for responsive material, it places the procedure at risk of abuse, as producing parties can argue that they have met and discharged their discovery obligations to produce relevant electronically stored information from computer systems and databases. United States judges are not keen on revisiting the issue of e-discovery if parties failed to raise certain issues at the initial planning conference.[542] Although the United States is at the forefront of e-discovery, judicial intervention is still required to curb abuse of the procedure during the discovery process.[543] On the one hand, rule 26 of the Fed.R.Civ.P allows courts to make certain protective orders when claims of privilege or protection of trial preparation material are raised. On the other hand, the court can also sanction a party for failing to comply with rule 26 or when the court is of the view that a party is abusing the rules of court.

---

539 See Fed.R.Civ.P 26(f) that requires parties to discuss issues of privilege at scheduling conference and trial court may include provisions related to privilege in their scheduling orders. This issue of privilege is also discussed with reference to quick-peek agreements.

540 See Fed.R.Civ.P. 34(b) (1(C).

541 PB31B paragraph dictates to litigants in what format information must be made available. Unlike the position in the USA where a party need to specify at the planning conference in which format, they need the information.

542 *Wells Fargo Bank v LaSelle Bank* 2009 U.S Dist. LEXIS 70514(S.D Ohio July 24, 2009).

543 Cohen and Lender (n 3 above) 2-22. Courts is expected to play an active role in case management early on in proceedings to avoid later disputes.

## 6.4 ELECTRONIC DISCOVERY IN THE UNITED KINGDOM

Civil matters instituted in the courts in the United Kingdom are currently governed by the rules outlined in the CPR[544] as well as the Civil Evidence Act, 1995. The CPR provides the procedural framework and Civil Evidence Act deals with evidentiary rules in regard to evidence in the United Kingdom. For more than a century, the issue of disclosure and inspection of evidence in the United Kingdom was based on the *Compagnie Finacière et Commerciale du Pacifique v Peruvian Guano Co* test[545] formulated by Lord Justice Brett:[546]

> It seems to me that every document relates to the matters in question in the action, which not only would be evidenced upon any issue, but also which, it is reasonable to suppose, contains information which may—not which must—either directly or indirectly enable the party requiring the affidavit either to advance his own case or to damage the case of his adversary. I have put in the words 'either directly or indirectly' because, as it seems to me, a document can properly be said to contain information which may enable the party requiring the affidavit either to advance his own case or to damage the case of his adversary, if it is a document which may fairly lead him to a train of inquiry, which may have either of these two consequences.

The CPR and Commercial Court Guide (hereinafter referred to as the CCG) was formulated for the discovery of paper documents. The capturing and storing of information digitally challenged the provisions of the CPR and CCG. Courts in the United Kingdom that were faced with these challenges opted to extend the ambit and scope of the term "document". As a result, courts included electronic evidence in legal proceedings on a case-by-case basis.[547]

The matter of *Hands v. Morrison Construction Services Ltd*[548] was the first reported English decision in which the court considered the discovery of electronic documents. Deputy Judge Michael Briggs QC declined to order pre-action disclosure of electronic documents despite an offer by the applicant to meet the cost on the ground that there

544 See (n 77 above).
545 See *Compagnie Finacière et Commerciale du Pacifique v Peruvian Guano Co (1882)11 QBD* 55.
546 See *Compagnie Finacière et Commerciale du Pacifique v Peruvian Guano Co* (n 545 above) 63.
547 Harvey (n 98 above) 22.
548 [2006] E.W.H.C. 2018 (Ch).

is an undue burden on the responding party.[549] Surprisingly, the judge took this stance in view of the fact that the electronic documents met the requirements of rule 31.6 of the CPR. *In casu,* the court refrained from ruling on the critical issue of whether the requested electronic documents were disclosable or not.

Part 31 of the CPR was introduced in 1999 to facilitate the disclosure and inspection of evidence, including electronic information in the United Kingdom. The CPR is supplemented by additional requirements dealing with disclosure of electronic information set out in Practice Direction 31A (hereinafter referred to as PD 31A) and Practice Direction 31B (hereinafter referred to as PD 31B). Practice Directions does not operate in isolation. It forms part of the general principles that pervade civil litigation in the United Kingdom.[550]

The process of disclosure and inspection is initiated by requesting standard disclosure. Generally, courts expect parties to discuss issues of disclosure and inspection of evidence, including electronic information at the first CMC. Rule 31.4 of the CPR sets out the scope and ambit of what documents must be disclosed and must be read in conjunction with rule 31.6 of the CPR.[551] Rule 31.6 of the CPR reads as follows:

> Standard disclosure requires a party to disclose only–(a) the documents on which he relies; and(b) the documents which –(i) adversely affect his own case;(ii) adversely affect another party's case; or(iii) support another party's case; and(c) the documents which he is required to disclose by a relevant practice direction"

In terms of rule 31.6 courts have the discretion to direct parties to disclose documents in electronic form or any other format to the requesting party.[552] In terms of rule 31.5 of the CPR, a court may give various orders that dispense with or limit disclosure of evidence, including electronic information. The order contemplated under rule 31.5 is normally referred to as standard disclosure.[553] Rule 31.5 of the CPR states:

---

549 The court only made an order for limited discovery of the hard copies of requested information. In this matter, the Court omitted to give guidance on how litigants must apply the Practice Direction of the Court.

550 Hibbert (n 216 above) 191.

551 Rule 31.6 of the CPR reads as follows: "Standard disclosure requires a party to disclose only–(a) the documents on which he relies; and(b) the documents which –(i) adversely affect his own case;(ii) adversely affect another party's case; or(iii) support another party's case; and(c) the documents which he is required to disclose by a relevant practice direction."

552 See *Mueller Europe Ltd v Central Roofing (South Wales) Ltd*, 2012 WL 6933786 (2012).

553 See Mason (n 23 above) 219. The new rule 31.5 came into effect in April 2013.

(1) In all claims to which rule 31.5(2) does not apply –

(a) an order to give disclosure is an order to give standard disclosure unless the court directs otherwise.

Courts in the United Kingdom are of the view that parties should not use the process of disclosure to establish legal issues, but rather to request disclosure of documents that is reasonable to dispose of factual issues in a case.[554] Part 31 of the CPR attempts to simplify the process of disclosure, and at the same time attempts to outline the process as comprehensively as possible.[555]

Part 31 of the CPR was supplemented in 2005 by PD 31A.[556] Paragraph 2A.1 of PD 31A[557] refers to the definition of the term "document" mentioned in rule 31.4 of the CPR. This paragraph pertinently states that the term "document" includes electronic documents.[558] Part 31 of the CPR was further supplemented in October 2010.[559] This led to the introduction of PD 31B.[560] Paragraph 1 of PD 31B also refers to the term

554 See *Compagnie Finacière et Commerciale du Pacifique v Peruvian Guano (1882) 11 QBD 55; Radio Corp of America v Rauland Corp [1956] 1Q.B.* 618*; British Leyland Motor Corp v Wyatt Interpart* [1979] F.S.R.39 45 and *DigiCell (St. Lucia) v Cable and Wireless Plc*, 2008 WL 4698881(2008).

555 Van Heerden (n 24 above) 77.

556 PD 31A supplements CPR Part 31 and deals with disclosure and inspection. Paragraph 2A (1) of the aforementioned practice directive provides a detailed and broad description of what can be included in the definition of document.

557 Rule 31.4 contains a broad definition of a document. This extends to electronic documents, including e-mail and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been 'deleted'. It also extends to additional information stored and associated with electronic documents known as metadata. The word document as defined in CPR PD31A include material such as databases and disks holding information in electronic form.

558 PD31A paragraph 2A.1 reads as follows: "Rule 31.4 contains a broad definition of a document. This extends to electronic documents, including e-mail and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been 'deleted'. It also extends to additional information stored and associated with electronic documents known as metadata".

559 See Hollander (n 229 above) 393. The Civil Procedure Rules Committee introduced CPR PD31B after a long consultative process led Senior Master Whitaker. PD 31B applies to claims issued on or after 1 October 2010. PD 31B contains definitions of terms such as electronic document and metadata. Parties need to take cognisance of PD 31B when dealing with EGI and ESI prior to disclosure and as the process unfolds. During this process Parties must ensure that they minimise costs and ensure that the give effect to the primary objectives of the process of disclosure.

560 CPR PD31B provides detailed definitions of relevant terms such as 'electronic document' and 'metadata'. CPR PD 31B is applicable to claims instituted on or after 1 October 2010 and formulated to aid litigants to resolve disclosure of electronic documents.

"document" as defined in Rule 31.4 of the CPR and mentions that the term "document" includes electronic documents.[561] The definition of the term "document" is qualified in Practice Directions 31A[562] and 31B[563] where a definition of "electronic document", is also provided. The definition provides that an "electronic document" is any document held in electronic form. The introduction of PD 31A and PD 31B ensured that digital information is on equal footing with paper documents and not lost as evidence in the United Kingdom.

PD 31B[564] was specifically inserted into Part 31 of the CPR to eliminate the challenges posed by e-discovery. PD 31B directs parties to discuss the discovery of electronic documents before the first CMC.[565] Before the commencement of the CMC, parties can voluntarily exchange an Electronic Document Questionnaire.[566] In this questionnaire, parties may raise any issue related to the disclosure and inspection of electronic documents.

It seems from the drafting of paragraph 2A.1 of PD 31A and paragraph 1 of PD 31B that the drafters of the Practice Directions took cognisance of case law.[567] Paragraph 2A.1 of PD 31A stipulate that electronic documents, such as e-mails, other electronic

561 See CPR PD31B paragraph 1(1) that reads as follows: "Rule 31.4 contains a broad definition of document. This extends to electronic documents."

562 See Paragraph 2A.1 reads as follows: "at 2A.1 Rule 31.4 contains a broad definition of a document and reads as follows: "This extends to electronic documents, including e-mail and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been 'deleted'. It also extends to additional information stored and associated with electronic documents known as metadata."

563 See paragraph5 (3) reads as follows: "Electronic Document' means any document held in electronic form. It includes, for example, email and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones. In addition to documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes metadata and other embedded data which is not typically visible on screen or a printout."

564 See paragraph 10 of the practice direction in this regard.

565 Wheater and Raffin (n 2 above) 83. See CPR PD58 paragraph 10.1.

566 See paragraph 10 of PD31B that stipulates as follows: In some cases, the parties may find it helpful to exchange the Electronic Documents Questionnaire in order to provide information to each other in relation to the scope, extent and most suitable format for disclosure of Electronic Documents in the proceedings. This questionnaire consists of fourteen questions that enables litigants to identify and locate relevant electronic information. The aforementioned questionnaire assists parties in regard to the extent and ambit of a reasonable search of electronically recorded and stored information. See Addendum F attached to this research.

567 See *Derby & Co Ltd v Weldon* (n 84 above).

communications, word-processed documents, and databases fall within the ambit of a document.[568] Paragraph 5(3) reads as follows:

> Electronic Document' means any document held in electronic form. It includes, for example, email and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones. In addition to documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes metadata and other embedded data which is not typically visible on screen or a printout.

Apart from documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that have been deleted.[569] It also extends to hidden information stored and associated with electronic documents known as metadata.[570] CPR PD 31B paragraph 5(7) defines metadata as:

> Metadata' is data about data. In the case of an Electronic Document, metadata is typically embedded information about the document which is not readily accessible once the Native Electronic Document has been converted into an Electronic Image or paper document. It may include (for example) the date and time of creation or modification of a word-processing file, or the author and the date and time of sending an email. Metadata may be created automatically by a computer system or manually by a user.

In a watershed ruling, Morgan J came to the rescue of litigants in the matter of *Digicel (St Lucia) Ltd v Cable and Wireless Plc*.[571] In his judgment, Morgan J set out a methodical approach that he considered to be appropriate under the circumstances in the application of PD 31A and PD 31B in e-discovery cases in the United Kingdom.

---

568 See *Derby & Co Ltd v Weldon* (n 84 above).

569 This includes information that is destroyed by routine business operation as well as information that was intentionally destroyed to defeat a claim or defense.

570 See paragraph 28 and 33 of PD31B that deals with discovery of electronic documents and the metadata associated related to the electronic documents. CPR PD31B paragraph 5(7) defines metadata as follows:
"(7) 'Metadata' is data about data. In the case of an Electronic Document, metadata is typically embedded information about the document which is not readily accessible once the Native Electronic Document has been converted into an Electronic Image or paper document. It may include (for example) the date and time of creation or modification of a word-processing file, or the author and the date and time of sending an email. Metadata may be created automatically by a computer system or manually by a user."

571 [2008] EWHC 2522 (Ch).

Firstly, the Court set out the relevant provisions of Practice Direction 31A that applied to the legal issues before the court. In paragraphs, 33-36 of its judgment the court dealt with various issues it deemed relevant to disclosure of electronic documents in the matter before the court. The court first evaluated if the information can be seen as electronic documents and the procedure that parties need to follow to execute a reasonable search for responsive information to comply with the CPR.[572]

The court also investigated the possibility of other search methods in case no responsive information is found through a reasonable search of the electronic documents. The court also considered specific disclosure if the responding party fails to meet his or her disclosure and inspection obligations under rule 31.5 of the CPR.

Secondly, the court incorporated the findings of the Creswell report[573] into its judgment as well as the relevant provisions of the CPR that had bearing on the facts of the case that was before the court. Morgan J in his judgment set out what he thought parties should consider when dealing with e-discovery.[574]

In the *Digicel (St Lucia) Ltd v Cable and Wireless Plc* judgment[575] Morgan J gave a detailed approach on the application of PD 31A as well as PD 31B on the disclosure and inspection of electronic documents. This set the benchmark for the disclosure and inspection of electronically stored information in the United Kingdom. The *Digicel* matter provides a good yardstick to legal practitioners and judicial officers that they may employ to tackle the challenges posed by the disclosure and inspection of electronic information in the United Kingdom.

The CPR allows parties to seek specific disclosure if a responding party failed to meet their disclosure obligations.[576]

572 See paragraphs 33-36 of Addendum G at the end of this thesis.
573 See http://webarchive.nationalarchives.gov.uk/20110218200720/http://www.hmcourts-service.gov.uk/docs/electronic_disclosure1004.doc accessed last on 06 August 2018.
574 See paragraphs 37- 40 of Addendum G at the end of this thesis.
575 See *DigiCell (St Lucia) Ltd v Cable and Wireless Plc* (n 571 above).
576 See rule 31.12 of the CPR in the United Kingdom.

Legal Practitioners in the United Kingdom also utilise the EDRM model to plan for the identification, collection, preservation, and production of electronic information as evidence in legal proceedings. This is evident from Part 31 of the CPR that parties must discuss matters related to the discovery of electronic information from the onset.[577]

The Civil Evidence Act 1995 governs the authentication of evidence in civil matters in the United Kingdom[578] and the Criminal Justice Act 1988 applies to criminal matters. Evidence is admissible if it is relevant to the factual disputes of the matter. However, certain exceptions are applicable in the United Kingdom.[579] Part 33 of the CPR contains miscellaneous rules of evidence that the Courts use to aid with authenticating electronic evidence. Parties must discuss the admissibility of electronic evidence at the first CMC in the United Kingdom. Judges in the United Kingdom have an explicit general power to exclude any evidence even though it might be admissible.[580]

577 The Creswell Report identified five stages a party had to go through to comply with disclosure obligations in relation to ESI:(1) identify how many of the documents which might be relevant to the case have been created by electronic means; (2) identify whether these electronic documents have been preserved and where they might be stored; (3) retrieve, and search for, any relevant electronic documents; (4) conduct a review of the electronic documents; and (5) produce the electronic documents, ideally, in an agreed format.

578 Section 9 of the Civil Evidence Act 1995 provides: "that documents that form part of the records of a business or public authority, as defined in that section, may be received in evidence without further proof." The admissibility of secondary evidence in civil proceedings is regulated by section 8 of the Civil Evidence Act 1995, which permits the introduction of copies of documents into evidence for the purpose of proving the statement contained in the document. Section 8 of the Civil Evidence Act provides: "(1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved—(a) by the production of that document, or (b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve. (2) It is immaterial for this purpose how many removes there are between a copy and the original."

579 For example, the Business Records Exception to the Hearsay Rule and the Hearsay Rule in the United Kingdom.

580 Rule 32.1 of the CPR states as follows:
"(1) The court may control the evidence by giving directions as to –(a) the issues on which it requires evidence;(b) the nature of the evidence which it requires to decide those issues; and (c) the way in which the evidence is to be placed before the court. (2) The court may use its power under this rule to exclude evidence that would otherwise be admissible."

## 6.5 DISCOVERY IN SOUTH AFRICA

Attorneys are increasingly moving away from paper-based litigation to e-litigation.[581] This, in turn, leads to the question of what constitutes a "document", as mentioned in rule 23 of the Magistrates' Court Rules, rule 6(9) of the Labour Court Rules, and rule 35 of the Uniform Rules of Court respectively. Neither the Magistrates' Court Rules[582] nor the Uniform Rules of Court[583] provide any definition of the term "document". This poses the challenge of whether electronic information is real- or documentary evidence, as well as what would fit in the traditional concept of the term "document". Issues such as originality, authenticity, and reliability, and admissibility are fearlessly debated to determine the admissibility of electronically generated and stored information.

This raises the question of whether the discovery of electronic information differs from conventional paper-based discovery.[584] This chapter will investigate whether or not the discovery of electronic information differs from conventional paper discovery during pre-trial and trial preparation stages.[585] This chapter will further investigate whether electronic evidence is so different from paper-based evidence that new rules are required to regulate and facilitate the discovery of electronic information in legal proceedings. It is evident from the literature that electronic information differs from traditional documents[586] and can be classified as either real or documentary evidence.[587]

---

581 See Hughes (n 2 above) 24 and Burke et al (n 53 above). Recently Judge President Mlambo, issued a practice directive for the full implementation of Case Lines in the North and South Gauteng Division of the High Court. The pilot program commenced in Gauteng in the third term of 2019 and the full implementation of the Case Lines commenced during January 2020.

582 See section 2 of the Magistrates Court Rules.

583 See section 1 of the Uniform Rules.

584 See SALRC report (n 12 above).

585 In *Byers v. Illinois State Police*, 53 Fed. R. Serv. 3d 740 (N.D. III. May 31, 2002) Magistrate Judge Nolan highlighted a few differences between traditional paper document and electronic documents as follows: "Computer files, including emails, are discoverable…. However, the Court is not persuaded by the plaintiffs' attempt to equate traditional paper-based discovery with the discovery of email files…. Chief among these differences is the sheer volume of electronic information. Emails have replaced other forms of communication besides just paper-based communication. Many informal messages that were previously relayed by telephone or at the water cooler are now sent via email. Additionally, computers have the ability to capture several copies (or drafts) of the same email, thus multiplying the volume of documents. All of these emails must be scanned for both relevance and privilege. Also, unlike most paper-based discovery, archived emails typically lack a coherent filing system. Moreover, dated archival systems commonly store information on magnetic tapes that have become obsolete. Thus, parties incur additional costs in translating the data from the tapes into useable form".

586 See www.sedonaconference.org.

587 Swales (n 44 above) 21.

Although rule 23 of the Magistrates' Court Rules and rule 35 of the Uniform Rules strive towards the same goal, these rules are distinctly different.[588] This lack of cohesiveness between these rules further creates uncertainty amongst legal practitioners and judicial officers on issues related to the discovery of evidence, including electronic information. To permit a meaningful discussion of the process of discovery in South African law it is necessary to explain and analyse the discovery in the Magistrates' Court and High Courts respectively. A comparison between these court procedures is required to identify deviations and gaps between the two processes within the South African context.

The South African procedural framework requires that if a party intends to adduce evidence, including electronic information, it must be preserved[589] and later produced in its original form.[590] In terms of the prevailing law, the requirement of the integrity of a "data message" is met if it remained unaltered in the light of the purpose for which the information was generated and taking cognisance of all relevant circumstances.

Rule 23 of the Magistrates' Courts Rules,[591] rule 35 of the Uniform Rules[592] , and rule 6 of the Labour Court Rules respectively regulate the process of discovery when parties in civil proceedings are required to discover on oath all documents relating to the matter in question in litigation, and to make available those documents for inspection in South Africa. The provisions of the aforementioned rules are set out below.

In terms of rule 23(1):

> Any party to any action may require any other party thereto, by notice in writing, to make discovery on oath within twenty (20) days of all documents and tape, electronic, digital or other forms of recordings relating to any matter in question in such action, whether such matter is one arising between the party requiring discovery and the party required to make discovery or not, which are or have at any time been in the possession or control of such other party.

---

588 According to Van Dorsten (n 3 above) Van Dorsten the wording of rule of 35 of the Uniform Rules of Court of Court is inadequate to provide for the discovery of 'documents and tape recordings' and differs from rule 23 of the Magistrates Court Rules which speaks to the discovery of 'all documents and tape, electronic, digital or other forms of recordings relating to any matter in question'.

589 Section 16 of the ECTA.

590 Section 14 of the ECTA.

591 Rule 23(1) is the procedural tool employed in the Magistrates Court to request the producing party to make available evidence that might advance or damage the requesting party's case.

592 Rule 35(1) is the procedural tool employed in the High Courts to request the producing party to make available evidence that might adversely affect or assist to prove the requesting party's case.

Rule 35(1) states:

> Any party to any action may require any other party thereto, by notice in writing, to make discovery on oath within twenty (20) days of all documents and tape recordings relating to any matter in question in such action (whether such matter is one arising between the party requiring discovery and the party required to make discovery or not) which are or have at any time been in the possession or control of such other party. Such notice shall not, save with the leave of a judge, be given before the close of pleadings.

Rule 6(9) reads as follows:

> (a) A document or tape recording not disclosed may not, except with the leave of the court granted on whatever terms the court deems fit, be used for any purpose at the hearing by the person who was obliged to disclose it, except that the document or tape recording may be used by a person other than the person who was obliged to disclose it.
> (b) If the parties cannot reach an agreement regarding the discovery of documents and tape recordings, either party may apply to the court for an appropriate order, including an order as to costs.
> (c) For the purpose of this rule, a tape recording includes a soundtrack, film, magnetic tape, record or any other materials on which visual images, sound or other information can be recorded.

The wording of rule 23(1) of the Magistrates' Court Rules and rule 35(1) of the Uniform Rules of Court differs in that rule 23(1) requires parties to discover the following: "all documents and tape, electronic, digital or other forms of recordings" whilst the rule 35(1) of the Uniform Rules of Court only requires: "all documents and tape recordings". Rule 23(1) of the Magistrates' Courts Rules seems to extend further than rule 35(1) of the Uniform Rules of Court to include electronic and digital and other forms of recordings.[593] The wording of rule 35 of the Uniform Rules of Court seems to restrict evidence that can be discovered under this rule.[594] Furthermore, it seems that rule 35 does not adequately provide for the discovery of electronically created and stored information and retrieved primarily in its native electronic form. This difference creates the impression that these two procedural tools seek to obtain different outcomes from litigants. It appears that rule 23 can facilitate the discovery of electronic and digital forms of recording and is possibly a step in the right direction. However, rule 23 fails to address issues such as

593 See Cassim (n 19 above) 26.

594 See Van Dorsten (n 3 above) 36. Van Dorsten is of the view that the Uniform Rules of Court in South Africa does not make provision for the discovery electronically stored information. In my view, the Magistrates Court Rules also falls short in this regard.

how parties need to preserve, retain, manage and eventually discover electronic information

In the matter of *Le Roux and Others v Viana NO and Others* court circumvented the procedural restrictions imposed on it by the Insolvency Act and by implication extended the definition of the word "document". In the matter of *Le Roux and Others v Viana NO and Others*, the court found that the word "document" has nothing to do with the form in which information is kept.[595] In the matter *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd and Another (WCC)*[596], the court also followed an approach similar to the *Viana* case and held that the backed-up tapes on which a company stored and preserved its electronic information were discoverable under rule 35 of the Uniform Rules of Court. Parties may also request courts to direct the discovery of ESI.

definition of a tape recording in rule 35(15) of the Uniform Rules of Court is wide enough to include all electronic information. However, the court failed or neglected to provide clarity on the question as to whether the electronic information must be in a readable format or not.

In the matter of *Makate v Vodacom,* the court extended the definition of a tape recording to allow the discovery of electronic information.[597] Both Rule 35(15) of the Uniform Rules of Court as well rule 23(16) of the Magistrates' Court contains a definition of a tape recording. A tape recording is defined as:

"a tape recording includes a soundtrack, film, magnetic tape, record or any other material on which visual images, sound or other information can be recorded."

595 See *Le Roux and Others v Viana NO and Others* ( n 415 above) at paragraph 10.

596 See *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd* ( n 418 above).

597 In *Makate v Vodacom (Pty) Ltd* ( n 45 above) at paragraph at 202I-204B the court held: [t]hat an e-document, i.e electronic material, whether it be in the form of a communication or stored data that is retrievable through a filtering process or a data search, is discoverable under rule 35 procedures and that, even if it were not so, it would be open to utilize the provisions of rule 35(7) [i.e the equivalent of magistrates' courts rule 23(7)] in order to ensure that the discovery process achieves its objective in the electronic age.

The court interpreted the definition of a tape recording in rule 35(15) and rule 23(16) to include all different kinds of material as evidence if it is stored as visual images, sound, and other information. At face value, it appears that the definitions of tape recording are wide enough to include all types of material on which visual images, sound, and other information may be stored. Even if one considers a purposive interpretation of the definition of a tape recording in rule 35(15)[598] and rule 23(16)[599] it seems that both rules focus on the medium on which the information is stored rather than the information itself.[600] The position regarding the discovery of electronic information is challenging in the current digital age, where documents are created and stored electronically *vis-à-vis* the storage of hard copies.

This implied position is a means to end, but it still has certain inadequacies in that the rules do not make provision for the evidentiary aspects applicable to real or documentary evidence that is admissible in legal proceedings. For example, rule 23 of the Magistrates' Court Rules and rule 35 of the Uniform Rules of Court do not contain any provision in regard to the format in which electronic information must be produced or made available for inspection and trial. According to Van Dorsten the Magistrates Court Rules, the Uniform Rules of Court, and the Labour Court Rules do not make provision for the discovery of electronic information.[601]

Legal practitioners are sceptical to rely on electronic information as evidence because of the fact that the Magistrates' Court Rules, Labour Court Rules, and the Uniform Rules of Court do not contain explicit provisions that specifically deal with the discovery of electronic evidence as well as unlawfully obtained- and inadvertent disclosure of

598 Rule 35(15) of the Uniform Rules of Court.

599 Rule 23(16) of the Magistrates' Court Rules. The definition of 'tape recording' is wide enough to encompass all the different kinds of material on which visual images, sound and other information can be stored.

600 See Van Dorsten (n 3 above) 34-46 states that a recording is defined as a 'recorded broadcast or performance' or 'a disc or tape on which sounds, or visual images have been recorded. This focuses primarily on the storage medium instead of the electronic information itself. It would have been preferable to use the word 'stored', which in relation to information is defined to mean retained or entered 'for future electronic retrieval'

601 See Papadoulos and Snail *The law of the Internet in South Africa* (4th ed) Cyberlaw@SA IV 456 and Van Dorsten (n 3 above) 36. Van Dorsten is of the view that the Uniform Rules of Court in South Africa does not make provision for the discovery electronically stored information. In my view, the Magistrates Court Rules also falls short in this regard.

information. This lack of detailed procedures is an important part of this study into the discovery of electronic information.[602]

In the matter of *Makate v Vodacom (Pty) Ltd*.[603] Spilg J stated:[604]

> an e-document, i.e. electronic material, whether it be in the form of a communication or stored data that is retrievable through a filtering process or a data search, is discoverable under rule 35 of the Uniform Rules and that, even if it were not so, it would be open to utilise the provisions of rule 35(7) [i.e., the equivalent of magistrates' courts rule 23(7)] in order to ensure that 'the discovery process achieves its objective in the electronic age.

*In casu*, the court seems to suggest that the discovery of electronic information can be achieved within the current rules at the disposal of parties in South Africa. However, the court failed to take cognisance of the features of electronic information[605] and the cost involved especially where large volumes of information must be reviewed for privileged and recovered from backup servers or systems.[606] The court also assumed that parties would ensure that the production of electronic information will be in readable format for the requesting party.

It seems that the legal profession is divided on the issue of whether electronic information falls with the ambit of a "document" for purposes of discovery and if a "data message" and a "document" can be equated to each other.[607] The wording of section 17 of the ECTA equates a "document" to a "data message" and *vice versa*.[608] If we accept that a "data message" is the equivalent of a "document" or *vice versa,* there is very limited guidance in the ECTA or the procedural framework that judicial officers and legal practitioners can consult to navigate the terrain of this new source of evidence.[609]

---

602 See Bouwer (n 17 above) 157 and Hofman (n 17) 274.
603 2014 (1) SA 191 (GSJ) at paragraph 40. This view was supported by Judge in in *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd* ( n 418 above).
604 See *Makate v Vodacom (Pty) Ltd* ( n 45 above) at paragraph 202I–204B
605 See chapter 2.2 above.
606 See Herbstein and Van Winsen (n 2 above) 813.
607 See Discussion Paper No. 131.Project 126. "*Review of the Law of Evidence*" Electronic Evidence in Civil proceedings: Admissibility and Related Issues (31 March 2015).
608 See section 19(2) of the ECTA. This is based on the doctrine of functional equivalence that is derived from the UNCITRAL MLEC.
609 See sections 14-19 of the ECTA.

The ECTA makes provision to produce a data message:[610]

> Production of document or information
>
> 17. (1) Subject to section 28. where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information. and if-
>
> (a) considering all the relevant circumstances at the time that the data message was sent. the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and
>
> (b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference;
>
> (2) For the purposes of subsection 1, the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for-
>
> (a) the addition of any endorsement: or
>
> any immaterial change, which arises in the normal course of communication, storage or display.

Although the ECTA makes provision for the production of a "data message", it makes no provision for the discovery of metadata associated with that "data message" and the form in which the "data message" must be produced.[611] Very often the requesting party and the producing party use different software programs that may render a "data message" unreadable and the ECTA together with the Magistrates' Court Rules and the Uniform Rules of Court provides no mechanism to counter this obstacle. A requesting party will need to approach a court to request that electronic information be inspected on the producing party's servers or network that poses a new challenge of privacy and confidentiality. Further, the ECTA, Magistrates' Court Rules, and the Uniform Rules of Court are silent on the issue of information disclosed in error and the cost associated with document review. If information is inadvertently disclosed a party must approach a court for the relief sought. Neither the ECTA, nor Magistrates' Court Rules and the Uniform Rules of Court deals with the exorbitant costs associated with the production and inspection of electronic information.

---

610 See sections 17 and 14(1) (b) of the ECTA. In order to qualify as evidence in civil proceedings the original must be produced.

611 See Herbstein and Van Winsen (n 2 above) 810.

In this regard, the legislature overlooked the fact that a "data message" can be classified as real- or documentary evidence. This implies that the rules of discovery applicable to electronic information may differ depending on the fact if it is real- or documentary evidence as mentioned in chapter 2. This is one of the many examples where the legislature took a shortcut and failed to take cognisance of the procedural and evidentiary aspects that attach to evidence in electronic format.

## 6.6 CONCLUSION

The shortcomings of our procedural framework about the process of discovery in South Africa cannot be ascribed to the inherent shortcomings of the process alone but are also because the procedure in the Magistrates' Courts differs from the procedure in the High Court.

It seems that rule 23 extends further than rule 35 in regards to the discovery of electronic information. However, both rules seem to focus on the storage medium rather than the electronic information itself. This is a clear indication that we need legislative intervention to ensure that evidence in electronic form is not lost or excluded purely based on the fact that it is in digital form.[612]

An amendment to the definition of the term "document" in both the CPEA and the CPA is needed. The amended definition of the term "document" The legislature should insert the amended definition of the term "document" in the definition clauses in the Magistrates Court Rules and the Uniform Rules of Court. that is uniform with the ECTA, CPEA, and the CPA. This will ensure that all legislation in South Africa is conceptually sound and up-to-date.

612 See Papadoulos and Snail (n 601 above) 459. We need to adequately provide for discovery of electronic information as evidence.

# CHAPTER 7

# 7. CONCLUSION AND RECOMMENDATIONS

## 7.1 OVERVIEW

The challenges posed by evidence in electronic form are haunting legal practitioners and judicial officers since 1976 in South Africa.[613] Certain legislative interventions attempted to restrain this ghost with little success.[614] The use of electronic information in legal proceedings as evidence is inevitable and the justice system in South Africa needs to embrace it.[615] The increased use and flow of private and confidential information in business transactions and e-commerce led to legislative interventions to regulate the flow, use, and dissemination of information in South Africa.[616]

The increased use of digital devices and the impact of information technology globally on modern life, coupled with the capacity to accumulate and store huge volumes of electronic information have necessitated the repeal of the Computer Evidence Act and the promulgation of the ECTA, to facilitate and regulate the admissibility of electronic information as evidence in legal proceedings. The ECTA is based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.

The aim and objective of this study are to draw the attention of legal practitioners and judicial officers to the problems in practice that attaches to the discovery of electronic information as evidence in legal disputes. The need for a comprehensive overhaul of the South African procedural framework is imminent. Judicial officers are expected to use our current procedural framework and apply our traditional evidentiary rules to the digital paradigm we found ourselves in today. Of particular concern is that our procedural framework provides for the discovery of oral-, real- and documentary evidence. The question hovering on the periphery is, can we expect discovery rules

613 See *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A). SALRC reports on the review of the Law of evidence.
614 See the Computer Evidence Act 57 of 1983.
615 Swales (n 44 above) and Schwikkard 4th ed (n 16 above) 437.
616 See ECTA, RICA, POPIA, and the POSI Bill.

primarily designed to deal with paper documents to be fully functional in an ever-increasing paperless world?

The law of evidence and the procedural framework that regulates evidence, including electronic information in South Africa requires reform. In addition, given recent technological advancements, the rise, and the importance of e-commerce in South Africa, it is prudent that the South African Law Reform Commission establish a multi-disciplinary working group of individuals with various expertise to review all technology-related legislation currently in operation in South Africa.

The discovery of electronic information in the United States and the United Kingdom is well developed although the United States seems to be at the forefront.[617] Particular reference will be made to the development of the court rules applicable to the preservation and production of electronic information as evidence in the United States and the United Kingdom. This will assist me to have a clear understanding of the developed positions in the United States and the United Kingdom and if any of these developments may have an influence on the procedural framework and evidentiary rules applicable in South Africa and thus inform the dissertations' conclusion.

The South African procedural law lacks detailed procedures on the collection, storage, preservation, and production of electronic information as evidence in court.[618] Practice Directives may be introduced to supplement the court rules as was done in the United Kingdom. The emphasis should be on the importance of such procedures as it essentially deals with the chain of custody of electronic information, which will be adduced as evidence to ensure the integrity, reliability, and authenticity of the electronic evidence, even during litigation. This would provide judicial confidence regarding the treatment of electronic evidence in legal proceedings.

617 See Hollander (n 229 above) 155; Foggo, G. Grosso S., Harrison, B and Rodriguez-Barrera, J V "Comparing E-Discovery in the United States, Canada, the United Kingdom, and Mexico" Committee on Commercial & Business Law Litigation, Section of Litigation, American Bar Association (Newsletter, Vol. 8, no. 4, Summer 2007) p5. This article supports the view of Hollander that jurisprudence in regard to e-discovery is less developed in the United Kingdom.

618

Prior to the arrival of electronically generated- and electronically stored information, if one was asked to describe a "document" then one would have responded that a "document" is a piece of paper that contains written information. The definition might have included a medium other than paper, such as pauper or parchment.[619] The arrival of digital devices, backup systems, and cloud servers totally changed the landscape of what constitutes a "document".

The CPA and CPEA both contain a definition of the term "document". However, there is a disparity between the definition of the term "document" provided in the CPA and CPEA respectively. The ECTA also makes mention of the term "document". However, it does not define the term "document".

On the one hand, the ECTA refers to electronic information as "data" and in the event of dissemination thereof, it is a "data message"[620]. On the other hand, the Cybercrimes Act[621] also contains a definition of a "data message". This effectively means South Africa has two definitions for the term "data message". This disparity between the ECTA and the Cybercrimes Act should be corrected to bring about uniformity.

As a starting point, South Africa ought to ensure uniformity in regards to the definition of the term "document" in all legislation operational in South Africa. It is my view that a single definition of the term "document" must be formulated which includes electronic information to give legal certainty as to what constitutes a document in South Africa.[622] The current definitions of the term "document" in the various pieces of national legislation[623] mentioned above must be amended to echo the doctrine of functional equivalence envisaged in the ECTA. It seems that the current definitions of the term "document" provided for in the CPA and CPEA is restrictive and may exclude electronic information as evidence based on its digital nature. We need to understand what constitutes a "document" and whether the electronic presentation of information on a screen of digital devices falls within the ambit of the term "document". It is my view that

619 See Theophilopoulos (n 19 above) 461.
620 See section 1 of the ECTA.
621 See section 1 of Act 19 of 2020.
622 See the proposed new e-rules and amendments to the Uniform and Magistrates' Courts rules for the electronic civil justice system available at https://www.justice.gov.za/rules_board/comment.html.
623 See section 221 of the CPA, section of the CPEA as well as section 33 of the LEAA.

the definition of the term document must be amended as mentioned in this work and this is in line with the recent invitation to the public by the Rules Board for Courts of Law to comment on the prosed new E-Rules.[624] The proposed amendment of the term "document" as mentioned in the proposed new E-rules will cover both definitions of "data messages" in the ECTA and Cybercrimes Act but it may be viewed that two types of " data messages" exist in the South African context. Alternatively, we need to also define what an electronic document is. There appear to be no jurisprudential or academic articles or writings that define an electronic document in South Africa.

Technology-related legislation in South Africa ought to ensure that functional equivalence is achieved between traditional paper documents and documents in electronic form. Based on international practices, the doctrine of functional equivalence is essential in the digital age, to promote paperless communication that promotes efficiency and effectiveness in international trade.[625] The doctrine of functional equivalence places the printed version of a document and the electronic version thereof on the same legal footing.[626] However, it seems that the printed version of a document and the electronic version thereof is not receiving even-handed treatment in South Africa.[627]

## 7.2 RECOMMENDATIONS

I recommend that the definition of the term "document" must be amended to make terminology consistent throughout all legislation and the court rules in South Africa. The definitions of the term "document" in the CPA[628] and the CPEA[629] must be uniform. In the event, that a uniform definition for the term "document" is formulated, this definition should be included in the definition sections of the Magistrates' Court Rules, Labour Court Rules, and the Uniform Rules of Court and also in the various pieces of national legislation mentioned in this dissertation.[630] Further, the term "document" must be amended to include "data messages" as mentioned in the ECTA[631] and Cybercrimes

624 See https://www.justice.gov.za/rules_board/comment.html last accessed on 15 August 2021.
625 See http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (last accessed on 14-10-2018).
626 See Model Law (n 74 above).
627 Hofman and De Jager (n 151 above) 682.
628 See (n 22 above).
629 See (n 23 above).
630 See SALRC report ( 12 above) at paragraph 4.139 81.
631 See the definition section of Act 25 of 2005.

Act[632] and all electronic information as a subset of the term "document".[633] Based on the recent invitation of the Rules Board for Courts of Law[634] to the public to comment on their proposed amendment to the definition of the term "document", it is clear that the Rules Board is of the view that the definition of the term "document" is outdated and must be amended to stay abreast of technological advancements and ensure that legislation and court rules are synchronised.

Alternatively, as an interim measure "data messages" and electronic information should be listed as part of the items listed as discoverable under rule 23 of the Magistrates' Court, rule 6 of the Labour Court Rules, and rule 35 of the Uniform Rules of Court.[635] In addition to the aforementioned, we should consider developing a definition for an "electronic document".[636] It is evident from submissions received by the South African Law Reform Commission[637] that the traditional definition of the term "document" is out of touch with the technological advances in the legal fraternity and the business world in general. The Law Commission as part of their Project 126 drafted the Law of Evidence Bill[638] in an attempt to eliminate the shortcomings of the ECTA and other national legislation operative in South Africa that only provides definitions for the term "document" and fails to take cognisance of electronic information and "data messages".[639]

Electronic information can be classified as either real- or documentary evidence.[640] Classification of evidence, including electronic information, is necessary to determine which evidentiary rules apply to the evidence.[641] From some of the cases mentioned in chapter 5 that have dealt with electronic information as evidence, it seems that the electronic information is generally placed before courts' by way of printouts from cloud

632 See the definition section in Act 19 of 2020.
633 See for example how rule 31.4 of the CPR in the United Kingdom is worded.
634 See https://www.justice.gov.za/rules_board/comment.html accessed last on 13 August 2021.
635 See for example rule how rule 26(a) (1) (A) (ii) of the Fed.R. Civ.P in the United States is worded.
636 See CPR PD31B.
637 See SALRC report (n 12 above).
638 See SALRC report (n 12 above).
639 See SALRC report (n 12 above) 91. The Draft Bill on the Law of Evidence proposes a definition of a "document" as well as a definition for an "electronic document".
640 Schwikkard (n 16 above) 445. See *S v Brown* (n 47 above) paragraph 18. *S v Ndiki* (n 18 above) paragraph 53.
641 See *S v Ndiki* 2008 (n 18 above); *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* (n 121 above); *Ex Parte Rosch* [1998] 1 All SA 319 (W); *Ndlovu v Minister of Correctional Services* (n above 24) and *S v Brown* (n 47 above).

servers and backup systems.[642] One must take into account the aim and objective for which the evidence, including electronic information, is presented when determining whether that evidence, including electronic information is real- or documentary evidence. If evidence, including electronic information, is tendered to prove the condition of the evidence[643] or that, the actual evidence exists or something other than the contents being true, it should be treated as real evidence.[644] This will imply that the evidence, including electronic information that is presented as an object, must be "genuine and authentic" or it must be what it purports to be.[645] Evidence, including electronic information, that is tendered for the court to read or listen to it and interpret the contents of a piece of evidence, should be documentary evidence.[646] The purpose test in my view should be adequate to determine if the evidence, including electronic information is real-or documentary evidence.

Further, to this is that electronic information that is classified, as documentary evidence can also constitute hearsay evidence.[647] Courts and academics still grapple with the issue of whether electronic information constitutes hearsay evidence within the scope and ambit of the LEAA.[648] Section 15 of the ECTA is not definitive in this aspect whether a "data message" of which the probative value of the content of the "data message" depends on the testimony of a person other than the person that testifies at trial and a "data message" that depends solely on the automated processing of information by a computer.[649] According to Theophilopoulos, the aforementioned distinctions between "data messages" that are mentioned in the *Ndlovu* and *Ndiki* cases are open for interpretation and may be problematic.[650] It appears from academic literature and case law, where parties rely on electronic information as evidence, that evidence is not

642 For example, see *S v Ndiki* ( n 18 above); *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* (n 121 above);*S v Meyer* (n 112 above) para 296 – 300 and *Experian South Africa v Haynes* 2013 1 SA 135 (GSJ).

643 For example, where the document that is presented as evidence is in fact a will.

644 See *S v M* 2002 (2) SACR 411 (SCA) 432.

645 De Villiers (n 1 above) 573, see also *S v M* 2002 (2) SACR 411 (SCA) 432 where a letter was received into evidence as proof that the letter was sent by the appellant to a witness and the contents were found to be irrelevant in that instance.

646 De Villiers (n 1 above) 569.

647 See *S v Ndiki* (n 18 above) paragraph 31.

648 Hofman and De Jager (n 151 above) 766; Theophilopoulos (n 19 above) 473 – 475 and Hofman and De Jager (n 151 above) 776 – 777.

649 Theophilopoulos (n 19 above) 473-474.

650 Theophilopoulos (n 19 above) 473-474.

exempted from the rules regulating hearsay.[651] The wording and interpretation of section 15 of the ECTA in the *Ndlovu* and *Ndiki* cases are in line with international practice. However, these distinctions seem to suggest that hearsay "data messages" are admitted without being tested against the statutory limitations set out in section 3 of the LEAA, and that section 15 overrides the evidentiary rules applicable to hearsay evidence. In some instances, South African courts had to come to the rescue of the legislature as a result of the ambiguity that exists between the rules of evidence and section 15 of the ECTA.[652] This lack of cohesiveness between the LEAA, the ECTA, and the common law should be corrected to avoid contentious situations and align the South African rules of evidence and statutory provisions with international best practices.[653] Cohesion and alignment between the statutory hearsay exceptions and the exceptions created by the ECTA in regards to electronic information are necessary.[654]

In South Africa, we have multiple sources of law that deal with the admissibility of evidence. Courts can no longer hold the view that evidence must be excluded because it is new or it challenges our traditional procedural, evidentiary, and legal framework. Our traditional evidentiary rules and principles need to be adapted to stay abreast of technological advancements that will influence the effectiveness of courts and to promote efficacy and efficiency in the functioning of courts in South Africa. The ECTA is the primary legislative instrument regulating the admission of electronic information as evidence.[655] The ECTA is in certain aspects, adequate to regulate the admissibility of evidence in the form of a "data message". The ECTA, the LEAA in so far as hearsay evidence is concerned, and the CPEA, together with the CPA in the context of civil and criminal matters, the common law and evidentiary rules in South Africa should be streamlined to ensure that the admissibility of electronic information is predictable as evidence.[656]

---

651 See Swales (n 44 above) 52, S v Ndiki (n 18 above); LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd (n 121 above)and S v Meyer (n 112 above) para 296 – 300.

652 See *S v Meyer* (n 112 above) paragraph 299; *S v Brown* (n 47 above) paragraph 18; *LA Consortium* LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd (n 121 above) paragraph 19; *S v Ndiki* (n 18 above) paragraph 31 and *Ndlovu v Minister of Correctional Services* (n 24 above) at 172 – 173.

653 See Swales (n 44 above) 51 and Stanfield (n 141 above) 1.

654 See Swales (n 44 above) 76.

655 See Swales (n 44 above) 97.

656 See Hofman (n 17 above) 30.

South Africa should adopt a more inclusionary approach that is flexible[657] and technologically neutral to regulate the admissibility of electronic information and to mitigate the loss of electronic information as evidence purely due to its nature.[658] A lack of clarity on the admission of electronic information as evidence in legal proceedings is one of the biggest hurdles for adducing electronic information as evidence.[659] This uncertainty in the South African context can be remedied by way of law reform. This can be achieved with reforms to existing statutes as suggested to the definition of the term "document", the evidentiary rules, the ECTA as well as the procedural framework.[660]

When discussing evidentiary issues related to the preservation and production of evidence, including electronic information, litigants must take cognisance of the rules of evidence applicable in their respective jurisdictions to determine the admissibility of electronic information. Electronic information must de be treated as the functional equivalent of a traditional "document". In order to admit electronic information as evidence, it must satisfy the requirements of relevance, originality, authenticity, and reliability when adduced as evidence in legal proceedings first.[661] Electronic information that is relevant to any party's claim or defense and is proportional to the needs of the case must be discoverable. Given the divergence in case law, it is my view that, in the short term, the courts may be able to address the shortcomings of the procedural framework, statutory provisions, and the rules of evidence on the admissibility of electronic information[662], but in the long-term reform is needed.[663] Documents or

657 LRCI Consultation Paper 57 (2009) 72.
658 Currie RJ &Coughlan S (2010) 268.
659 See Swales (n 44 above) 76.
660 See http://www.justice.gov.za/salrc/dpapers.htm.
661 See Schwikkard and Van der Merwe (n 16 above) 50, 446; Theophilopoulos (n 19 above) 474-475, De Villiers (n 1 above) 567 and Swales (n 44 above) 13. In the matter of *Ndlovu v Minister of Correctional Services and Another* (n 24 above) 172-173 Gautschi AJ stated as follows: "Documentary evidence, in order to be admissible in evidence, generally has to comply with three rules (a) the statements contained in the document must be relevant and otherwise admissible; (b) the authenticity of the document must be proved; and (c) the original document must normally be produced". The Court allowed that a computer-generated printout in the form of a "data message" to be adduced as evidence. (n 99 above) 193; See section 210 of the CPA and section 2 of the CPEA.
662 See Swales (n 44 above) 117.
663 See *S v Brown* (n 47 above) at paragraph 18.

information in electronic form that are relevant and authentic may nevertheless be inadmissible because of the rules of evidence that apply in a specific jurisdiction.[664]

The originality rule as encapsulated in the common law is somehow diluted by the enactment of ECTA,[665] coupled with the fact that the test for authenticity and integrity of the evidence, including electronic information as set out in the ECTA, is vague and it overlaps with criteria for assessing genuineness and trustworthiness of evidence. The ECTA supports the notion that courts should ensure that evidence of electronic nature is not excluded merely on the basis that it is in electronic form.[666] Further to that, is that the test in ECTA to authenticate electronic evidence[667] seems to be vague and impractical based on the proposition that authenticity should only be considered when determining the evidential weight assigned to evidence.[668]

Authentication of electronic information should receive more attention especially if it is classified as documentary evidence.[669] The concepts of "genuine and authentic" should not be confused with the authentication of evidence, including electronic evidence.[670] The traditional originality prerequisite should be adapted to make provision for electronic information in this digital age, especially if it is the best evidence reasonably available.[671] It is clear that judicial officers have the discretion to admit evidence, including electronic information, and this may lead to a disparity between the approaches followed by courts that can cause uncertainty and may lack consistency. However, we need to tread with caution as this may go to the extent to fetter judicial discretion by over legislating.

Courts analyse facts in light of substantive laws and deliver judgments based thereon. There must be rules that regulate how disputed evidence, including electronic

664 For example, rule 803 of the Fed.R.Evid applicable in the United States, Part 33 of the CPR applicable in the United Kingdom, and section 34 of the CPEA read with section 3(1) of the LEAA applicable in South Africa.
665 See section 14 read together with section 17 of the ECTA. Theophilopoulos (n 19 above) 467.
666 See section 15(1)(b) of the ECTA.
667 See section 14(2) of the ECTA.
668 See section 15(3) of the ECTA.
669 See Fed.R. Evid
670 De Villiers (n 1 above) 573. According to De Villiers (n 2 above) 724-725 "genuine and authentic basically speaks to the character and nature of the document and does not touch on the issue whether the content is true or not." Therefore, the accuracy and reliability of the evidence are not yet at issue at the stage when you deal with the question of whether the evidence is what it purports to be.
671 Theophilipoulos (n 18 above) 467-468.

information, is gathered, retained, exchanged between parties, and admitted into evidence by courts in legal disputes.

It is apparent from the various academic works that the electronic version of a document is different from the traditional printed version of the same document.[672] The rules of evidence, procedural framework, and statutory provisions in South Africa were primarily developed around paper documents.[673] Our rules of evidence and our procedural framework in South Africa should stay abreast of technological advancements and related challenges. Proper collection, retention, management, and preservation of evidence, including electronic information and correct application of the law of evidence and our procedural rules is of utmost importance to admit evidence in court.

Preservation of evidence, including electronic information, is part of modern litigation and has become a common aspect of litigation globally.[674] The voluminous and dynamic nature of electronic information may complicate the preservation obligations of parties in cases where electronic information is adduced as evidence. In South Africa, there is little said and done about the preservation of evidence, including electronic information in legislation. The Magistrates' Court Rules, the Labour Court Rules and the Uniform Rules of Court are silent on issues of collection, preservation, and production of electronic information as evidence in legal proceedings. Coupled with the aforementioned is that the CPEA and the ECTA are not coherent on issues of collection, preservation, and production of evidence, including electronic information as evidence in legal proceedings. The collection, preservation, and production are further aggravated by the difficulties in the identification and location of electronic information.

It is evident that the South African procedural framework, the evidentiary rules, and statutory provisions are inadequate, in that it lacks detailed procedures on collection, preservation, and management of electronic information for later use in anticipated or pending litigation in line with international trends and best practices.

---

672 *The Sedona Principles, Second Edition: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (2007), https://thesedonaconference.org/download-pub/81. ("Sedona Principles Second Edition") at 60.

673 Van der Merwe "a Comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda" PER / PELJ 2014(17)1.

674 See Swales (n 44 above) 14.

Specific provisions regulating the collection, preservation, and production of evidence, including electronic information and the metadata associated with the electronic information, should be inserted into Magistrates' Court Rules, Uniform Rules of Court, and the Labour Court Rules that direct parties to have an early discovery planning meeting to discuss all issues surrounding the collection, preservation, and the production of relevant and admissible evidence, including electronic information.[675] These provisions should apply to all sorts of discoverable evidence and in particular to electronic information and its metadata. The rules of the court should explicitly state that electronic information that is relevant, not privileged, and reasonably accessible that will satisfy the parties' discovery needs must be preserved for later discovery.

In terms of the practical impacts for parties involved in litigation, the courts may be moving towards developing a 'litigation hold' approach similar to that in the United States. Litigants will need to ensure that they have systems in place to ensure that electronic information can be easily managed, retained, and made available for review upon request by the other side when litigation is pending or anticipated. It is likely to be prudent to manage and preserve this electronic information as soon as litigation is anticipated or at an early stage as soon as the factual issues are clear to avoid any sanctions by the court.

Alternatively, as an interim solution, we can introduce Practice Directives to supplement our existing procedural framework whilst we wait for legislative reforms[676] to make provision for the challenges posed by electronic information during the discovery process similar to what was done in the United Kingdom.[677] In addition, we can have an EDQ like the UK designed to assist the parties to agree on the scope and manner in which electronic disclosure is required.[678] Parties must be directed to discuss and agree with each other on the extent of a "reasonable search", and how disclosure should be

675 See Fed R. Civ. P and Fed. R. Evid in the USA and the CPR and Practice Directions that forms part of the CPR in the United Kingdom. The LSSA supports the idea that the Rules of Court must be amended. See http://www.lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf with specific reference to the Law Society of South Africa's (LSSA) submissions to the SALRC on Discussion Paper 131 on the Review of the Law of Evidence made on 29 July 2015 26-28.

676 See CPR, 1998 as amended.

677 See CPR Part 31.

678 See EDQ in Addendum C.

given. The rationale behind supplementing the procedural framework with directives is because the promulgation of legislation in South Africa is normally prolonged and protracted by parliamentary processes.[679] The process of promulgating legislation can frustrate legal practitioners and judicial officers who are faced with the preservation, retention, and discovery of electronic information as evidence on a daily basis.[680] The aforementioned possibilities can address the shortcomings in regards to retention, preservation, and management of electronic information in line with international trends and best practices.

The ECTA makes provision for the retention and production of "data messages" but deals with it dismissively.[681] The ECTA fails to take cognisance of when the duty arises to preserve and retain evidence, including electronic information. Secondly, the ECTA does not provide guidance on the scope of the duty to preserve and retain evidence, including electronic information, and if there are any consequences for a spoliator. Although the ECTA makes provision for the retention and production of "data messages", it is silent on the procedural requirements needed to avoid lackluster preservation and management of evidence, including electronic information.

Our current procedural framework, statutory provisions, and evidentiary rules in South Africa contain no provisions to ensure that evidence, including electronic information is not lost or destroyed in the normal course of business when litigation is pending or anticipated. As part of the early discovery planning meeting, parties' should find a balance between the competing needs to preserve relevant evidence, including electronic information, and to continue with routine document creation, retention, and destruction operations and outline reasonable preservation steps that will not hamper its ongoing activities.

---

679 In 1982, the SALRC released a report about "Admissibility in Civil Proceedings of Evidence Generated by Computers", Project 6, Review of the Law of Evidence (1982). Today we are still faced with the challenges that were identified in 1982. It seems that the CPEA and the CPA may assist parties to admit into evidence particular types of electronic evidence, such as trade or business records.

680 The matter of *Narlis v South African Bank of Athens* (n 613 above) was the first reported South African case that dealt with the admissibility of electronic evidence and was heard more than 25 years before the ECTA came into operation.

681 See sections 16 and 17 of the ECTA.

The normal operating procedure for computer systems involves both the routine creation and retention as well as the automatic destruction or overwriting of electronic information. If parties fail to address preservation issues when litigation is anticipated or early in the litigation process, it increases the risks of disputes over lackluster preservation of evidence, including electronic information. In South Africa, relevant and admissible evidence, including electronic information might be destroyed accidentally, wilfully or as a result of routine document destruction policies before proceedings are initiated. This calls for legislative reform in this digital age to deal with routine, accidental, and willful destruction of evidence, including electronic information.

As mentioned earlier in this text, electronic information contains embedded information referred to as metadata. The metadata associated with evidence, including electronic information, is invisible when it is printed out as a traditional paper document. Our procedural law needs to be amended to allow parties to use relevant metadata as evidence if it is admissible, and authentic under our procedural framework and evidentiary rules.[682] The amendment should consider that even metadata must be kept in the format it is used in the ordinary course of business. It is my view that we can opt for either one of the two approaches followed in the United States of the United Kingdom.

The South African procedural law and common law have certain shortfalls and are inadequate to ensure that rights contained in the Bill of Rights,[683] are not infringed during the process of the discovery of electronic information.[684] Organisations or businesses that do not have sophisticated systems or networks, still receive and disseminate significant volumes of electronic information.[685] This makes information security an important aspect of the day-to-day operations of that organisations or businesses. Retention and management of electronic information on cloud servers in electronic form make information much more vulnerable to impropriety, alteration, willful or accidental destruction. In the digital paradigm we find ourselves in, tampering with electronic information is a real risk[686] and frequent occurrence. Expertise is readily available to

682 See paragraph 28 of Practice Direction 31B of the CPR.
683 The right to privacy as embodied in the Constitution of South Africa.
684 Basdeo (n 11 above) 196.
685 Swales (n 44 above) 14.
686 Hofman and De Jager ( n 151 above) 784 and Schwikkard and Van der Merwe (n 16 above) 438.

determine if any evidence, including electronic information, is the subject of tampering and our legal framework must endorse this change.[687]

If one thinks about evidence, including electronic information that was obtained improperly or unlawfully, one would think that the evidence is inadmissible and must be barred from production in any legal disputes. However, this is not the situation in South Africa. Unlike the United States and the United Kingdom, there are no clear guidelines in South African national legislation to direct litigants on how to deal with issues related to impropriety or inadvertent disclosure of evidence, including electronic information and its metadata for that matter. In the United States and the United Kingdom, certain provisions were specifically inserted into the Fed.R.Civ.P, Fed.R.Evid[688], and the CPR[689] respectively to address the issues associated with impropriety and inadvertent disclosure without the intervention of the judiciary. In South Africa, there is a *lacuna* in the ECTA as well as the rules of court when electronic information is disclosed in error or obtained by impropriety.

In the matter of *Harvey v Niland and Others* Plasket J considered the *Fedics Group (Pty) Ltd & Another v Matus & Others as well as the Fedics Group (Pty) Ltd & Another v Murphy & Others,* judgments to determine if the same principles apply to unlawfully obtained evidence in civil and criminal matters. Plasket J stated that an accused has a right to silence and against self-incrimination. An accused person is not obliged to disclose his or her defence or to assist the state to prove its case. Thus an accused person is under no obligation to provide the prosecution authority with any documents that may strengthen its case. However, the position is different in civil proceedings. Parties in civil litigation are obligated to discover all documents and tape, electronic, digital, or other forms of recordings that may advance their adversary's case or that may damage his case. Plasket J gave his view on how the judicial discretion to allow or disallow unlawfully obtained evidence is to be exercised and stated:[690]

> "Without trying to formulate principles of general validity or rules of general application, the implications of these differences between criminal and civil proceedings in the present context are,

687 Theophilopoulos (n 19 above) 461; Hofman and De Jager (n 151 above ) 761; *Heroldt v Wills* 2013 2 SA 530 (GSJ) 8.
688 See rule 26(b) (2) (5) of the Fed.R.Civ.P.
689 See rules 31.13 and 31.19 of the CPR.
690 See *Harvey v Niland and Others* ( n 260 above).

> in my view, twofold. On the one hand, the litigant who seeks to introduce evidence which was obtained through a deliberate violation of constitutional rights will have to explain why he could not achieve justice by following the ordinary procedure, including the Anton Piller procedure, available to him. On the other hand, the Court will, in the exercise of its discretion, have regard to the type of evidence which was in fact obtained. Is it the type of evidence which could never be lawfully obtained and or introduced without the opponent's co-operation, such as privileged communications, or the recording of a tapped telephone conversation, or is it the type of evidence involved in this case, namely documents and information which the litigant would or should eventually have obtained through lawful means? In the latter case, the Court should, I think, be more inclined to exercise its discretion in favour of the litigant who seeks to introduce the evidence than it would be in the case of the former. It goes without saying that the Court will, in any event, have regard to all the other circumstances of the particular case".'

When information is obtained by impropriety or disclosed in error, confidentiality, and privacy is at issue at this stage. Courts will have to turn to the common law to determine whether to admit such evidence, including electronic information. This would require courts to determine whether the admission of such evidence, including electronic information, would render the trial unfair or otherwise be detrimental to the administration of justice.[691] If the answer to one of these legs is in the affirmative, such evidence, including electronic information must be excluded.

In essence, when a judicial officer exercises his or her discretion to exclude unlawfully obtained evidence, all relevant factors must be considered. These would include the extent to which, and how, one litigant's right to privacy (or any other right for that matter) has been encroached upon and the nature of the evidence, including electronic information concerned if the party that seeks to rely on the tainted evidence made any attempts to gain access to the evidence lawfully.

Statutes dealing with privacy, confidentiality, privilege, and the common law in South Africa that applies to relevant and admissible electronic information do not provide adequate safeguards to address impropriety and inadvertent disclosure of evidence, including electronic information and its metadata. The silence of South African statutes in regards to issues of privacy, confidentiality, and privilege where evidence, including electronic information, is unlawfully obtained or disclosed in error and adduced as

691 See Harvey v Niland (n 260 above).

evidence in legal disputes, creates uncertainty among legal practitioners and the judiciary let alone when individuals appear in person.[692] It is sometimes problematic for unrepresented parties to grasp the basic court processes, especially in civil litigation to invoke their rights. Chaskalson CJ made this comment:[693]

> Lay litigants should not be held to the same standard of accuracy, skill and precision in the presentation of their case required of lawyers.

The aforementioned may undermine the right to privacy, the right to a fair trial, and the right to access to information. Although the ECTA[694] and POPIA[695] stipulate how data handlers need to operate when handling private and confidential information of persons. Both pieces of legislation are silent on the issues of impropriety or inadvertent disclosure of information. POPIA and the ECTA may even prevent the retention and production of relevant electronic information in legal proceedings. The ECTA does not explain how privilege and confidentiality constrain the production of electronic information in "possession" or under "control" of parties in legal proceedings. This *lacuna* in the ECTA allows for the abuse of the claim of privilege when face with a discovery request and must be addressed.[696]

The Magistrates Court Rules and the Uniform Rules of Court must be amended to direct the parties to discuss issues of privilege, privacy, and confidentiality in regards to trial-preparation material at a very early stage similar to the United States or the United Kingdom respectively before production occurs.[697] This will allow parties to assert a claim of privilege if electronic information is inadvertently produced and will assist courts to determine if a waiver has occurred or not. If a party withholds information based on privilege or protection as trial-preparation material the party making the claim must do so that the requesting party can decide whether to contest the claim and the court can resolve the dispute.

692 See *S v Ndiki* (n 18 above) and *Ndlovu v Minister of Correctional Services* (n 24 above).
693 See *Xinwa & Others v Volkswagen of South Africa (Pty) Ltd* 2003(4) SA 390 (CC) at paragraph 13.
694 See sections 50 and 51 of the ECTA.
695 See chapter 3 of POPIA.
696 Theophilopoulos (n 301 above) 598.
697 See rules 16, 26, and 34 of the Fed.R.Civ.P as well as Part 31 of the CPR.

In Chapter 5 above, I referred to various court decisions where electronic information was admitted as evidence in courts in South Africa. The progressive judgments in some instances by our judiciary in instances where our procedural framework and our rules of evidence are lacking indicate that our profession is ready to embrace technological advances. In my view, our judiciary and legal practitioners in South Africa must update themselves about international best practices concerning the admissibility of evidence, including electronic information so that hindrances be avoided in litigation. It is evident from jurisprudence that our courts followed different approaches when dealing with the admittance of electronic information, as evidence. Electronic information and the challenges posed by it will not disappear and we need to embrace the technological advances to expedite and streamline our court process instead of seeing it as an obstacle.[698]

In this digital age, paper is increasingly taking a back seat compared to electronic information. The terms "document", “possession" and even "control" take on an ambiguity in the context of discovery. This raises the question of what types of electronic information fall within the ambit of the term "document" in the context of rule 23 of the Magistrates’ Court Rules, rule 6 of the Labour Court Rules, and rule 35 of the Uniform Rules of Court?

As electronic information continues to be created and stored in its “native” format which is in line with the originality requirement, it is speculated that the discovery of electronic information, as evidence will become commonplace in South Africa in the next few years. In the future, the discovery of evidence will be conducted using electronic versions of the documents, rather than hard copies and use of technology will be used to correspond with the courts to issue and file court papers, to attend to unopposed matters, postponements, and ex parte applications, rather than incurring extra expenses to appear in court.[699] Electronic documents will be able to be uploaded to the courts at

---

698 *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* (n 410 above) at paragraph 2 the court made the following remark: ‘it is …not unreasonable to expect the law to recognise such [technological] changes and accommodate [them]’.

699 See Practice Directive 1 of 2022 issued by Judge Mlambo that introduced CaseLines as well as the COVID19 Practice Directives of the South Gauteng High Court. Available at https://www.ppv.co.za/judge-presidents-practice-directive-1-of-2020/#:~:text=Practice%20Directives%20Judge%20President%20Mlambo%E2%80%99s%20first%20Practice%20Directive,High%20Courts%20with%20effect%20from%2027th%20January%202020.

the click of a button, and judges, magistrates, and legal practitioners will have access to electronic court files at their fingertips.

Information is the lifeblood of the commercial and business entities and more and more information is stored on hard drives, backup systems, and cloud servers. In most instances where commercial and business entities are served with a discovery request, more than often, they resort to their portable storage devices, backup systems, and cloud servers on which large volumes of evidence, including electronic information, are retained and stored to comply with these requests and reduce it to a printed version. In situations where parties anticipate the discovery of electronically stored information, parties should discuss issues surrounding the discovery of electronic information to avoid later difficulties.

Courts in South Africa over the past few years slowly but surely allowed electronic information to be produced as evidence[700] and even embraced the use of technology in legal proceedings[701] despite the shortcomings of our procedural framework.[702] It seems that our courts are of the view that storage devices and servers fall within the ambit of the term "document" as mentioned in rule 23 of the Magistrates' Court Rules, rule 6 of the Labour Court Rules, and rule 35 of the Uniform Rules Court and discoverable in legal proceedings.[703] It is my view that electronic media such as servers and backup drives is merely a storage facility similar to a filing cabinet full of paper documents and that the information in electronic form as a functional equivalent of the traditional document must be discoverable in legal proceedings. The cases mentioned in chapter 5 of this study that has dealt with preservation, retention, and discovery of electronic information have not provided much clarity on the issues surrounding the preservation, retention, management, and eventually the discovery of electronic information as evidence in legal proceedings.

A court may order that a storage device be discoverable[704] while recognising that it would likely contain large volumes of irrelevant, privileged, confidential, and private

700 See chapter 5 above.
701 See chapter 5 above as well as the introduction of the pilot project known as CaseLines in Gauteng.
702 See chapter 5 above.
703 See *Le Roux and Others v Viana NO and Others* (n 415 above).
704 See *Le Roux and Others v Viana NO and Others* (n 415 above).

material.[705] This will place an undue burden on the responding party to identify, screen, or mask such material for privilege or confidentially and the fact that our procedural framework and evidentiary rules are silent on inadvertent disclosure of evidence, including electronic information aggravates the situation further.

In the United States and the United Kingdom, the courts developed the law to ensure that electronic information is not lost as evidence because of its digital nature. This in turn led to the numerous amendments to the Fed.R.Civ.P and Fed.R.Evid in the United States and the CPR in the United Kingdom respectively as a direct result of the series of *Zubulake* cases in the United States and the *Digicel* case in the United Kingdom. The amendment of the Fed.R.Civ.P in the United States dealt with the restrictive nature of the term "document" and introduced an additional category of discoverable material into the equation.[706] In the United States, rule 26 and rule 34 of the Fed.R.Civ.P was amended, and electronically stored information was specifically listed as one of the items of evidence that is susceptible to discovery under the Fed.R.Civ.P.[707]

In the United Kingdom, the definition of the term "document" was amended and it stipulates that electronic information such as e-mails and other electronic communications, word-processed documents, and databases is documents and subject to disclosure.[708] In addition, the legislature in the United Kingdom introduced Practice Directions and also defined what is an "electronic document". This made it clear that an "electronic document" falls within the broader definition of the term "document" which in turn implies that electronic information is subject to disclosure in the United Kingdom.

As mentioned earlier the Rules Board for Courts of Law of the Republic of South Africa( hereinafter the Rules Board) recently came to realise that the term "document" mentioned in the CPEA and CPA can no longer be seen to exclude electronic information and proposed a new definition for the term "document". The Rules Board made the following two (2) proposals for the definitions of 'document' to be considered:

---

705 See *Le Roux and Others v Viana NO and Others* (n 415 above).

706 See Schwerha; Bagby and Esler (n 3 above) 810.

707 After the 2005 amendments section 26(a)(1)(ii) read as follows: "of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses unless the use would be solely for impeachment.

708 See rule 31.4 of the CPR as amended.

> **OPTION 1:** "document' means any written, printed, or electronic matter including data and data messages as defined in the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)"; or
>
> **OPTION 2**: "document' means any written, printed, or electronic matter including pleadings and notices and data and data messages as defined in the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)".

It is my view, that if South Africa follows the United States' approach,[709] that a new category of discoverable material namely electronic information should be inserted into the Magistrates' Court Rules, the Labour Court Rules, and the Uniform Rules of Court. This will imply that rule 23 of the Magistrates Court Rules and rule 35 of the Uniform Rules of Court need to be amended and specific provisions inserted to address issues related to the identification, collection, preservation, and discovery of electronic information.[710] It is my view that we can use Addendum A of this study as a guide to model rule 23 of the Magistrates Court Rules and rule 35 of the Uniform Rules of Court. The downside of the United States approach might be the time-lapse to promulgate and enact legislation in South Africa.

Alternatively, South Africa can follow the United Kingdom's approach in amending the term "document".[711] In Addendum B under Rule 31.4 and Practice Direction paragraph 2A.1 a model definition of the term "document" is provided that we may use as a guide. Further, Addendum B outlines the procedural framework and in particular the Practice Direction operative in the United Kingdom that may aid South Africa to deal with electronic information in courts. In addition, Practice directives can be introduced in South Africa to supplement our current procedural framework where it lacks procedures that speak to identification, collection, preservation, and eventually, the discovery of electronic information as evidence in legal proceedings, as was the case in the United Kingdom.

709 See Addendum A setting out rules 26, 34 of the Fed.R. Civ.P below.
710 See SALRC report ( n 12 above) at paragraph 4.139 on 81.
711 See Addendum B setting out Part 31 and Practice Directions 31A and 31B below.

As the position currently stands in South Africa "data messages" are discoverable as evidence under section 17 of the ECTA and the rules of court in particular rule 23 of the Magistrate's Court Rules to a limited extent make provision for the discovery of electronic information in that it stipulates that 'electronic and digital recordings' is discoverable.[712] However, the ECTA and our rules of court lack detailed procedures to ensure that parties meet their discovery obligations in regards to evidence in electronic form for foreseeable or pending litigation. This ought to change to include electronic information or "data messages" as items that must be discovered if available.[713]

The South African Law Reform Commission made mention of the challenges posed by electronic information that litigants are faced with if they wish to adduce electronic information as evidence in their possession or that of third parties or their adversaries in legal proceedings.[714] South African courts and procedural law are not fully equipped to deal with electronic information produced as evidence.[715] The Magistrates' Court Rules, as well as the Uniform Rules of Court, must also make provision for the identification, collection, preservation, and eventually, the discovery of electronic information and its metadata as soon as litigation is anticipated or when it is pending as set out in the ECTA.[716] However, the ECTA is silent on the metadata that attaches to the electronic information as well as the procedures to be followed to ensure the authenticity and integrity of the "data messages" are maintained.

We need to introduce a provision in the Magistrates Court Rules as well as the Uniform Rules of Court that direct the parties to have an early discussion on the discovery of electronic information similar to what happens in the United States[717] and the United Kingdom[718] respectively. This provision should focus and direct parties to discuss the

712 The wording of Rule 23 (1) See Rule 23(16) of the Magistrates Court Rules and Rule 35(15) of the Uniform Rules of Court refers to the definition of a tape recording. However, Rule 23 and Rule 35 do not provide proper guidance on how to deal with this type of evidence.
713 See SALRC report ( n 12 above) paragraph 4.139 on 81.
714 See SALRC Issue Paper report (n 59 above). This issue received further attention in SALRC report (n 12 above) wherein the Law Commissionproposed the Law of Evidence Bill.
715 See Hughes and Stander (n 67 above) 61.
716 See section 16 of the ECTA.
717 See rule 16 and 26 of the Fed.R.Civ.P in the United States.
718 For example, the mandatory CMC that parties must attend in the United Kingdom.

form in which electronically stored information should be preserved and retained and later produced as evidence.[719]

Further to that, a requesting party must specify the form in which it wants electronic information to be discovered. If the requesting party does not specify a form, the responding party should state the form in which it intends to use electronic information in the proceedings. This will enable parties to determine what form of discovery will meet both parties' needs to curb the cost of retrieving or restoring electronic information and to fast-track searches for responsive electronic information. In situations where parties anticipate the discovery of electronically stored information, parties should discuss issues surrounding the discovery of electronic information to avoid later difficulties.

Parties need to tailor their early discovery discussion to the specifics of the given case at hand. For example, the parties may specify the search topics, methods of searches, and the period for which discovery will be sought. Parties may identify the sources of reasonably accessible information within a party's possession or under his or her control that should be searched for responsive electronically stored information, including the cost involved in retrieving and reviewing the information.

719 See rule 16 of the Fed.R. Civ.P in the United States and the mandatory CMC that parties must attend in the United Kingdom.

**ADDENDUM A**

**RULE 26 OF THE FEDERAL RULES OF CIVIL PROCEDURE IN THE UNITED STATES**

(a) Required Disclosures.

(1) Initial Disclosure.

(A) In General. Except as exempted by Rule 26(a)(1)(B) or as otherwise stipulated or ordered by the court, a party must, without awaiting a discovery request, provide to the other parties:

(i) the name and, if known, the address and telephone number of each individual likely to have discoverable information—along with the subjects of that information—that the disclosing party may use to support its claims or defenses, unless the use would be solely for impeachment;

(ii) a copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment;

(iii) a computation of each category of damages claimed by the disclosing party—who must also make available for inspection and copying as under Rule 34 the documents or other evidentiary material, unless privileged or protected from disclosure, on which each computation is based, including materials bearing on the nature and extent of injuries suffered; and

(iv) for inspection and copying as under Rule 34, any insurance agreement under which an insurance business may be liable to satisfy all or part of a possible judgment in the action or to indemnify or reimburse for payments made to satisfy the judgment.

(B) Proceedings Exempt from Initial Disclosure. The following proceedings are exempt from initial disclosure:

(i) an action for review on an administrative record;

(ii) a forfeiture action in rem arising from a federal statute;

(iii) a petition for habeas corpus or any other proceeding to challenge a criminal conviction or sentence;

(iv) an action brought without an attorney by a person in the custody of the United States, a state, or a state subdivision;

(v) an action to enforce or quash an administrative summons or subpoena;

(vi) an action by the United States to recover benefit payments;

(vii) an action by the United States to collect on a student loan guaranteed by the United States;

(viii) a proceeding ancillary to a proceeding in another court; and

(ix) an action to enforce an arbitration award.

(C) Time for Initial Disclosures—

In General. A party must make the initial disclosures at or within 14 days after the parties' Rule 26(f) conference unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in this action and states the objection in the proposed discovery plan. In ruling on the objection, the court must determine what disclosures, if any, are to be made and must set the time for disclosure.

(D) Time for Initial Disclosures—For Parties Served or Joined Later. A party that is first served or otherwise joined after the Rule 26(f) conference must make the initial disclosures within 30 days after being served or joined, unless a different time is set by stipulation or court order.

(E) Basis for Initial Disclosure; Unacceptable Excuses. A party must make its initial disclosures based on the information then reasonably available to it. A party is not excused from making its disclosures because it has not fully investigated the case or because it challenges the sufficiency of another party's disclosures or because another party has not made its disclosures.

(2) Disclosure of Expert Testimony.

(A) In General. In addition to the disclosures required by Rule 26(a)(1), a party must disclose to the other parties the identity of any witness it may use at trial to present evidence under Federal Rule of Evidence 702, 703, or 705.

(B) Witnesses Who Must Provide a Written Report. Unless otherwise stipulated or ordered by the court, this disclosure must be accompanied by a written report—prepared and signed by the witness—if the witness is one retained or specially employed to provide expert testimony in the case or one whose

duties as the party's employee regularly involve giving expert testimony. The report must contain:

(i) a complete statement of all opinions the witness will express and the basis and reasons for them;

(ii) the facts or data considered by the witness in forming them;

(iii) any exhibits that will be used to summarize or support them;

(iv) the witness's qualifications, including a list of all publications authored in the previous 10 years;

(v) a list of all other cases in which, during the previous 4 years, the witness testified as an expert at trial or by deposition; and

(vi) a statement of the compensation to be paid for the study and testimony in the case.

(C) Witnesses Who Do Not Provide a Written Report. Unless otherwise stipulated or ordered by the court, if the witness is not required to provide a written report, this disclosure must state:

(i) the subject matter on which the witness is expected to present evidence under Federal Rule of Evidence 702, 703, or 705; and

(ii) a summary of the facts and opinions to which the witness is expected to testify.

(D) Time to Disclose Expert Testimony.

A party must make these disclosures at the times and in the sequence that the court orders. Absent a stipulation or a court order, the disclosures must be made:

(i) at least 90 days before the date set for trial or for the case to be ready for trial; or

(ii) if the evidence is intended solely to contradict or rebut evidence on the same subject matter identified by another party under Rule 26(a)(2)(B) or (C), within 30 days after the other party's disclosure.

(E) Supplementing the Disclosure.

The parties must supplement these disclosures when required under Rule 26(e).

(3) Pretrial Disclosures.

(A) In General. In addition to the disclosures required by Rule 26(a)(1) and (2), a party must provide to the other parties and promptly file the following information about the evidence that it may present at trial other than solely for impeachment:

(i) the name and, if not previously provided, the address and telephone number of each witness—separately identifying those the party expects to present and those it may call if the need arises;

(ii) the designation of those witnesses whose testimony the party expects to present by deposition and, if not taken stenographically, a transcript of the pertinent parts of the deposition; and

(iii) an identification of each document or other exhibit, including summaries of other evidence—separately identifying those items the party expects to offer and those it may offer if the need arises.

(B) Time for Pretrial Disclosures; Objections.

Unless the court orders otherwise, these disclosures must be made at least 30 days before trial. Within 14 days after they are made, unless the court sets a different time, a party may serve and promptly file a list of the following objections: any objections to the use under Rule 32(a) of a deposition designated by another party under Rule 26(a)(3)(A)(ii); and any objection, together with the grounds for it, that may be made to the admissibility of materials identified under Rule 26(a)(3)(A)(iii). An objection not so made—except for one under Federal Rule of Evidence 402 or 403—is waived unless excused by the court for good cause.

(4) Form of Disclosures.

Unless the court orders otherwise, all disclosures under Rule 26(a) must be in writing, signed, and served.

(b) Discovery Scope and Limits.

(1) Scope in General.

Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

(2) Limitations on Frequency and Extent.

(A) When Permitted. By order, the court may alter the limits in these rules on the number of depositions and interrogatories or on the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

(B) Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(C) When Required.

On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

(ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or

(iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1).

(3) Trial Preparation: Materials.

(A) Documents and Tangible Things. Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent). But, subject to Rule 26(b)(4), those materials may be discovered if:

(i) they are otherwise discoverable under Rule 26(b)(1); and

(ii) the party shows that it has a substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.

(B) Protection Against Disclosure.

If the court orders discovery of those materials, it must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation.

(C) Previous Statement.

Any party or other person may, on request and without the required showing, obtain the person's own previous statement about the action or its subject matter. If the request is refused, the person may move for a court order, and Rule 37(a)(5) applies to the award of expenses. A previous statement is either:

(i) a written statement that the person has signed or otherwise adopted or approved; or

(ii) a contemporaneous stenographic, mechanical, electrical, or other recording—or a transcription of it—that recites substantially verbatim the person's oral statement.

(4) Trial Preparation: Experts.

(A) Deposition of an Expert Who May Testify. A party may depose any person who has been identified as an expert whose opinions may be presented at trial. If Rule 26(a)(2)(B) requires a report from the expert, the deposition may be conducted only after the report is provided.

(B) Trial-Preparation Protection for Draft Reports or Disclosures. Rules 26(b)(3)(A) and (B) protect drafts of any report or disclosure required under Rule 26(a)(2), regardless of the form in which the draft is recorded.

(C) Trial-Preparation Protection for Communications Between a Party's Attorney and Expert Witnesses. Rules 26(b)(3)(A) and (B) protect communications between the party's attorney and any witness required to provide a report under Rule 26(a)(2)(B), regardless of the form of the communications, except to the extent that the communications:

(i) relates to compensation for the expert's study or testimony;

(ii) identify facts or data that the party's attorney provided and that the expert considered in forming the opinions to be expressed; or

(iii) identify assumptions that the party's attorney provided and that the expert relied on in forming the opinions to be expressed.

(D) Expert Employed Only for Trial Preparation. Ordinarily, a party may not, by interrogatories or deposition, discover facts known or opinions held by an expert who has been retained or specially employed by another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial. But a party may do so only:

(i) as provided in Rule 35(b); or

(ii) on showing exceptional circumstances under which it is impracticable for the party to obtain facts or opinions on the same subject by other means.

(E) Payment. Unless manifest injustice would result, the court must require that the party seeking discovery:

(i) pay the expert a reasonable fee for time spent in responding to discovery under Rule 26(b)(4)(A) or (D); and

(ii) for discovery under (D), also pay the other party a fair portion of the fees and expenses it reasonably incurred in obtaining the expert's facts and opinions.

(5) Claiming Privilege or Protecting Trial-Preparation Materials.

(A) Information Withheld.

When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must:

(i) expressly make the claim; and

(ii) describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.

(B) Information Produced.

If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.

(c) Protective Orders.

(1) In General. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

(A) forbidding the disclosure or discovery;

(B) specifying terms, including time and place or the allocation of expenses, for the disclosure or discovery;

(C) prescribing a discovery method other than the one selected by the party seeking discovery;

(D) forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters;

(E) designating the persons who may be present while the discovery is conducted;

(F) requiring that a deposition be sealed and opened only on court order;

(G) requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way; and

(H) requiring that the parties simultaneously file specified documents or information in sealed envelopes, to be opened as the court directs.

(2) Ordering Discovery. If a motion for a protective order is wholly or partly denied, the court may, on just terms, order that any party or person provide or permit discovery.

(3) Awarding Expenses. Rule 37(a)(5) applies to the award of expenses.

(d) Timing and Sequence of Discovery.

(1) Timing. A party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order.

(2) Early Rule 34 Requests.

(A) Time to Deliver. More than 21 days after the summons and complaint are served on a party, a request under Rule 34 may be delivered:

(i) to that party by any other party, and

(ii) by that party to any plaintiff or to any other party that has been served.

(B) When Considered Served. The request is considered to have been served at the first Rule 26(f) conference.

(3) Sequence. Unless the parties stipulate or the court orders otherwise for the parties' and witnesses' convenience and in the interests of justice:
(A) methods of discovery may be used in any sequence; and
(B) discovery by one party does not require any other party to delay its discovery.

(e) Supplementing Disclosures and Responses.
(1) In General. A party who has made a disclosure under Rule 26(a)—or who has responded to an interrogatory, request for production, or request for admission—must supplement or correct its disclosure or response:
(A) in a timely manner if the party learns that in some material respect the disclosure or response is incomplete or incorrect, and if the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing; or
(B) as ordered by the court.

(2) Expert Witness. For an expert whose report must be disclosed under Rule 26(a)(2)(B), the party's duty to supplement extends both to information included in the report and to information given during the expert's deposition. Any additions or changes to this information must be disclosed by the time the party's pretrial disclosures under Rule 26(a)(3) are due.

(f) Conference of the Parties; Planning for Discovery.
(1) Conference Timing. Except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B) or when the court orders otherwise, the parties must confer as soon as practicable—and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b).
(2) Conference Content; Parties' Responsibilities. In conferring, the parties must consider the nature and basis of their claims and defenses and the possibilities for promptly settling or resolving the case; make or arrange for the disclosures required by Rule 26(a)(1); discuss any issues about

preserving discoverable information; and develop a proposed discovery plan. The attorneys of record and all unrepresented parties that have appeared in the case are jointly responsible for arranging the conference, for attempting in good faith to agree on the proposed discovery plan, and for submitting to the court within 14 days after the conference a written report outlining the plan. The court may order the parties or attorneys to attend the conference in person.

(3) Discovery Plan. A discovery plan must state the parties' views and proposals on:

(A) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement of when initial disclosures were made or will be made;

(B) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues;

(C) any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;

(D) any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502;

(E) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and

(F) any other orders that the court should issue under Rule 26(c) or under Rule 16(b) and (c).

(4) Expedited Schedule. If necessary to comply with its expedited schedule for Rule 16(b) conferences, a court may by local rule:

(A) require the parties' conference to occur less than 21 days before the scheduling conference is held or a scheduling order is due under Rule 16(b); and

(B) require the written report outlining the discovery plan to be filed less than 14 days after the parties' conference, or excuse the parties from submitting a written report and permit them to report orally on their discovery plan at Rule 16(b) conference.

(g) Signing Disclosures and Discovery Requests, Responses, and Objections.

(1) Signature Required; Effect of Signature. Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name—or by the party personally, if unrepresented—and must state the signer's address, e-mail address, and telephone number. By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

(A) with respect to a disclosure, it is complete and correct as of the time it is made; and

(B) with respect to a discovery request, response, or objection, it is:

(i) consistent with these rules and warranted by existing law or by a non-frivolous argument for extending, modifying, or reversing existing law, or for establishing new law;

(ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and

(iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.

(2) Failure to Sign.

Other parties have no duty to act on an unsigned disclosure, request, response, or objection until it is signed, and the court must strike it unless a signature is promptly supplied after the omission is called to the attorney's or party's attention.

(3) Sanction for Improper Certification.

If a certification violates this rule without substantial justification, the court, on motion or on its own, must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both. The sanction may include an order to pay the reasonable expenses, including attorney's fees, caused by the violation.

**RULE 34 OF THE FEDERAL RULES OF CIVIL PROCEDURE IN THE UNITED STATES**

(a) In General. A party may serve on any other party a request within the scope of Rule 26(b):

(1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:

(A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or

(B) any designated tangible things; or

(2) to permit entry onto designated land or other property possessed or controlled by the responding party, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

(b) Procedure.

(1) Contents of the Request. The request:

(A) must describe with reasonable particularity each item or category of items to be inspected;

(B) must specify a reasonable time, place, and manner for the inspection and for performing the related acts; and

(C) may specify the form or forms in which electronically stored information is to be produced.

(2) Responses and Objections.

(A) Time to Respond.

The party to whom the request is directed must respond in writing within 30 days after being served or—if the request was delivered under Rule 26(d)(2)—within 30 days after the parties' first Rule 26(f) conference. A shorter or longer time may be stipulated to under Rule 29 or be ordered by the court.

(B) Responding to Each Item.

For each item or category, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.

(C) Objections.

An objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.

(D) Responding to a Request for Production of Electronically Stored Information.

The response may state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form—or if no form was specified in the request—the party must state the form or forms it intends to use.

(E) Producing the Documents or Electronically Stored Information.

Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

(i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;

(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and

(iii) A party need not produce the same electronically stored information in more than one form.

## ADDENDUM B CIVIL PROCEDURE RULES (UNITED KINGDOM)

## PART 31 - DISCLOSURE AND INSPECTION OF DOCUMENTS

**Scope of this Part**

**31.1**

(1) This Part sets out rules about the disclosure and inspection of documents.

(2) This Part applies to all claims except a claim on the small claims track.

**Meaning of disclosure**

**31.2** A party discloses a document by stating that the document exists or has existed.

**Right of inspection of a disclosed document**

**31.3**

(1) A party to whom a document has been disclosed has a right to inspect that document except where –

(a) the document is no longer in the control of the party who disclosed it;

(b) the party disclosing the document has a right or a duty to withhold inspection of it;

(c) paragraph (2) applies; or

(d) rule 78.26 applies.

(Rule 31.8 sets out when a document is in the control of a party)

(Rule 31.19 sets out the procedure for claiming a right or duty to withhold inspection)

(Rule 78.26 contains rules in relation to the disclosure and inspection of evidence arising out of mediation of certain cross-border disputes.)

(2) Where a party considers that it would be disproportionate to the issues in the case to permit inspection of documents within a category or class of document disclosed under rule 31.6(b) –

(a) he is not required to permit inspection of documents within that category or class; but

(b) he must state in his disclosure statement that inspection of those documents will not be permitted on the grounds that to do so would be disproportionate.

(Rule 31.6 provides for standard disclosure)

(Rule 31.10 makes provision for a disclosure statement)

(Rule 31.12 provides for a party to apply for an order for specific inspection of documents)

**Meaning of document**

**31.4** In this Part –

'document' means anything in which information of any description is recorded; and

'copy', in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.

**Disclosure**

**31.5**

(1) In all claims to which rule 31.5(2) does not apply –

(a) an order to give disclosure is an order to give standard disclosure unless the court directs otherwise;

(b) the court may dispense with or limit standard disclosure; and

(c) the parties may agree in writing to dispense with or to limit standard disclosure.

(2) Unless the court otherwise orders, paragraphs (3) to (8) apply to all multi-track claims, other than those which include a claim for personal injuries.

(3) Not less than 14 days before the first case management conference each party must file and serve a report verified by a statement of truth, which –

(a) describes briefly what documents exist or may exist that are or may be relevant to the matters in issue in the case;

(b) describes where and with whom those documents are or may be located;

(c) in the case of electronic documents, describes how those documents are stored;

(d) estimates the broad range of costs that could be involved in giving standard disclosure in the case, including the costs of searching for and disclosing any electronically stored documents; and

(e) states which of the directions under paragraphs (7) or (8) are to be sought.

(4) In cases where the Electronic Documents Questionnaire has been exchanged, the Questionnaire should be filed with the report required by paragraph (3).

(5) Not less than seven days before the first case management conference, and on any other occasion as the court may direct, the parties must, at a meeting or by telephone, discuss and seek to agree a proposal in relation to disclosure that meets the overriding objective.

(6) If –

(a) the parties agree proposals for the scope of disclosure; and

(b) the court considers that the proposals are appropriate in all the circumstances,

the court may approve them without a hearing and give directions in the terms proposed.

(7) At the first or any subsequent case management conference, the court will decide, having regard to the overriding objective and the need to limit disclosure to that which is necessary to deal with the case justly, which of the following orders to make in relation to disclosure –

(a) an order dispensing with disclosure;

(b) an order that a party disclose the documents on which it relies, and at the same time request any specific disclosure it requires from any other party;

(c) an order that directs, where practicable, the disclosure to be given by each party on an issue by issue basis;

(d) an order that each party disclose any documents which it is reasonable to suppose may contain information which enables that party to advance its own case or to damage that of any other party, or which leads to an enquiry which has either of those consequences;

(e) an order that a party give standard disclosure;

(f) any other order in relation to disclosure that the court considers appropriate.

(8) The court may at any point give directions as to how disclosure is to be given, and in particular –

(a) what searches are to be undertaken, of where, for what, in respect of which time periods and by whom and the extent of any search for electronically stored documents;

(b) whether lists of documents are required;

(c) how and when the disclosure statement is to be given;

(d) in what format documents are to be disclosed (and whether any identification is required);

(e) what is required in relation to documents that once existed but no longer exist; and

(f) whether disclosure shall take place in stages.

(9) To the extent that the documents to be disclosed are electronic, the provisions of Practice Direction 31B – Disclosure of Electronic Documents will apply in addition to paragraphs (3) to (8).

**Standard disclosure – what documents are to be disclosed**

**31.6** Standard disclosure requires a party to disclose only–

(a) the documents on which he relies; and

(b) the documents which –

(i) adversely affect his own case;

(ii) adversely affect another party's case; or

(iii) support another party's case; and

(c) the documents which he is required to disclose by a relevant practice direction.

**Duty of search**

**31.7**

(1) When giving standard disclosure, a party is required to make a reasonable search for documents falling within rule 31.6(b) or (c).

(2) The factors relevant in deciding the reasonableness of a search include the following –

(a) the number of documents involved;

(b) the nature and complexity of the proceedings;

(c) the ease and expense of retrieval of any particular document; and

(d) the significance of any document which is likely to be located during the search.

(3) Where a party has not searched for a category or class of document on the grounds that to do so would be unreasonable, he must state this in his disclosure statement and identify the category or class of document.

(Rule 31.10 makes provision for a disclosure statement)

**Duty of disclosure limited to documents which are or have been in a party's control**

**31.8**

(1) A party's duty to disclose documents is limited to documents which are or have been in his control.

(2) For this purpose a party has or has had a document in his control if –

(a) it is or was in his physical possession;

(b) he has or has had a right to possession of it; or

(c) he has or has had a right to inspect or take copies of it.

**Disclosure of copies**

**31.9**

(1) A party need not disclose more than one copy of a document.

(2) A copy of a document that contains a modification, obliteration or other marking or feature –

(a) on which a party intends to rely; or

(b) which adversely affects his own case or another party's case or supports another party's case; shall be treated as a separate document.

(Rule 31.4 sets out the meaning of a copy of a document)

**Procedure for standard disclosure**

**31.10**

(1) The procedure for standard disclosure is as follows.

(2) Each party must make and serve on every other party, a list of documents in the relevant practice form.

(3) The list must identify the documents in a convenient order and manner and as concisely as possible.

(4) The list must indicate –

(a) those documents in respect of which the party claims a right or duty to withhold inspection; and

(b)

(i) those documents which are no longer in the party's control; and

(ii) what has happened to those documents.

(Rule 31.19 (3) and (4) require a statement in the list of documents relating to any documents inspection of which a person claims he has a right or duty to withhold)

(5) The list must include a disclosure statement.

(6) A disclosure statement is a statement made by the party disclosing the documents –

(a) setting out the extent of the search that has been made to locate documents which he is required to disclose;

(b) certifying that he understands the duty to disclose documents; and

(c) certifying that to the best of his knowledge he has carried out that duty.

(7) Where the party making the disclosure statement is a company, firm, association or other organisation, the statement must also–

(a) identify the person making the statement; and

(b) explain why he is considered an appropriate person to make the statement.

(8) The parties may agree in writing –

(a) to disclose documents without making a list; and

(b) to disclose documents without the disclosing party making a disclosure statement.

(9) A disclosure statement may be made by a person who is not a party where this is permitted by a relevant practice direction.

**Duty of disclosure continues during proceedings**

**31.11**

(1) Any duty of disclosure continues until the proceedings are concluded.

(2) If documents to which that duty extends come to a party's notice at any time during the proceedings, he must immediately notify every other party.

**Specific disclosure or inspection**

**31.12**

(1) The court may make an order for specific disclosure or specific inspection.

(2) An order for specific disclosure is an order that a party must do one or more of the following things –

(a) disclose documents or classes of documents specified in the order;

(b) carry out a search to the extent stated in the order;

(c) disclose any documents located as a result of that search.

(3) An order for specific inspection is an order that a party permit inspection of a document referred to in rule 31.3(2).

(Rule 31.3(2) allows a party to state in his disclosure statement that he will not permit inspection of a document on the grounds that it would be disproportionate to do so)

(Rule 78.26 contains rules in relation to the disclosure and inspection of evidence arising out of mediation of certain cross-border disputes.)

**Disclosure in stages**

**31.13** The parties may agree in writing, or the court may direct, that disclosure or inspection or both shall take place in stages.

**Documents referred to in statements of case etc.**

**31.14**

(1) A party may inspect a document mentioned in –

(a) a statement of case;

(b) a witness statement;

(c) a witness summary; or

(d) an affidavit

(e) Revoked.

(2) Subject to rule 35.10(4), a party may apply for an order for inspection of any document mentioned in an expert's report which has not already been disclosed in the proceedings.

(Rule 35.10(4) makes provision in relation to instructions referred to in an expert's report)

**Inspection and copying of documents**

**31.15** Where a party has a right to inspect a document–

(a) that party must give the party who disclosed the document written notice of his wish to inspect it;

(b) the party who disclosed the document must permit inspection not more than 7 days after the date on which he received the notice; and

(c) that party may request a copy of the document and, if he also undertakes to pay reasonable copying costs, the party who disclosed the document must supply him with a copy not more than 7 days after the date on which he received the request.

(Rule 31.3 and 31.14 deal with the right of a party to inspect a document)

**Disclosure before proceedings start**

**31.16**

(1) This rule applies where an application is made to the court under any Act for disclosure before proceedings have started[1].

(2) The application must be supported by evidence.

(3) The court may make an order under this rule only where–

(a) the respondent is likely to be a party to subsequent proceedings;

(b) the applicant is also likely to be a party to those proceedings;

(c) if proceedings had started, the respondent's duty by way of standard disclosure, set out in rule 31.6, would extend to the documents or classes of documents of which the applicant seeks disclosure; and

(d) disclosure before proceedings have started is desirable in order to –

(i) dispose fairly of the anticipated proceedings;

(ii) assist the dispute to be resolved without proceedings; or

(iii) save costs.

(4) An order under this rule must –

(a) specify the documents or the classes of documents which the respondent must disclose; and

(b) require him, when making disclosure, to specify any of those documents –

(i) which are no longer in his control; or

(ii) in respect of which he claims a right or duty to withhold inspection.

(5) Such an order may –

(a) require the respondent to indicate what has happened to any documents which are no longer in his control; and

(b) specify the time and place for disclosure and inspection.

(Rule 78.26 contains rules in relation to the disclosure and inspection of evidence arising out of mediation of certain cross-border disputes.)

**Orders for disclosure against a person not a party**

**31.17**

(1) This rule applies where an application is made to the court under any Act for disclosure by a person who is not a party to the proceedings.

(2) The application must be supported by evidence.

(3) The court may make an order under this rule only where–

(a) the documents of which disclosure is sought are likely to support the case of the applicant or adversely affect the case of one of the other parties to the proceedings; and

(b) disclosure is necessary in order to dispose fairly of the claim or to save costs.

(4) An order under this rule must –

(a) specify the documents or the classes of documents which the respondent must disclose; and

(b) require the respondent, when making disclosure, to specify any of those documents –

(i) which are no longer in his control; or

(ii) in respect of which he claims a right or duty to withhold inspection.

(5) Such an order may –

(a) require the respondent to indicate what has happened to any documents which are no longer in his control; and

(b) specify the time and place for disclosure and inspection.

Rule 78.26 contains rules in relation to the disclosure and inspection of evidence arising out of mediation of certain cross-border disputes.)

**Rules not to limit other powers of the court to order disclosure**

**31.18** Rules 31.16 and 31.17 do not limit any other power which the court may have to order –

(a) disclosure before proceedings have started; and

(b) disclosure against a person who is not a party to proceedings.

**Claim to withhold inspection or disclosure of a document**

**31.19**

(1) A person may apply, without notice, for an order permitting him to withhold disclosure of a document on the ground that disclosure would damage the public interest.

(2) Unless the court orders otherwise, an order of the court under paragraph (1) –

(a) must not be served on any other person; and

(b) must not be open to inspection by any person.

(3) A person who wishes to claim that he has a right or a duty to withhold inspection of a document, or part of a document, must state in writing –

(a) that he has such a right or duty; and

(b) the grounds on which he claims that right or duty.

(4) The statement referred to in paragraph (3) must be made–

(a) in the list in which the document is disclosed; or

(b) if there is no list, to the person wishing to inspect the document.

(5) A party may apply to the court to decide whether a claim made under paragraph (3) should be upheld.

(6) For the purpose of deciding an application under paragraph (1) (application to withhold disclosure) or paragraph (3) (claim to withhold inspection) the court may –

(a) require the person seeking to withhold disclosure or inspection of a document to produce that document to the court; and

(b) invite any person, whether or not a party, to make representations.

(7) An application under paragraph (1) or paragraph (5) must be supported by evidence.

(8) This Part does not affect any rule of law which permits or requires a document to be withheld from disclosure or inspection on the ground that its disclosure or inspection would damage the public interest.

**Restriction on use of a privileged document inspection of which has been inadvertently allowed**

**31.20** Where a party inadvertently allows a privileged document to be inspected, the party who has inspected the document may use it or its contents only with the permission of the court.

**Consequence of failure to disclose documents or permit inspection**

**31.21** A party may not rely on any document which he fails to disclose or in respect of which he fails to permit inspection unless the court gives permission.

**Subsequent use of disclosed documents and completed Electronic Documents Questionnaires**

**31.22**

(1) A party to whom a document has been disclosed may use the document only for the purpose of the proceedings in which it is disclosed, except where –

(a) the document has been read to or by the court, or referred to, at a hearing which has been held in public;

(b) the court gives permission; or

(c) the party who disclosed the document and the person to whom the document belongs agree.

(2) The court may make an order restricting or prohibiting the use of a document which has been disclosed, even where the document has been read to or by the court, or referred to, at a hearing which has been held in public.

(3) An application for such an order may be made –

(a) by a party; or

(b) by any person to whom the document belongs.

(4) For the purpose of this rule, an Electronic Documents Questionnaire which has been completed and served by another party pursuant to Practice Direction 31B is to be treated as if it is a document which has been disclosed.

**False disclosure statements**

**31.23**

(1) Proceedings for contempt of court may be brought against a person if he makes, or causes to be made, a false disclosure statement, without an honest belief in its truth.

(Section 6 of Part 81 contains provisions in relation to committal for making a false disclosure statement.)

# PRACTICE DIRECTION 31A – DISCLOSURE AND INSPECTION

**This Practice Direction supplements CPR Part 31**



## General

**1.1** The normal order for disclosure will be an order that the parties give standard disclosure.

**1.2** In order to give standard disclosure the disclosing party must make a reasonable search for documents falling within the paragraphs of rule 31.6.

**1.3** Having made the search the disclosing party must (unless rule 31.10(8) applies) make a list of the documents of whose existence the party is aware that fall within those paragraphs and which are or have been in the party's control (see rule 31.8).

**1.4** The obligations imposed by an order for standard disclosure may be dispensed with or limited either by the court or by written agreement between the parties. Any such written agreement should be lodged with the court.

## The search

**2** The extent of the search which must be made will depend upon the circumstances of the case including, in particular, the factors referred to in rule 31.7(2). The parties should bear in mind the overriding principle of proportionality (see rule 1.1(2)(c)). It may, for example, be reasonable to decide not to search for documents coming into existence before some particular date, or to limit the search to documents in some particular place or places, or to documents falling into particular categories.

## Electronic disclosure

**2A.1** Rule 31.4 contains a broad definition of a document. This extends to electronic documents, including e-mail and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been 'deleted'. It also extends to additional information stored and associated with electronic documents known as metadata.

**2A.2** Practice Direction 31B contains additional provisions in relation to the disclosure of electronic documents in cases that are likely to be allocated to the multi-track.

**The list**

**3.1** The list should be in Form N265.

**3.2** In order to comply with rule 31.10(3) it will normally be necessary to list the documents in date order, to number them consecutively and to give each a concise description (e.g. letter, claimant to defendant). Where there is a large number of documents all falling into a particular category the disclosing party may list those documents as a category rather than individually e.g. 50 bank statements relating to account number _ at _ Bank, _20_ to _20_; or, 35 letters passing between _ and _ between _20_ and _20_.

**3.3** The obligations imposed by an order for disclosure will continue until the proceedings come to an end. If, after a list of documents has been prepared and served, the existence of further documents to which the order applies comes to the attention of the disclosing party, the party must prepare and serve a supplemental list.

**Disclosure statement**

**4.1** A list of documents must (unless rule 31.10(8)(b) applies) contain a disclosure statement complying with rule 31.10. The form of disclosure statement is set out in the Annex to this practice direction.

**4.2** The disclosure statement should:

(1) expressly state that the disclosing party believes the extent of the search to have been reasonable in all the circumstances, and

(2) in setting out the extent of the search (see rule 31.10(6)) draw attention to any particular limitations on the extent of the search which were adopted for proportionality reasons and give the reasons why the limitations were adopted, e.g.

the difficulty or expense that a search not subject to those limitations would have entailed or the marginal relevance of categories of documents omitted from the search.

**4.3** Where rule 31.10(7) applies, the details given in the disclosure statement about the person making the statement must include his name and address and the office or position he holds in the disclosing party or the basis upon which he makes the statement on behalf of the party.

**4.4** If the disclosing party has a legal representative acting for him, the legal representative must endeavour to ensure that the person making the disclosure statement (whether the disclosing party or, in a case to which rule 31.10(7) applies, some other person) understands the duty of disclosure under Part 31.

**4.5** If the disclosing party wishes to claim that he has a right or duty to withhold a document, or part of a document, in his list of documents from inspection (see rule 31.19(3)), he must state in writing:

(1) that he has such a right or duty, and

(2) the grounds on which he claims that right or duty.

**4.6** The statement referred to in paragraph 4.5 above should normally be included in the disclosure statement and must indicate the document, or part of a document, to which the claim relates.

**4.7** An insurer or the Motor Insurers' Bureau may sign a disclosure statement on behalf of a party where the insurer or the Motor Insurers' Bureau has a financial interest in the result of proceedings brought wholly or partially by or against that party. Rule 31.10(7) and paragraph 4.3 above shall apply to the insurer or the Motor Insurers' Bureau making such a statement.

**Specific disclosure**

**5.1** If a party believes that the disclosure of documents given by a disclosing party is inadequate he may make an application for an order for specific disclosure (see rule 31.12).

**5.2** The application notice must specify the order that the applicant intends to ask the court to make and must be supported by evidence (see rule 31.12(2) which describes the orders the court may make).

**5.3** The grounds on which the order is sought may be set out in the application notice itself but if not there set out must be set out in the evidence filed in support of the application.

**5.4** In deciding whether or not to make an order for specific disclosure the court will take into account all the circumstances of the case and, in particular, the overriding objective described in Part 1. But if the court concludes that the party from whom specific disclosure is sought has failed adequately to comply with the obligations imposed by an order for disclosure (whether by failing to make a sufficient search for documents or otherwise) the court will usually make such order as is necessary to ensure that those obligations are properly complied with.

**5.5** An order for specific disclosure may in an appropriate case direct a party to –

(1) carry out a search for any documents which it is reasonable to suppose may contain information which may–

(a) enable the party applying for disclosure either to advance his own case or to damage that of the party giving disclosure; or

(b) lead to a train of enquiry which has either of those consequences; and

(2) disclose any documents found as a result of that search.

**Claims to withhold disclosure or inspection of a document**

**6.1** A claim to withhold inspection of a document, or part of a document, disclosed in a list of documents does not require an application to the court. Where such a claim has been made, a party who wishes to challenge it must apply to the court (see rule 31.19(5)).

**6.2** Rule 31.19(1) and (6) provide a procedure enabling a party to apply for an order permitting disclosure of the existence of a document to be withheld.

**Inspection of documents mentioned in expert's report (Rule 31.14(2))**

**7.1** If a party wishes to inspect documents referred to in the expert report of another party, before issuing an application he should request inspection of the documents informally, and inspection should be provided by agreement unless the request is unreasonable.

**7.2** Where an expert report refers to a large number or volume of documents and it would be burdensome to copy or collate them, the court will only order inspection of such documents if it is satisfied that it is necessary for the just disposal of the proceedings and the party cannot reasonably obtain the documents from another source.

**False disclosure statement**

**8** Attention is drawn to rule 31.23 which sets out the consequences of making a false disclosure statement without an honest belief in its truth, and to the procedures set out in rule 81.18 and paragraphs 5.1 to 5.7 of Practice Direction 81 - Applications and proceedings in relation to contempt of court.

**ANNEX**

**Disclosure statement**

I, the above named claimant [or defendant] [if party making disclosure is a company, firm or other organisation identify here who the person making the disclosure statement is and why he is the appropriate person to make it] state that I have carried out a reasonable and proportionate search to locate all the documents which I am required to disclose under the order made by the court on day of . I did not search:

(1) for documents predating .....,

(2) for documents located elsewhere than .....,

(3) for documents in categories other than .....

(4) for electronic documents

I carried out a search for electronic documents contained on or created by the following: [list what was searched and extent of search]

I did not search for the following:

(1) documents created before.....,

(2) documents contained on or created by the Claimant's/Defendant's PCs/portable data storage media/databases/servers/back-up tapes/off-site storage/mobile phones/laptops/notebooks/handheld devices/PDA devices (delete as appropriate),

(3) documents contained on or created by the Claimant's/Defendant's mail files/document files/calendar files/spreadsheet files/graphic and presentation files/web-based applications (delete as appropriate),

(4) documents other than by reference to the following keyword(s)/concepts..... (delete if your search was not confined to specific keywords or concepts).

I certify that I understand the duty of disclosure and to the best of my knowledge I have carried out that duty. I certify that the list above is a complete list of all documents which are or have been in my control and which I am obliged under the said order to disclose.

# PRACTICE DIRECTION 31B – DISCLOSURE OF ELECTRONIC DOCUMENTS

**This Practice Direction supplements CPR Part 31**



## Purpose, scope and interpretation

**1** Rule 31.4 contains a broad definition of 'document'. This extends to Electronic Documents.

**2** The purpose of this Practice Direction is to encourage and assist the parties to reach agreement in relation to the disclosure of Electronic Documents in a proportionate and cost-effective manner.

**3** Unless the court orders otherwise, this Practice Direction only applies to proceedings that are (or are likely to be) allocated to the multi-track.

**4** Unless the court orders otherwise, this Practice Direction only applies to proceedings started on or after 1st October 2010. Paragraph 2A.2 to 2A.5 of Practice Direction 31A in force immediately before that date continues to apply to proceedings started before that date.

**5** In this Practice Direction –

(1) 'Data Sampling' means the process of checking data by identifying and checking representative individual documents;

(2) 'Disclosure Data' means data relating to disclosed documents, including for example the type of document, the date of the document, the names of the author or sender and the recipient, and the party disclosing the document;

(3) 'Electronic Document' means any document held in electronic form. It includes, for example, email and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones. In addition to documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes metadata and other embedded data which is not typically visible on screen or a print out;

(4) 'Electronic Image' means an electronic representation of a paper document;

(5) 'Electronic Documents Questionnaire' means the questionnaire in the Schedule to this Practice Direction;

(6) 'Keyword Search' means a software-aided search for words across the text of an Electronic Document;

(7) 'Metadata' is data about data. In the case of an Electronic Document, metadata is typically embedded information about the document which is not readily accessible once the Native Electronic Document has been converted into an Electronic Image or paper document. It may include (for example) the date and time of creation or modification of a word-processing file, or the author and the date and time of sending an email. Metadata may be created automatically by a computer system or manually by a user;

(8) 'Native Electronic Document' or 'Native Format' means an Electronic Document stored in the original form in which it was created by a computer software program; and

(9) 'Optical Character Recognition (OCR)' means the computer-facilitated recognition of printed or written text characters in an Electronic Image in which the text-based contents cannot be searched electronically.

**General principles**

**6** When considering disclosure of Electronic Documents, the parties and their legal representatives should bear in mind the following general principles –

(1) Electronic Documents should be managed efficiently in order to minimise the cost incurred;

(2) technology should be used in order to ensure that document management activities are undertaken efficiently and effectively;

(3) disclosure should be given in a manner which gives effect to the overriding objective;

(4) Electronic Documents should generally be made available for inspection in a form which allows the party receiving the documents the same ability to access, search, review and display the documents as the party giving disclosure; and

(5) disclosure of Electronic Documents which are of no relevance to the proceedings may place an excessive burden in time and cost on the party to whom disclosure is given.

**Preservation of documents**

**7** As soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include Electronic Documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business.

**Discussions between the parties before the first Case Management Conference in relation to the use of technology and disclosure**

**8** The parties and their legal representatives must, before the first case management conference, discuss the use of technology in the management of Electronic Documents and the conduct of proceedings, in particular for the purpose of –

(1) creating lists of documents to be disclosed;

(2) giving disclosure by providing documents and information regarding documents in electronic format; and

(3) presenting documents and other material to the court at the trial.

**9** The parties and their legal representatives must also, before the first case management conference, discuss the disclosure of Electronic Documents. In some cases (for example heavy and complex cases) it may be appropriate to begin discussions before proceedings are commenced. The discussions should include (where appropriate) the following matters –

(1) the categories of Electronic Documents within the parties' control, the computer systems, electronic devices and media on which any relevant documents may be held, storage systems and document retention policies;

(2) the scope of the reasonable search for Electronic Documents required by rule 31.7;

(3) the tools and techniques (if any) which should be considered to reduce the burden and cost of disclosure of Electronic Documents, including –

(a) limiting disclosure of documents or certain categories of documents to particular date ranges, to particular custodians of documents, or to particular types of documents;

(b) the use of agreed Keyword Searches;

(c) the use of agreed software tools;

(d) the methods to be used to identify duplicate documents;

(e) the use of Data Sampling;

(f) the methods to be used to identify privileged documents and other non-disclosable documents, to redact documents (where redaction is appropriate), and for dealing with privileged or other documents which have been inadvertently disclosed; and

(g) the use of a staged approach to the disclosure of Electronic Documents;

(4) the preservation of Electronic Documents, with a view to preventing loss of such documents before the trial;

(5) the exchange of data relating to Electronic Documents in an agreed electronic format using agreed fields;

(6) the formats in which Electronic Documents are to be provided on inspection and the methods to be used;

(7) the basis of charging for or sharing the cost of the provision of Electronic Documents, and whether any arrangements for charging or sharing of costs are final or are subject to re-allocation in accordance with any order for costs subsequently made; and

(8) whether it would be appropriate to use the services of a neutral electronic repository for storage of Electronic Documents.

**The Electronic Documents Questionnaire**

**10** In some cases the parties may find it helpful to exchange the Electronic Documents Questionnaire in order to provide information to each other in relation

to the scope, extent and most suitable format for disclosure of Electronic Documents in the proceedings.

**11** The answers to the Electronic Documents Questionnaire must be verified by a statement of truth.

**12** Answers to the Electronic Documents Questionnaire will only be available for inspection by non-parties if permission is given under rule 5.4C(2).

**13** Rule 31.22 makes provision regulating the use of answers to the Electronic Documents Questionnaire.

**Preparation for the first Case Management Conference**

**14** The documents submitted to the court in advance of the first case management conference should include a summary of the matters on which the parties agree in relation to the disclosure of Electronic Documents and a summary of the matters on which they disagree.

**15** If the parties indicate that they have been unable to reach agreement in relation to the disclosure of Electronic Documents and that no agreement is likely, the court will give written directions in relation to disclosure or order a separate hearing in relation to disclosure. When doing so, the court will consider making an order that the parties must complete and exchange all or any part of the Electronic Documents Questionnaire within 14 days or such other period as the court may direct.

**16** The person signing the Electronic Documents Questionnaire should attend the first case management conference, and any subsequent hearing at which disclosure is likely to be considered.

**Where the parties are unable to reach an appropriate agreement in relation to the disclosure of Electronic Documents**

**17** If at any time it becomes apparent that the parties are unable to reach agreement in relation to the disclosure of Electronic Documents, the parties should seek directions from the court at the earliest practical date.

**18** If the court considers that the parties' agreement in relation to the disclosure of Electronic Documents is inappropriate or insufficient, the court will give directions in relation to disclosure. When doing so, the court will consider making an order that the parties must complete and exchange all or any part of the Electronic Documents Questionnaire within 14 days or such other period as the court may direct.

**19** If a party gives disclosure of Electronic Documents without first discussing with other parties how to plan and manage such disclosure, the court may require that party to carry out further searches for documents or to repeat other steps which that party has already carried out.

**The reasonable search**

**20** The extent of the reasonable search required by rule 31.7 for the purposes of standard disclosure is affected by the existence of Electronic Documents. The extent of the search which must be made will depend on the circumstances of the case including, in particular, the factors referred to in rule 31.7(2). The parties should bear in mind that the overriding objective includes dealing with the case in ways which are proportionate.

**21** The factors that may be relevant in deciding the reasonableness of a search for Electronic Documents include (but are not limited to) the following –

(1) the number of documents involved;

(2) the nature and complexity of the proceedings;

(3) the ease and expense of retrieval of any particular document. This includes:

(a) the accessibility of Electronic Documents including e-mail communications on computer systems, servers, back-up systems and other electronic devices or media that may contain such documents taking into account alterations or developments in hardware or software systems used by the disclosing party and/or available to enable access to such documents;

(b) the location of relevant Electronic Documents, data, computer systems, servers, back-up systems and other electronic devices or media that may contain such documents;

(c) the likelihood of locating relevant data;

(d) the cost of recovering any Electronic Documents;

(e) the cost of disclosing and providing inspection of any relevant Electronic Documents; and

(f) the likelihood that Electronic Documents will be materially altered in the course of recovery, disclosure or inspection;

(4) the availability of documents or contents of documents from other sources; and

(5) the significance of any document which is likely to be located during the search.

**22** Depending on the circumstances, it may be reasonable to search all of the parties' electronic storage systems, or to search only some part of those systems. For example, it may be reasonable to decide not to search for documents coming into existence before a particular date, or to limit the search to documents in a particular place or places, or to documents falling into particular categories.

**23** In some cases a staged approach may be appropriate, with disclosure initially being given of limited categories of documents. Those categories may subsequently be extended or limited depending on the results initially obtained.

**24** The primary source of disclosure of Electronic Documents is normally reasonably accessible data. A party requesting under rule 31.12 specific disclosure of Electronic Documents which are not reasonably accessible must demonstrate that the relevance and materiality justify the cost and burden of retrieving and producing it.

**Keyword and other automated searches**

**25** It may be reasonable to search for Electronic Documents by means of Keyword Searches or other automated methods of searching if a full review of each and every document would be unreasonable.

**26** However, it will often be insufficient to use simple Keyword Searches or other automated methods of searching alone. The injudicious use of Keyword Searches and other automated search techniques –

(1) may result in failure to find important documents which ought to be disclosed, and/or

(2) may find excessive quantities of irrelevant documents, which if disclosed would place an excessive burden in time and cost on the party to whom disclosure is given.

**27** The parties should consider supplementing Keyword Searches and other automated searches with additional techniques such as individually reviewing certain documents or categories of documents (for example important documents generated by key personnel) and taking such other steps as may be required in order to justify the selection to the court.

**Disclosure of metadata**

**28** Where copies of disclosed documents are provided in Native Format in accordance with paragraph 33 below, some metadata will be disclosed with each document. A party requesting disclosure of additional metadata or forensic image copies of disclosed documents (for example in relation to a dispute concerning authenticity) must demonstrate that the relevance and materiality of the requested metadata justify the cost and burden of producing that metadata.

**29** Parties using document management or litigation support systems should be alert to the possibility that Metadata or other useful information relating to documents may not be stored with the documents.

**Lists of documents**

**30** If a party is giving disclosure of Electronic Documents, paragraph 3 of Practice Direction 31A is to be read subject to the following –

(1) Form N265 may be amended to accommodate the sub-paragraphs which follow;

(2) a list of documents may by agreement between the parties be an electronic file in .csv (comma-separated values) or other agreed format;

(3) documents may be listed otherwise than in date order where a different order would be more convenient;

(4) save where otherwise agreed or ordered, documents should be listed individually if a party already possesses data relating to the document (for example, type of document and date of creation) which make this possible (so that as far as possible each document may be given a unique reference number);

(5) a party should be consistent in the way in which documents are listed;

(6) consistent column headings should be repeated on each page of the list on which documents are listed, where the software used for preparing the list enables this to be carried out automatically; and

(7) the disclosure list number used in any supplemental list of documents should be unique and should run sequentially from the last number used in the previous list.

**Provision of disclosure data in electronic form**

**31** Where a party provides another party with disclosure data in electronic form, the following provisions will apply unless the parties agree or the court directs otherwise –

(1) Disclosure data should be set out in a single, continuous table or spreadsheet, each separate column containing exclusively one of the following types of disclosure data –

(a) disclosure list number (sequential)

(b) date

(c) document type

(d) author/sender

(e) recipient

(f) disclosure list number of any parent or covering document;

(2) other than for disclosure list numbers, blank entries are permissible and preferred if there is no relevant disclosure data (that is, the field should be left blank rather than state ‘Undated’);

(3) dates should be set out in the alphanumeric form ‘01 Jan 2010’; and

(4) Disclosure data should be set out in a consistent manner.

**Provision of electronic copies of disclosed documents**

**32** The parties should co-operate at an early stage about the format in which Electronic Documents are to be provided on inspection. In the case of difficulty or disagreement, the matter should be referred to the court for directions at the earliest practical date, if possible at the first case management conference.

**33** Save where otherwise agreed or ordered, electronic copies of disclosed documents should be provided in their Native Format, in a manner which preserves Metadata relating to the date of creation of each document.

**34** A party should provide any available searchable OCR versions of Electronic Documents with the original. A party may however choose not to provide OCR versions of documents which have been redacted. If OCR versions are provided, they are provided on an 'as is' basis, with no assurance to the other party that the OCR versions are complete or accurate.

**35**

(1) Subject to sub-paragraph (2) below, if a party is providing in electronic form copies of disclosed documents and wishes to redact or otherwise make alterations to a document or documents, then –

(a) the party redacting or altering the document must inform the other party in accordance with rule 31.19 that redacted or altered versions are being supplied; and

(b) the party redacting or altering the document must ensure that the original unredacted and unaltered version is preserved, so that it remains available to be inspected if required.

(2) Sub-paragraph (1) above does not apply where the only alteration made to the document is an alteration to the Metadata as a result of the ordinary process of copying and/or accessing the document. Sub-paragraph (1) does apply to the alteration or suppression of Metadata in other situations.

**Specialised technology**

**36** If Electronic Documents are best accessed using technology which is not readily available to the party entitled to disclosure, and that party reasonably requires additional inspection facilities, the party making disclosure shall co-operate in making available to the other party such reasonable additional inspection facilities as may be appropriate in order to afford inspection in accordance with rule 31.3

**ADDENDUM C**

**SCHEDULE**

**ANNEXURE C- ELECTRONIC DOCUMENTS QUESTIONNAIRE IN UNITED KINGDOM**

**Part 1 – Your disclosure**

**Date range and custodians**

1. What date range do you consider that your searches for Electronic Documents should cover ('the date range')?

2. Identify the custodians or creators of your Electronic Documents whose repositories of documents you consider should be searched[1].

**Communications**

2. Which forms of electronic communication were in use during the date range (so far as is relevant to these proceedings)?

| A | B | C | D | E |
|---|---|---|---|---|
| **Communication** | **In use during the date range? (yes/no)** | **Are you searching for relevant documents in this category? (yes/no)** | **Where and on what type of software/equipment/media is this communication stored[2]?** | |
| i) Email | | | | |
| ii) Other (provide details for each type). | | | | |

**Electronic Documents**

4. Apart from attachments to emails, which forms of Electronic Documents were created or stored by you during the date range?

| A | B | C | D | E |
|---|---|---|---|---|
| **Document Type** | **In use during the date** | **Are you searching for relevant documents in** | **Where and on what type of software/equipment/media are these documents[5]?** | **(a) Are back-ups or archives of these documents available, and (b)** |

| | range? (yes/no) | this category? (yes/no) | if so, are you searching the back-ups or archives? |
|---|---|---|---|
| i) Word (or equivalent - state which) | | | |
| ii) Excel (or equivalent - state which) | | | |
| iii) Electronic Images | | | |
| iv) Other (state which) | | | |

**Databases of Electronic Documents**

5. In the following table identify database systems, including document management systems, used by you during the date range and which may contain disclosable Electronic Documents.

| A | B | C | D | E |
|---|---|---|---|---|
| **Name** | **Brief description** | **Nature of data held** | **Are you disclosing documents held in this database? (yes/no)** | **Proposals for provision of relevant documents to or access by other parties to this litigation** |
| 1. | | | | |
| 2. (etc) | | | | |

**Key words**

6. Do you consider that Keyword Searches should be used as part of the process of determining which Electronic Documents you should disclose?

If yes, provide details of –

(1) the keywords used or to be used (by reference, if applicable, to individual custodians, creators, repositories, file types and/or date ranges); and

(2) the extent to which the Keyword Searches have been or will be supplemented by a review of individual documents.

**Other types of automated searches**

7. Do you consider that automated searches or automated techniques other than Keyword Searches (for example, concept searches or clustering) should be used as part of the process of determining which Electronic Documents you should disclose? If yes, provide details of –

   (1) the process(es) used or to be used (by reference, if applicable, to individual custodians, creators, repositories, file types and/or date ranges);

   (2) the extent to which the processes have been or will be supplemented by a review of individual documents; and

   (3) how the methodology of automated searches will be made available for consideration by other parties.

8. If the answer to Question 6 or 7 is yes, state whether attachments to (a) emails (b) compressed files (c) embedded files and (d) imaged text will respond to your Keyword Searches or other automated search.

9. Are you using or intending to use computer software for other purposes in relation to disclosure? If so, provide details of the software, processes and methods to be used.

10. Do any of the sources and/or documents identified in this Electronic Documents Questionnaire raise questions about the reasonableness of the search which ought to be taken into account? If so, give details.

11. Are any documents which may be disclosable encrypted, password-protected or for other reasons difficult to access, or do you have any reason to believe that they may be? If so, state which of the categories identified at Questions 3, 4 and 5 above are affected, and your proposals for making them accessible.

12. Are you aware of any other points in relation to disclosure of your Electronic Documents which require discussion between the parties? If so, give details.

13. Do you have a document retention policy?

14. Have you given an instruction to preserve Electronic Documents, and if so, when?

15. Subject to re-consideration after receiving the responses of other parties to this Electronic Documents Questionnaire, (a) in what format and (b) on what media do you intend to provide to other parties copies of disclosed documents, which are or will be available in electronic form?

16. Subject to re-consideration after receiving the responses of other parties to this Electronic Documents Questionnaire, do you intend to provide other parties with

Disclosure Data electronically, and if so, (a) in what format and (b) on what media?

17. Insofar as you have available or will have available searchable OCR versions of Electronic Documents, do you intend to provide the searchable OCR version to other parties? If not, why not

**Part 2 - The disclosure of other parties**

18. Do you at this stage have any The extent and content proposals about the date ranges which should be searched by other parties to the proceedings? If so, provide details.

19. Do you at this stage have any proposals about the custodians or creators whose repositories of documents should be searched for disclosable documents by other parties to the proceedings? If so, provide details.

20. Do you consider that the other party(ies) should disclose all available metadata attaching to any documents? If yes, provide details of the documents or categories of documents.

21. Do you at this stage have any proposals about the Keyword Searches, or other automated searches, which should be applied by other parties to their document sets? If so, provide details.

22. Subject to re-consideration after receiving the responses of other parties to this Electronic Documents Questionnaire, (a) in what format and (b) on what media do you wish to receive copies of disclosed documents, which are or will be available in electronic form?

23. Subject to re-consideration after receiving the responses of other parties to this Electronic Documents Questionnaire, do you wish to receive Disclosure Data electronically, and if so, (a) in what format and (b) on what media?

**STATEMENT OF TRUTH**

*[I believe][The [claimant][defendant] believes] that the facts stated in the answers to this Electronic Documents Questionnaire are true.

*I am duly authorised by the [claimant][defendant] to sign this statement.

Full name_____

Name of legal representative's firm_____

Signed _____

Position or office held (if signing on behalf of firm or company) _____

Date _____

**ADDENDUM D**

**EXTRACTS FROM PROTECTION OF PERSONAL INFORMATION ACT**

**PROTECTION OF CLASSIFIED INFORMATION BEFORE COURTS**

Protection of classified information before courts

49. (1) In any proceedings where an official or a functionary of an organ of state intends to file a record that contains classified information, that official or functionary must alert court officials and the court of the classification of the information and request court officials to protect the record or parts of the record that contain classified information from disclosure or publication pending a court determination on the proper handling of such information during the course of the legal proceedings.

(2) Classified information that is filed in the manner contemplated in subsection (1) may not be disclosed to persons not authorised to receive such information unless a court, in the interests of justice, and upon considering issues of national security, orders full or limited disclosure, with or without conditions.

(3) Unless a court orders the disclosure of classified information or orders the limited or conditional disclosure of classified information, the court must issue directions for the proper protection of such information during the course of legal proceedings, which may include, but is not limited to—

(a) the holding of proceedings, or part thereof, in camera;

(b) the protection from disclosure or publication of those portions of the record containing the classified information; or

(c) the implementation of measures to confine disclosure to those specifically authorised to receive the classified information. 21 5 10 15 20 25 30 35 40 45 50 (4) A court may not order the disclosure of classified information without taking reasonable steps to obtain the written or oral submissions of the classification authority that made the classifications in question or alternatively to obtain the submissions of the Director-General of the Agency. (5) If it appears to a court that it would, in any hearing held in terms of this section be in the interest of the national security or in the interest of justice that such hearing be held in camera or that the submission referred to in subsection (4) be not publicly disclosed, the court may direct that the hearing must be held in camera and that any person not authorised to receive such classified information may not be present at such hearing. (6) A court may, if it considers it appropriate,

seek the written or oral submissions of interested parties, persons and organisations but may not disclose the actual classified information to such persons or parties prior to its order to disclose the classified information in terms of subsection (2). (7) A classification authority or the Director-General of the Agency, as the case may be, in consultation with the relevant Minister, must declassify classified information required in legal proceedings, either in whole or in part, unless it is strictly necessary to maintain the classification in terms of this Act. (8) In addition to the measures set out in this section, a court in criminal proceedings has the same powers as those conferred upon a court under sections 154(1) and (4) of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), and the said section applies with the necessary changes. (9) Any person who discloses or publishes any classified information in contravention of an order or direction issued by a court in terms of this section is guilty of an offence and liable on conviction to imprisonment for a period not exceeding five years. (10) A court which acts in terms of this section must endeavour to accommodate the principle of open justice to as great an extent as possible without risking or compromising national security.

## ADDENDUM E: SEDONA PRINCIPLES

1. Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.
2. When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in Fed. R. Civ. P. 26(b)(2) and its state law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.
3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.
4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.
5. The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.
6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents.
7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.
8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that

outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.

9. Absent a showing of special need and relevance a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual data or documents.
10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.
11. A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data most likely to contain responsive information.
12. Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.
13. Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.
14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

## ADDENDUM F: ABBREVIATIONS

| Abbreviation | Description |
|---|---|
| | |
| BSB | Bar Standards Board |
| CCG | Commercial Court Guide |
| CD | Compact Disc |
| CMC | Case Management Conference |
| CPA | Criminal Procedure Act |
| CPEA | Civil Proceedings Evidence Act |
| CPR | Civil Procedure Rules, UK |
| DVD | Digital Versatile Disc |
| ECTA | Electronic Communications and Transactions Act |
| EDRM | Electronic Discovery Reference Model |
| EGI | Electronically Stored Information |
| ESI | Electronically Stored Information |
| EU | European Union |
| FED. R .CIV P | Federal Rules of Civil Procedure (USA) |
| FED. R. EVID | Federal Rules of Evidence (USA) |
| LEAA | Law of Evidence Amendment Act (RSA) |
| PAIA | Promotion to Access to Information Act |
| PD31A | Practice Direction 31A |

| | |
|---|---|
| PD31B | Practice Direction 31B |
| PDF | Portable Document Format |
| POPIA | Protection of Personal Information Act |
| SMS | Short Message Service |
| TIFF | Tagged Image File Format |
| RICA | Regulation of Interception of Communications and Provision of Communication-Related Information Act |
| UK | United Kingdom |
| USA | United States of America |
| USB | Universal Serial Bus |

## ADDENDUM G-PARAGRAPHS FROM DIGICEL CASE

Set out its approach as follows:[720]

33. Paragraph 2A of the Practice Direction deals with electronic disclosure and is in these terms:

**ELECTRONIC DISCLOSURE**

2A.1 Rule 31.4 contains a broad definition of a document. This extends to electronic documents, including e-mail and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been 'deleted'. It also extends to additional information stored and associated with electronic documents known as metadata.

2A.2 The parties should, prior to the first Case Management Conference, discuss any issues that may arise regarding searches for and the preservation of electronic documents. This may involve the parties providing information about the categories of electronic documents within their control, the computer systems, electronic devices and media on which any relevant documents may be held, the storage systems maintained by the parties and their document retention policies. In the case of difficulty or disagreement, the matter should be referred to a judge for directions at the earliest practical date, if possible, at the first Case Management Conference.

2A. 3 The parties should co-operate at an early stage regarding the format in which electronic copy documents are to be provided on inspection. In the case of difficulty or disagreement, the matter should be referred to a Judge for directions at the earliest practical date, if possible, at the first Case Management Conference.

2A.4 The existence of electronic documents impacts upon the extent of the reasonable search required by Rule 31.7 for the purposes of standard disclosure. The factors that may be relevant in deciding the reasonableness of a search for electronic documents include (but are not limited to) the following: -

(a) The number of documents involved.

(b) The nature and complexity of the proceedings.

(c) The ease and expense of retrieval of any particular document. This includes:

(i) The accessibility of electronic documents or data including e-mail communications on computer systems, servers, back-up systems and other electronic devices or media that may contain such documents taking into account alterations or developments in hardware or software systems used by the disclosing party and/or available to enable access to such documents.

720 *DigiCell (St Lucia) Ltd v Cable and Wireless Plc* [2008] EWHC 2522 (Ch) at paragraphs 33-36.

(ii) The location of relevant electronic documents, data, computer systems, servers, back-up systems and other electronic devices or media that may contain such documents.

(iii) The likelihood of locating relevant data.

(iv) The cost of recovering any electronic documents.

(v) The cost of disclosing and providing inspection of any relevant electronic documents.

(vi) The likelihood that electronic documents will be materially altered in the course of recovery, disclosure or inspection.

(d) The significance of any document likely to be located during the search.

2A.5 It may be reasonable to search some or all of the parties' electronic storage systems. In some circumstances, it may be reasonable to search for electronic documents using keyword searches (agreed as far as possible between the parties), even where a full review of each and every document would be unreasonable. There may be other forms of electronic search that may be appropriate in particular circumstances.

34. It will be noted that paragraph 2A. 1 of the Practice Direction refers to the range of electronic documents including e-mail communications within the definition of "documents". The same paragraph also refers to back-up systems. Paragraph 2A.2 states that the parties should discuss any issues that might arise regarding searches for electronic documents at an early stage. Paragraph 2A.3 again refers to the need for the parties to cooperate regarding the format in which electronic copy documents are to be provided for inspection. Paragraph 2A.4 supplements the factors listed in CPR Rule 31.7(2) by identifying 6 specific matters in paragraph 2A.4(c). Paragraph 2A.5 of the PD refers to the possibility of searching electronic documents using keyword searches and adds that these searches are agreed upon as far as possible between the parties.

35. Paragraph 5.1 of the Practice Direction deals with specific disclosure. Paragraph 5.4 states: In deciding whether or not to make an order for specific disclosure, the court will take into account all the circumstances of the case and, in particular, the overriding objective described in Part 1. But if the court concludes that the party from whom specific disclosure is sought has failed adequately to comply with the obligations imposed by an order for disclosure (whether by failing to make a sufficient search for documents or otherwise), the court will usually make such order as is necessary to ensure that those obligations are properly complied with.

36. Paragraph 5.4 of the Practice Direction makes it clear that the procedure of applying to the court for an order for specific disclosure is available where the applicant alleges that the respondent is in breach of its obligation to give standard disclosure, whether by failing to make a sufficient search for documents or otherwise. Where there is a failure to make a sufficient search, the court will "usually" make such order as is necessary to ensure that the obligations on the respondent are properly complied with. However, an order for specific disclosure under CPR Rule 31.12 is not confined to a case where the respondent is in breach

of an obligation to give standard disclosure. The court can make an order for specific disclosure even where the respondent has properly complied with its obligations to provide standard disclosure, but the applicant satisfies the court that such disclosure is "inadequate" or that the case is one where something more than standard disclosure is called for, for example, disclosure of documents which may lead to a train of inquiry with the consequence of producing documents which advance the applicant's case or damage the respondent's case: see paragraph 5.5 of the Practice Direction.

37. Paragraph 2A of Part 31 Practice Direction was introduced following the recommendations of a working party chaired by Justice Cresswell on the subject of electronic disclosure. The report was not cited to me, but nonetheless, it provides very useful background reading when considering an application of the kind which is before me.

38. The Cresswell Report makes a number of points that are useful to record. At paragraph 3.3, the report explains why the issues which arise in relation to disclosure of electronic documents are different from the issues which arise in relation to disclosure of paper documents. These reasons include the huge volume of documents which are created and stored electronically, the ease of duplication of electronic documents, the lack of order in the storage of electronic documents, the differing retention policies of the parties, the existence of metadata and the fact that electronic documents are more difficult to dispose of than paper documents.

39. At paragraph 2.15, the Cresswell Report discusses the duty to search for documents. It states that Part 31 gives a party "a certain degree of latitude" as to the extent of the search because what may be reasonable in one case may be inadequate in another. The test of "a reasonable search" in Rule 31.7 has the virtue of flexibility and takes account of the overriding objective: see paragraph 2.18. At paragraph 2.18(4), the report refers to back-up data and describes this as commonly having the disadvantage that the data is compressed and it can be difficult and costly to retrieve. At paragraph 2.20, the report refers to the possibility of a search being carried out electronically using specified words or strings of words rather than manually.

40. The Cresswell Report refers to the experience and approach in the United States of America. It concludes that the case law in the United States illustrated some of the difficulties in practice but did not build up a coherent pattern of decisions. Later in the report (paragraph 2.29), there is a discussion of the Sedona Principles first laid down at the Sedona Conference in 2004. The report considered that these principles were not suitable for wholesale adoption in England and Wales. Nonetheless, it can be seen by comparing the Sedona Principles with the recommendations of the working party that the working party picked those parts of the Sedona Principles which were appropriate for adoption in this jurisdiction.

Electronic information can be altered easily[721] and this raises admissibility issues.[722] The Fed.R.Evid contains the evidentiary rules applicable to all forms of evidence that are adduced in legal proceedings in the United States.[723] The Fed.R.Evid provides a safeguard against tampering with evidence, including electronic information, to ensure the authenticity and reliability of electronic information when adduced as evidence. Article IX of the Fed.R.Evid governs the authentication of evidence, including electronic information. Courts have a broad authority to determine the admissibility of evidence.[724] Rule 901(a) of the Fed. R Evid under Article IX and reads as follows:

> (a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

Rule 901(a) of the Federal Rules of Civil Procedure sets out the requirements for authentication of electronically stored evidence. Rule 901 of the Fed.R. Evid is silent on the process that one needs to follow to authenticate evidence.[725] It provides examples of how authentication can be achieved.[726] These examples include authentication through processes or systems that require evidence describing the process or system used to produce a result and showing that the process or system produced an accurate result. Rule 901(b) (7) of the Fed.R. Evid deems public records and reports with their metadata stored on servers or computers to be authentic. In terms of this rule, parties do not have to provide any evidence to show that the computer system producing the public records was reliable or the records accurate.[727] In contrast, Rule 901(b) (9) of the Fed.R. Evid deals with scenarios where the accuracy of the public record or report depends upon a computer processor system that produces it.[728] A

721 Cohen and Lender (n 3 above) 6-3.
722 Cohen and Lender (n 3 above) 6-3 and Schwikkard and Van der Merwe (n 35 above) 411.
723 See Fed.R. Evid in the United States.
724 In *United States v Sanders,* (1984) 749 F.2d 195, 197 (5th Cir. 1984).
725 Grimm, Bergstrom and O'Toole-Loureiro "Authentication of social media evidence". *Am. J. Trial Advoc.* 36(3), 433-472.
726 Stanfield (n 141 above) 190.
727 See Fed.R. Evid
728 See rule 901 that reads as follows: "Authenticating or Identifying Evidence
(a) IN GENERAL. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.
(b) EXAMPLES. The following are examples only—not a complete list—of evidence that satisfies the requirement-… (9) *Evidence About a Process or System.* Evidence describing a process or system and showing that it produces an accurate result."

litigant that adduces evidence must describe the process or system used to produce a result and illustrate that the process or system produces an accurate result.[729]

One needs to bear in mind that the Fed.R. Evid was not amended or modified to fit in with technological advances. Judicial officers had to adapt their approach when dealing with electronic information as evidence to meet the requirements of relevance, authenticity, and admissibility in the United States.[730] In addition, the parties need to also discuss issues related to privilege under Fed.R.Evid 502.

## Reference List

729 Stanfield (n 141 above) 190.
730 Grimm "Authenticating digital evidence" (n 145 above) 47.

**Books**

Currie, I & De Waal, J *The Bill of Rights Handbook* (2013) Juta: Cape Town

Cohen, AI & Lender, DJ *Electronic Discovery: Law & Practice* (2008) Aspen: New York

Du Toit, E; De Jager, FJ; Paizes, A; Skeen, AS; Van Der Merwe, S; & Terblanche, S *Commentary on the Criminal Procedure Revision 67* (2021) Juta: Cape Town

Engeland, P *Expert Privilege in Civil Evidence* (2011) Hart: Portland (OR)

Fishman, CS & McKenna, AT, *Jones On Evidence Civil and Criminal* (2001) Thomson Reuters: [Place of Publication]

Erasmus, HJ & Van Loggerenberg, DE *Jones & Buckle: The Civil Practice of the Magistrates Courts in South Africa Volume 1* (2021) Juta: Cape Town

Erasmus, HJ & Van Loggerenberg, DE, *Jones & Buckle: The Civil Practice of the Magistrates Courts in South Africa Volume 2* (2022) Juta: Cape Town

Gahten, AM *Electronic Evidence* (1999) Carswell Thomson Professional Publishing : Toronto

Harvey, D *Collisions in the Digital Paradigm* (2017) Hart Publishing: Oxford and Portland, Oregan

Hedges, RJ *Discovery of Electronically Stored Information Surveying the Legal Landscape* (2007) Newark: New Jersey

Cilliers, AC; Loots, C & Nel, HC Herbstein and Van Winsen *The Civil Practice of the High Courts of South Africa" Volume1* (2012) Juta: Cape Town

Iller, M *Civil Evidence: The Essential Guide* (2006) Sweet & Maxwell: London

Joubert, WA & Faris JA, The Law of South Africa *Volume 4* (2012) LexisNexis: Durban

Schmidt, CWH & Rademeyer, H *Law of Evidence* Issue 19 (2021) LexisNexis: Durban.

Mason, S, *Electronic Evidence* (2007) LexisNexis Butterworths: London

Mason, S, *Electronic Evidence: Disclosure* (2010) LexisNexis Butterworths: London

Mason, S, *Electronic Evidence: Disclosure* (2012) LexisNexis Butterworths: London

Mason; S *Electronic Evidence: Disclosure* (2017) LexisNexis Butterworths: London

Mueller, CK & Kirkpatrick, LC *Evidence* (2012) Wolter Kluwers:

Papadoulos, S & Snail ka Mtuze, S *The law of the Internet in South Africa* (3rd ed) Cyberlaw@SA III (2012) Van Schaik: Pretoria

Papadoulos, S & Snail ka Mtuze, S *The law of the Internet in South Africa* (4th ed) Cyberlaw@SA IV (2022) Van Schaik: Pretoria

Schwikkard, PJ; Van der Merwe, SE; Collier, DW; De Vos, WL & Van Der Berg, E *Principles of Evidence* (2018) Juta: Cape Town

Sharpe, S *Electronically Recorded Evidence* (1989) Fourmet Publishing: Londen.

Van der Merwe, D; Roos, A; Pistorius, T & Eiselen, S *Information and Communications Technology Law* (2008) LexisNexis: Durban

Wheater, M & Raffin, C *Electronic Disclosure Law and Practice* (2017) Oxford University Press: Oxford

Zeffert, DT; Paizes, AP & Skeen, AS *The South African Law of Evidence* (formerly known Hoffman and Zeffert) LexisNexis Butterworths: Durban.

Zeffert, DT & Paizes, AP *The South African Law of Evidence* (2009) LexisNexis: Durban.

**Chapters in books**

Hofman, J, "South Africa" in S Mason (ed) "Electronic Evidence in South Africa" in Electronic Evidence: Disclosure, Discovery and Admissibility (2007) LexisNexis Butterworths: London

Hofman, J & De Jager J, "South Africa" in Mason (ed) *Electronic Evidence* (2012) LexisNexis Butterworths: London

Mason, Sheldon and Dries "Proof: the technical collection and examination of electronic evidence" in Mason and Seng *Electronic Evidence* (2017) LexisNexis Butterworths: London

Schafer and Mason "The characteristics of electronic evidence" in Mason and Seng (ed) *Electronic Evidence* (2017) LexisNexis Butterworths: London

Schafer and Sheldon "Proof: the technical collection and examination of electronic evidence" in Mason and Seng (ed) *Electronic Evidence* (2017) 285

Schwerha; Bagby and Esler "United States of America" in Mason *Electronic Evidence* (2012) LexisNexis Butterworths: London

**Unpublished LLD thesises**

Van Heerden CM, 'Voorbereiding vir verhoor ter verwesenliking van die waarborg van n billike verhoor ' ( unpublished LLD dissertation, Rand Afrikaanse Universiteit, 2004).

Swales *"An analysis of the regulatory environment governing electronic evidence in South Africa: Suggestions for reform"* (unpublished LLD thesis UCT 2018) 26.

**South African Law Reform Commission Reports and Papers**

South African Law Reform Commission "Electronic Evidence in Criminal and Civil Proceedings" *Review of the Law of Evidence* Issue Paper No. 27, Project 126 (30 June 2010)

South African Law Reform Commission "Electronic Evidence in Civil proceedings: Admissibility and Related Issues" *Review of the Law of Evidence* Discussion Paper No. 131, Project 126 (31 October 2014)

**Journal Articles**

Basdeo, V 'The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis' 2012(2) *South African Journal of Criminal Justice* 195 -212

Bouwer, G "Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context" 2014(2) *South African Journal of Criminal Justice* 156-171

Burke, T; Ward, JD; Sipior, JC; Hopkins, JP; Purwin, C & Volonino, L "Electronic Discovery : Rules for a Digital Age" 2012 (18) *Boston University Journal of Science &Technology Law* 150-198

Cassim, F " The use of electronic discovery and cloud computing technology by lawyers in practice: Lessons from abroad" 2017(42) *Journal for Juridical Science* 19-40

Chorvat, TJ & Pelanek, LE "Electronic Stored Information in Litigation" 2011(67) *The Business Lawyer* 285-292

Danna, ER "Weathering the Evolving Landscapes of Electronic Discovery" 2017(29) *Singapore Academy of Law Journal* 343-374

De Villiers, DS "Old "documents", "videotapes" and new "data messages" – a functional approach to the law of evidence" (Part 1) 2010(3) *Tydsfrif vir Suid Afrikaanse Reg* 558-575

De Villiers, DS "Old "documents" "videotapes" and new "data messages" – a functional approach to the law of evidence" (Part 2) 2010(4) *Tydsfrif vir Suid Afrikaanse Reg* 720-735

Downing, RW "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" 2004-2005(43) *Columbia Journal of Transitional Law* 705-762

Eloff, D "Legal professional privilege and Internet hacking" November 2017 *De Rebus*

Ewan, DE; Richards, JA &Tank, MHK "It's the Message, Not the Medium! Electronic Record and Electronic Signature Rules Preserve Existing Focus of the Law Content, Not Medium of Recorded Land Title Instruments" 2005 (60) *The Business Lawyer* 1487-1506

George, CN "Someone's Watching: Protecting Privilege on Both Sides of the Table during Electronic Discovery" 2004(2) *Journal of Law, Technology & Policy 283*-294

Goode, S "The Admissibility of Electronic Evidence" 2009-2010(29) *The Review Litigation* 1-64

Greenwood, DJ & Campbell, RA "Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication 1997(53) *The Business Lawyer* 53 307-339

Grobler, MM & Von Solms SH "Fusing Business, Science and Law: Presenting Digital Evidence in Court" Journal of Contemporary Management 2009 (6) 375 – 389

Grimm, PW; Bergstrom, L & O'Toole-Loureiro, MM (2013) “Authentication of social media evidence” 2013 (36) *American Journal of Trial Advocacy* 433-472.

Heyink, M “Why are South African lawyers remaining in the dark with POPI?” August 2015 *De Rebus* 30-33

Hofman, J "Electronic Evidence in Criminal Cases" 2006(3) *South African Journal of Criminal Justice* 257-275

Hirt, TC “The quest for proportionality in electronic discovery-moving from theory to reality in civil litigation” 2011(5) *Federal Courts Law Review* 171-200

Hughes B “The rise of electronic discovery” January/ February 2012 *De Rebus* 24-26

Marcus, RL “Confronting the Future: Coping with Discovery of Electronic material” 2001(64) *Law and Contemporary Problems Journal* 253-281

Manyathi-Jele, N “Unlawfully’ obtained Facebook communication admissible in court” April 2016 *De Rebus* 38-39

Mupangavanhu, Y “Electronic signatures and non-variation clauses in the modern digital world: The case of South Africa” 2016(133) *South African Law Journal* 853-873

Oostenrijk, LS “Paper or Plastic: Electronic Discovery and Spoliation in the Digital Age” 42 2005() *Houston Law Review* 1163-1203

Parkins, Z “Electronic Discovery: Why the appointment of special masters in all large electronic discovery disputes is vital to the progress of the American civil justice” 2011(5) *American Journal of Mediation* 97-110

Rockwood, R "Shifting the Burdens and Concealing Electronic Evidence: Discovery in the Digital Era" 2005-2006(12) *Richmond Journal of Law & Technology* 1-19

Scheindlin, SA & Rabkin, J "Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?" 2000 (41) *Boston Law Review* 327-382

Smith, JM "Electronic Discovery and the Constitution: Inaccessible Justice" 2012 (6) *Journal of Legal Technology and Risk Management* 122-*172*

Swales, L An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One 2018(21) *Potchefstroom Electronic Law Journal* 1-30

Swales, L An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two 2018(21) *Potchefstroom Electronic Law Journal*

Takombe, MO "The rise of the machines - understanding electronic evidence" August 2014 *De Rebus* 32-34.

Tennis, BT "Cost-shifting in electronic Discovery" 2010(119) *The Yale Law Journal* 1113- 1121

Theophilopoulos, C "Defining the limits of the common-law, South African and European privilege against self-incrimination" 2014(1) *Stellenbosch Law Review* 160-186

.

Theophilopoulos, C "Electronic Documents, Encryption, Cloud Storage And The Privilege against Self-Incrimination" 2015(132) *The South African Law Journal* 596-615

Theophilopoulos, C "The Admissibility of Data, Data Messages, and Electronic Documents at Trial" 2015(3) *Tydskrif vir Suid Afrikaanse Reg* 461-481

Van der Merwe, D " Comparative Overview of The (Sometimes Uneasy) Relationship between Digital Information and Certain Legal Fields in South Africa 2014 (17) *Potchefstroom Electronic Law Journal* 297-328

Van Dorsten, J "Discovery of electronic documents and attorneys' obligations" November 2012 *De Rebus* 34-36

Wang, Z "Ethics and Electronic Discovery: New Medium, Same Problems" 2008 (75) *Defense Counsel Journal* 328-345

Watney, M "Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position" (2009) (1) *Journal of Information, Law & Technology* 1-13

Withers, KJ "*Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*" 2006(4) *New Jersey Journal of Technology & IntellectualProperty*171- 200

Zuchlewski; P "The Uses and Abuses of Electronic Discovery" 2011(57) *The Wayne Law Review* 1391-1409

**Case law**

**Foreign Case Law**

**United States of America**

*Byers v. Illinois State Police*, 53 Fed. R. Serv. 3d 740 (N.D. III. May 31, 2002)

*Brookfield Asset Management, Inc. v. AIG Financial Products Corp* (S.D.N.Y. Jan. 7, 2013)

*Zubulake v UBS Warburg* LLC 220 F.R.D. 212 (S.D.N.Y 2003)

*Zubulake v UBS Warburg* LLC 217 F.R.D. 309 (S.D.N.Y 2003)

*Zubulake v UBS Warburg* LLC 230 F.R.D. 290 (S.D.N.Y 2003)

*Zubulake v UBS Warburg* LLC 216 F.R.D. 280 (S.D.N.Y 2003)

**United Kingdom**

*Abela v Hammonds Suddards* (2008) All ER (D) 22

*Arrow Nominees Inc v Blackledge* (2000) All ER (D) 854

*Al Rawi v Security Service* (2011) UKSC 34
*Bank St Petersburg PJSC and another v Arkhangelsky and another* (2015) EWHC 2997 (Ch)
*Compagnie Fiancière et Commerciale du Pacifique v Peruvian Guano* (1882) 11 QBD 55
*Derby v Weldon* (1990) 3 All ER 161

*Digicel (St Lucia) Ltd and others v Cable & Wireless plc and others* (2010) All ER (D) 166

*Digicel (St Lucia) v Cable Wireless* (2008) All ER (D) 226

*Digicel (St. Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* (2009) 2 All ER 1094

*Digicel v Cable & Wireless PLC* (2010) All ER (D) 166

*Digicel v Cable and Wireless PLC* (2008) All ER (D) 226

*Douglas and others v Hello! and others* (2003) All ER (D) 238

*Earles v Barclays Bank*, [2009] EWHC 2500 (QB), (2009) All ER (D) 179

*Fiddes v Channel 4 TV Corporation* (2010) EWCA Civ 516

*Goodale & others v the Ministry of Justice & others* (2009) EWHC 3834 (QB)

*Harlequin Property (SVG) Ltd & Anor v Wilkins Kennedy (A Firm) (No. 2)*(2015) All ER (D) 268

*Hedrich and another v Standard Bank London*(2008) All ER (D) 390

*Hedrich v Standard Chartered Bank* (2008) All ER (D) 390

*Hellard & Goldfarb v Robbins* (2008) EWHC 2275 (Ch)

*HRH Prince Abdulaziz Bin Mishal Bin Abdulaziz Al Saud v Apex Global Management Ltd and another*(2014) All ER (D) 278

*Icon SE LLC v SE Shipping Lines* (2012) All ER (D) 116

*IG Index Ltd v Cloete* (2014) EWCSA Civ 1128

*Lonrho v Shell Petroleum* (1980) 1 WLR 627

*Mueller Europe v Central Roofing* (2012) EWHC 3417 (TCC)

*Myers v Elman* (1939) 4 All ER 484

*North Shore Ventures v Anstead Holdings* (2012) EWCA Civ 11

*Phaestos Ltd & Anor v Ho* (2012) EWHC 668 (TCC)

*Phaestos v Ho/Ikos Cif Limited v Gover* (2012) EWHC 1996 (TCC)

*Re Atrium Training Services Ltd (in liquidation) Smailes and another v McNally and others and another case* (2013) EWHC 2882 (Ch)

*Re Cawgate Ltd and others v Heller and others* (2004) All ER (D) 364

*Rawlinson and Hunter Trustees S.A. & Ors v Director of the Serious Fraud Office* (2014) EWCA Civ 1129

*Rawlinson and Hunter Trustees S.A. & Ors v Director of the Serious Fraud Office (No2)* (2014) EWCA Civ 1129

*Science Research Council v Nasse* (1979) 3 All ER 673

*Sclumberger Holdings v Electromagnetic Geoservices* (2008) EWHC 56

*Tchenguiz and others v Serious Fraud Office* (2014) All ER (D) 267

*Tchenguiz and others v Serious Fraud Office* (2014) EWCA Civ 1409

*Three Rivers v Bank of England No 4* (2002) All ER (D) 524

*West African Gas Pipeline Company Ltd v Willbros Global Holdings Inc* (2012) EWHC 396 (TCC)

*Woods v Martins Bank* (1958) 3 All ER 166

**South Africa**

*A Company v Commissioner, South African Revenue Service* 2014 (4) SA 549 (WCC)

*Blue Chip Consultants (Pty) Ltd v Shamrock* 2002 (3) SA 231 (W)

*Bogoshi v Van Vuuren* 1993 (3) SA 953 (T)

*Bosasa Operations (Pty)Ltd Basson* 2013 (2) SA 570 (GSJ)

*Bridon International GmbH v International Trade Administration Commission* 2013(3) SA197(SCA)

*Capalcor Manufacturing (Pty) Ltd v GDC Hauliers (Pty) Ltd (formerly GDC Hauliers* CC) 2000 (3) SA 181 (W)

*Centre for Child Law v The Governing Body of Hoerskool Fochville* 2016 (2) SA 121 (SCA) (8 October 2015

*City of Cape Town v South African National Roads Authority Limited and Others* [2015] ZASCA 58 (Cape Town v SANRAL)

*Democratic Alliance v African National Congress and Another* [2015] ZACC 1; 2015 (2) SA 232 (CC); 2015 (3) BCLR 298 (CC)
*Fedics Group (Pty)Ltd v Matus* 1998(2) SA 617 (C)

*FirstRand Bank Ltd t/a Wesbank v Manhattan Operations (Pty) Ltd* 2013 (5) SA 238 (GSJ)

*Gaertner & Others v Minister of Finance& Others* 2014 (1) BCLR 38 (CC)

*Governing Body of Hoerskool Fochville and Another v Centre for Child Law; In Re: Governing Body of Hoerskool Fochville and Another v MEC Education Gauteng and Others* 2014 (6) SA 561 (GJ)

*Harvey v Niland and Others* (5021/2015) [2015] ZAECGHC 149; 2016 (2) SA 436 (ECG)

*Independent Newspapers (Pty) Ltd v Minister for Intelligence Services: In re Masethla v President of the Republic of South Africa* [2008] ZACC

*Isparta v Richter and Another* 2013 (6) SA 529 (GNP)

*Jafta v Ezemvelo KZN Wildlife* (2009) 30 ILJ 131

*Le Roux and Others v Viana NO and Others* 2008 (2) SA 173 (SCA)

*Makate v Vodacom (Pty) Ltd* 2014 (1) SA 191 (GSJ)

*Multichoice (Proprietary) Limited and Others v National Prosecuting Authority and Another, In re: S v Pistorius, In re Media 24 Limited and Others v Director of Public Prosecutions North Gauteng and Others* [2014] ZAGPPHC 37 (Multichoice).

*My Vote Counts NPC v Speaker of the National Assembly and Others* 2016 (1) SA 132 (CC).

*My Vote Counts NPC v President of the Republic of South Africa and Others* (13372/2016) [2017] ZAWCHC 105 (27 September 2017)

*Ndlovu v Minister of Correctional Services* 2006 4 ALL SA165 (W)

*Pacifique v PerivanGuano Co* (1882) 11 QBD 55

*R v Special Commissioner of Income Tax* [2003] 1 A.C. 563.

*S v Agliotti 2011* (2) SACR 437 (GSJ)

*S v Mashiyi and Another* 2002 (2) SACR 387 (Tk)

*S v Ndiki and Others* 2008 (2) SACR 252 (Ck)

*S v Brown* 2016(1) SACR 206 (WCC)

*SABC v Avusa* 2010 (1) SA 280 (GSJ)

*Santam Ltd v Segal* 2010(2) SA 160 (N) at 165D-G;

*South African Airways Soc v BDFM Publishers (Pty) Ltd* 2016 (2) SA 561 (GJ)

*South African Broadcasting Corporation Limited v Director of Public Prosecutions, South Gauteng High Courts, Johannesburg and Others; In re: S v Krejcir and Others* [2014] ZAGPJHC 241

*Sihlali v South African Broadcasting Corporation Ltd* (2010) 31 ILJ 1477 (LC)

*The MV Urgup: Owners of the MV Urgup v Western Bulk Carriers (Australia) (Pty) Ltd and Others* 1999 (3) SA 500 (C)

*Thint (Pty) Ltd v National Director of Public Prosecutions; Zuma v National Director of Public Prosecutions* 2009 (1) SA 1 (CC)

*Transnet Ltd v MV Alina* 11 2013 (6) SA 556 (WCC)

**Unreported case law**

*Le Roux v The Honourable Magistrate Mr Viana and Others* case no 496/10 (SCA) dated 30 November 2007

*S v Oscar Leonard Pistorius* case no CC113/13 (reported).

**Legislation**

**United States of America**

Federal Rules of Civil Procedure (as amended 01 December 2015)

Federal Rules of Evidence

**United Kingdom**

Civil Procedure Rules,1998 (as amended 01 October 2010)

Civil Evidence Act

Freedom of Information Act

**South Africa**

Civil Proceedings Evidence Act 25 of 1965

Criminal Procedure Act 51 of 1977(As amended)

Cybercrimes Act, 19 of 2022

Electronic Communications Act 36 of 2005

Electronic Communications and Transactions Act 25 of 2002

Law of Evidence Amendment Act 45 of 1988

Legal Aid South Africa Act 39 of 2014

Magistrates' Court Act 32 of 1944

National Credit Act34 of 2005

Promotion of Administration of Justice Act 3 of 2000

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

Rules regulating the Conduct of Proceedings of the Magistrates' Court of South Africa

Rules Regulating the Conduct of Proceedings of the Several Provincial and Local Divisions of the High Courts of South Africa in terms of the Supreme Court Act

Superior Courts Act 10 of 2013

The Constitution of the Republic of South Africa,1996

**Internet Sources**

Creswell Report available at http://webarchive.nationalarchives.gov.uk/20110218200720/http://www.hmcourts-service.gov.uk/docs/electronic_disclosure1004.doc (last accessed on 06 August 2018.

Heyink, M "Electronic signatures for South African law firms' guidelines" (2014) Law Society of South Africa http://www.lssa.org.za/upload/LSSA%20Guidelines_Electronic%20Signatures%20for%20South%20African%20Law%20Firms_October%202014.pdf (accessed on 26 May 2015).

Hughes, K & Stander A "e-Discovery in South Africa and the Challenges it Faces" 2015 59-65. https://www.researchgate.net/publication/284173757_Ediscovery_in_South_Africa_and_the_Challenges_it_Faces (accessed on 02 August 2018). https://www.semanticscholar.org/paper/eDiscovery-in-South-Africa-and-the-challenges-it-Hughes-Stander/f3c6c0b8d7dd3eeebcf1c2d0ade308d0f05e39ed (accessed on 29 April 2022)

Infology "Comments and submissions in response to issue paper 27" http://www.infology.net/downloads/Infology%20Submission%20in%20response%20to%20Issue%20Paper%2027.doc.

LAWtrust makes history as the first accredited SA provider of advanced electronic signatures https://www.lawtrust.co.za/content/lawtrust-makes-history-first-accredited-sa-provider-advanced-electronic-signatures-0 (accessed 13 August 2014).

Practice Directive 1 of 2022 issued by Judge Mlambo that introduced CaseLines as well as the COVID19 Practice Directives of the South Gauteng High Court. Available at https://www.ppv.co.za/judge-presidents-practice-directive-1-of-2020/#:~:text=Practice%20Directives%20Judge%20President%20Mlambo%E2%80%99s%20first%20Practice%20Directive,High%20Courts%20with%20effect%20from%2027th%20January%202020 (last accessed on 22 September 2022).

Nkhwashu, N "Why the need for confidentiality on the content of Suspicious Transaction Reports?" http://www.derebus.org.za/need-confidentiality-content-suspicious-transaction-reports/ (accessed on 06 July 2018).

Pinnington, D "Why electronic documents are different" LAWPRO https://www.lians.ca/sites/default/files/presentations/why_electronic_documents_are_different-pinnington.pdf (accessed 26 April 2022 ).

Randburg Cases available at https://www.southafricanlawyer.co.za/article/2018/06/digital-letters-of-demand-the-way-forward/# (last accessed on 13 June 2022)

South African Law Reform Commission Discussion Paper 131 Project 126 "Review of the Law of Evidence" available at http://www.justice.gov.za/salrc/dpapers/dp131-prj126-ReviewLawOfEvidence.pdf accessed on 24 June 2018.

The Sedona Conference *"*Commentary on Protection of Privileged ESI*"* 2016 (17) *The Sedona Conference Journal* 108-109 https://thesedonaconference.org/sites/default/files/Handout%20-%202015%20Commentary%20on%20Protection%20of%20Prvileged%20ESI.PDF (last accessed on 29 April 2022)

The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (Second Edition) 2007 https://thesedonaconference.org/publication/Guidelines_for_Managing_Information_and_Electronic_Records (last accessed 10 June 2022)

The Sedona Conference Glossary: *E-Discovery & Digital Information Management*, *Third Edition* (2011) (accessed on 06 July 2018).

The Sedona Conference Glossary: *E-Discovery & Digital Information Management*, *Fifth Edition* (2020)

https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary (last accessed 10 June 2022)

Yang, M “The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response” https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1208&context=njtip (accessed 26 April 2022).