F Cassim
Associate Professor,
Department of Criminal
and Procedural Law,
University of South Africa

DOI: https://dx.doi.org/
10.18820/24150517/
JJS42.v1.2

ISSN 0258-252X (Print)
ISSN 2415-0517 (Online)

Journal for Juridical
Science
2017 42(1):19-40

The use of electronic discovery and cloud-computing technology by lawyers in practice: Lessons from abroad

Abstract

In the present electronically driven world, it is vitally important for lawyers to understand advancing or new technology and to have adequate computer literacy in order to best represent their clients. The so-called "e-information explosion" requires lawyers to request, produce and manage electronic documents in order to protect their clients' interests and to obtain a strategic advantage over their opponents. Lawyers or legal practitioners should adapt to technological changes, develop an awareness of the unique challenges posed by the advances in technology, and embrace technology's role in both their practices and the legal system. This article examines issues pertaining to electronic discovery and cloud-computing technology in civil practice in South Africa, the United States of America and the United Kingdom. The article also examines current electronic discovery (e-discovery) practices and the use of cloud-computing technology in the United States of America and the United Kingdom to ascertain whether useful lessons can be gleaned from these jurisdictions for possible incorporation into South African law. The study notes that, while South African law has taken great strides to address advancing technology, useful lessons from abroad can be adopted such as, *inter alia*, the need for greater preservation of electronic evidence; the use of a wider definition of the term 'document' to include all types of electronic information and future technological developments; the amendment of the rules to include the discovery of electronically stored information; the use of the proportionality principle in trials, and the incorporation of the cost-shifting regime. The article concludes that lawyers need to learn more about relevant law such as the *ECT Act* and *POPI*, and embrace advancing technology more enthusiastically, yet responsibly, in order to succeed in their new competitive and changing legal environments and to provide the best service for their clients.

1. Introduction

A common feature of the current digital or electronic age is the constant use of written communication between individuals by way of e-mails, text messages and social media rather than by conventional letters.[1] This has resulted in numerous documents being created, transmitted and signed electronically. Many lawyers are realising that a basic understanding of technology and computer proficiency is essential to litigate a case effectively.[2] The so-called "e-information explosion" requires lawyers to request, produce and manage electronic documents in order to protect their clients' interests and to obtain a strategic advantage over their opponents.[3] The use of electronic evidence in litigation is increasing, with some American commentators calling it "explosive" and a "tsunami".[4] Therefore, it is essential that legal practitioners adapt to technological changes, develop an awareness of the unique challenges posed by the advances in technology, and embrace technology's role in both their practices and the legal system.

The purpose of discovery is to ascertain from other parties to the action what information or documentation exists that might be relevant to the action. This enables a party to properly prepare for trial and prevents that party from being taken by surprise at the trial.[5] The question thus arises in this digital age as to whether parties have discovered relevant electronic documents in their possession. A failure to disclose may be prejudicial to the other party's case. Therefore, lawyers need to improve their discovery techniques to include electronically created and stored data. However, extreme care should be taken to protect confidential data during the discovery process.[6]

Electronic discovery refers to the discovery of electronically stored information (ESI).[7] This includes e-mail, web pages, word-processing files, computer databases and any information that is stored on a computer or other electronic device. On the other hand, paper discovery refers to the discovery of printed words that can be read without the aid of electronic devices. This shift from a paper-based environment to an electronic environment requires lawyers to ensure and maintain confidentiality of client information in electronic records and communications.

---

1 Cassim 2013:85.
2 Wall & Lange 2003:31. Note that the terms 'lawyers' and 'legal practitioners' will be used interchangeably, and that this article will focus on civil practice.
3 Wall & Lange 2003:31.
4 Coumbe 2004:130.
5 The aim is also to avoid "incontrovertible points of debate". See also *Hall v Multilateral Motor Vehicle Accidents Fund* 1998 4 SA 195 C 1991; Hughes & Stander 2016.
6 Nelson & Simek 2005:42.
7 Cassim 2013:86.

Searching for ESI can be challenging and expensive.[8] Modern technology has transformed traditional discovery to the extent that lawyers find it to be a constant challenge to keep abreast. The challenges have led to calls to amend the existing legislation in order to address the obstacles.

This article examines issues pertaining to electronic discovery and cloud computing in civil practice in South Africa, the United States of America and the United Kingdom. The purpose of the examination of current e-discovery practices and the impact of cloud-computing technology in the United States of America and the United Kingdom is to ascertain whether useful lessons can be gleaned from these jurisdictions for incorporation into South African law. The article concludes that lawyers need to embrace technological changes such as electronic discovery and cloud-computing technology in their practices more enthusiastically, yet responsibly, in order to thrive in their new competitive and changing legal environments and to best represent their clients' interests.

2. Electronic discovery (E-discovery)

Discovery in civil practice is aimed at preparation for trial, and prevents one party from being taken by surprise at the trial.[9] Previously, discovery took place by way of paper documents; however, this has changed with the advent of the digital era. Electronic discovery refers to the discovery of ESI, and includes the storage of information using computers and digital media.[10] The discovery of relevant data and information in ESI is called e-discovery.[11] It is submitted that, in the present electronic age, many lawyers are using their computers and digital media to store their files and documents. This leads to discovery by electronic means or electronic discovery, which can be distinguished from traditional paper discovery. The use of the traditional paper discovery medium in trials may result in lawyers spending a large amount of time on document management activities instead of researching the law and formulating successful trial strategies.[12] Electronic discovery has been punted as one of the most significant practical opportunities to improve the experience of litigation, while ensuring the delivery of the best professional service to clients in the electronic information age.[13] In foreign jurisdictions, provision has been made for ESI by either issuing practice directions or amending the rules

8 In the current electronically driven world, lawyers are communicating more, and processing and storing information electronically in an increasing and ever-changing media. This can be challenging. See Brown 2011:18.

9 See rule 35 of the Uniform Rules of Court and rule 23 of the Magistrates' Courts Rules that apply in South Africa; Hughes & Stander 2016. It should be noted that rule 26 of the Federal Rules of Civil Procedure and rule 31 of the United Kingdom Civil Procedure Rules apply to discovery in the United States of America and the United Kingdom, respectively.

10 Cassim 2013:86; Araiza 2011:7.

11 Hughes & Stander 2016.

12 Hughes 2012:25.

13 Hughes 2012:24.

of court, such as by expanding the definition of 'document' to include electronic information in the United Kingdom, or by inserting specific provisions for the discovery of electronic information as in the United States of America.[14]

E-mail messages are easier to discover, because they are quite often forwarded and passed to individuals or groups and the senders and recipients can examine the precise words used in the e-mail messages. E-mail messages may also contain vital information to a trial or embarrassing information pertaining to the plaintiff. To illustrate this, in *Leslie v Boston Software Collaborative Inc*,[15] the production of e-mails demonstrated the plaintiff's difficult personality, which was found to be embarrassing. Lawyers are also urged to take appropriate measures to protect their clients' metadata from becoming public until the court orders such disclosure.[16] Metadata refers to background information embedded in a document, such as a user's name, comments on the documents, different document versions, and the names of servers.[17] An example of inadvertent disclosure of a client's metadata occurred when Microsoft furnished its annual report in a downloadable Word format in 1999 from its website; however, Microsoft's failure to remove its metadata from the report revealed that part of the document was prepared on a Macintosh computer.[18] It is important to notify all parties of one's intention to conduct electronic discovery early in the trial or case in order to avoid destruction of potentially relevant information.[19] Therefore, a client should preserve all electronic data at the outset of the case. Extreme caution should also be taken to protect confidential data in electronic documents.[20]

Electronic discovery is not without criticism. It is regarded as being complex and expensive because of, *inter alia*, the huge volume and number of data messages; the problem of metadata; the changing status of electronic contents; the impact of technological changes on data; the use of different locations of electronic data, and the expenses involved in

14 Van Dorsten 2012:34.

15 *Leslie v Boston Software Collaborative Inc* 2002 Mass Super Lexis 57 (Mass Super 12 February 2002). This case dealt with the termination of a shareholder's employment in a close corporation that performed software consulting services. The termination resulted from complaints by employees regarding the shareholder's treatment of them in the workplace and complaints from customers about the quality of the shareholder's work. Records of email correspondences produced in court provided evidence of the shareholder abusing the employees, and this proved embarrassing to the shareholder (plaintiff) who sought reinstatement of his employment. See also Bacon 2003:19.

16 Bacon 2003:20; Araiza 2011:7.

17 Coumbe 2004:133.

18 Bacon 2003:20.

19 Bacon 2003:20.

20 It has been mooted that a confidentiality agreement is the cornerstone for protecting data during the discovery phase. See Nelson & Simek 2005:43-44.

the process.[21] While the courts have readily admitted electronic evidence in criminal cases,[22] there is a dearth of case law on the admissibility of electronic evidence in civil trials in South Africa.

The issue of which party bears the costs of electronic discovery is also problematic. According to Coumbe, the traditional position is that the costs of discovery, production and inspection are borne by the party making the discovery.[23] However, with electronic discovery, cost shifts to the requesting party, especially when electronic discovery imposes a heavy burden on the producing party.[24] In the American case of *Rowe Inc v William Morris Agency Inc*,[25] the court prescribed eight factors to determine whether to shift the costs of production to the requesting party. In some cases, American courts have also required parties to split the costs of electronic discovery.[26]

Similarly, in South Africa, the question has arisen as to which party bears the costs of electronic discovery. It was advocated that the courts should either refuse to order discovery if the request is not specifically tailored to discover relevant information, or shift the cost to the requesting

21 Cilliers *et al*. 2009:810-813. According to Basset, the huge number of electronic documents and communications raises issues of burdensomeness that can result in huge expense and inconvenience. See Bassett (2010:437) and Hughes & Stander (2016) regarding the differences between ESI and paper documents.

22 See *inter alia, Ndlovu v Minister of Correctional Services and Another* 2006 4 All SA 165, where the court had to ascertain, *inter alia*, whether a copy of a computer printout complied with the best evidence rule and whether it could be admitted into evidence unless properly proved. The court admitted into evidence the computer printout not in terms of sec. 15 of the *Electronic Communications and Transactions Act 25/2002 (ECT Act)*, but in terms of the court's statutory discretion in terms of the *Law of Evidence Amendment Act* 45/1988. The case received criticism because of its failure to provide clarity on the impact of sec. 15 of the *ECT Act* on the authenticity rule and the hearsay rule. See Collier (2005:6-9) in this regard. See also *S v Ndiki and Others* 2008 2 SACR 252, where the court's finding that part of the computer-based evidence constituted real evidence was lauded by academic writers. See Cassim 2013:89.

23 See Coumbe 2004:130-134; Nelson & Simek 2005:47.

24 This applies particularly in the United States of America and in New Zealand, where the courts consider factors such as purpose of the request, the availability of using other sources, and the feasibility of costs of production. Coumbe 2004:130-134.

25 *Rowe Inc v William Morris Agency Inc* 2002 US Dist Lexis 8308 (SD NY May 9 2002). In this case, the court ordered the requesting party to pay for the costs of the electronic discovery. The court set out eight factors, which included issues such as whether the discovery requests are narrowly tailored; the likelihood of retrieval of important information; the availability of information from other sources; the reason for retention of information; the benefit to the parties; the total costs; the ability of each party to control costs, and the parties' resources.

26 See *In re Bristol-Myers Squibb Securities Litigation* 205 FRD 437 (2002). See also the discussion in 5.2 below.

party when electronic discovery imposes an undue burden or expense on the producing party.[27]

3. The use of cloud-computing technology in legal practice

Cloud-computing technology is not a recent phenomenon. The term is used to describe third party-hosted services that run server-based software from a remote location.[28] Cloud-computing technology makes it easier for clients to access their data or run applications from any location with an Internet connection.[29] Cloud computing may offer benefits such as flexibility and affordable technologies.[30] However, it may also be problematic, as it places client data under the control of a third party cloud service provider, which may be risky and lead to contentious legal issues.[31] It is accepted in foreign law societies and international bar associations that lawyers may use cloud-computing technologies in their law practice. However, it is emphasised that such lawyers must ensure that "reasonable protective measures", sufficient safeguards and adequate technical solutions are taken to protect the confidentiality of sensitive client information.[32] This also protects the ethical responsibilities of lawyers towards their clients. The determination of "reasonable protective measures" will consider the facts and circumstances of each case; however, guidance can also be sought from legal organisations such as the Law Society of South Africa's electronic security guidelines.[33] Lawyers should, therefore, be aware of their ethical duties and responsibilities and how these duties impact on cloud computing. They should guard against the inherent risks with employing such technologies in their practice, keep abreast of changes to

27 See Cillers *et al*. 2009:813; *Rubico (Pty) Ltd v Paywell (Pty) Ltd* 2001 2 All SA 671 (W). In the *Rubico* case, the court was asked to interpret rule 35 of the Uniform Rules. Rule 35 discusses the discovery, inspection and production of documents.

28 LSSA Guidelines 2015:4. It is submitted that cloud-computing technology is commonly used by technologically savvy lawyers who are embracing the electronic age.

29 Araiza 2011:1. In this article, the writer maintains that the United States Federal Rules of Discovery should be amended to provide relevant guidelines and exceptions for shared data.

30 LSSA guidelines 2015:4; Araiza 2011:5.

31 To illustrate this, the data may be subject to foreign laws; it may create liabilities for clients if they inadvertently retrieve ESI belonging to other clients, and it may provide clients with avenues to avoid divulging certain information. See also Araiza (2011:3, 9-13) regarding the various problems that may arise.

32 As noted by the New Hampshire Bar Association in the United States of America. See also the LSSA Guidelines 2015:4. Technical solutions include the use of a hybrid approach; the tracking of metadata, and the use of encryption technology. See Araiza 2011:3, 16-17.

33 See LSSA Guidelines 2015:4.

the law and their practices, understand what cloud-computing technology means and its impact on their practices, use the services of third parties after careful screening, and comply with legislation such as the *Protection of Personal Information Act 4* of 2013 in South Africa.[34]

It has been mooted that the use of electronic discovery platforms has made discovery for litigation more efficient.[35] Although placing documents by a service provider on a database system for review does not translate to waiver of privilege; sharing access to that database with opposing attorneys may amount to a waiver of privilege if privileged documents are disclosed to the other party.[36] Therefore, lawyers must take adequate steps to protect client data from inadvertent disclosure.

The above discussion demonstrates that cloud computing may lead to new complexities or challenges with the discovery phase of litigation. Therefore, lawyers must learn to use new technologies responsibly and ethically, and ensure that they do not compromise their clients' rights. They must also ensure that the third party service providers have implemented security protocols. It has also been recommended that South African lawyers host their data with a local company or a South African service provider to avoid extra-territorial seizure of data and to avoid being subject to laws of foreign countries regarding their data.[37]

4. Legislation in South Africa

It is submitted that South Africa does have legislation in place to address the discovery process and the protection of electronic data (as demonstrated below).

4.1 Uniform Rules and Magistrates' Courts Rules

In terms of the Uniform Rules of the High Court and the Magistrates' Courts Rules, litigants or parties are required to make discovery on oath of all documents relating to the matter in question in litigation, and to make available those documents for inspection.[38] The party who fails to discover in terms of a discovery request may be compelled to do so, failing which the court may make an adverse order as to costs or dismissal of the action.[39]

34 See LSSA Guidelines (2015:6) regarding a summary of internationally accepted duties; Bennet 2011:45. See also the discussion in 4.3 on the *Protection of Personal Information Act* 4/2013.
35 LSSA Guidelines 2015:8.
36 LSSA Guidelines 2015:8.
37 LSSA Guidelines 2015:9-10.
38 See Uniform Rule 35 of the High Court and Magistrates' Courts Rule 23, respectively.
39 See, for example, Magistrates' Courts Rule 23(8) and Uniform Rule 35(7), respectively, in this regard.

In the High Courts, rule 35 applies. According to rule 35(15) of the Uniform Rules, a tape recording includes a sound track, film, magnetic tape, record or any other material on which visual images, sound or other information can be recorded. Thus, the definition of tape recording appears wide enough to encompass all types of material on which visual images, sound and other information may be stored. However, Uniform Rule 35 does not specifically address the discovery of ESI.[40] The position regarding ESI is challenging in the present electronic age, where documents are electronically or digitally stored *vis-à-vis* the storage of hard copies. The electronic storage of documents poses challenges regarding the discovery of such documents.

Some courts have accorded an extended definition to the word 'document' in facilitating the discovery of electronic documents. In *Le Roux v The Honourable Magistrate Mr Viana*,[41] the court held that the definition of a tape recording in rule 35(15) is wide enough to include all ESI. However, the court did not pronounce on the question as to whether such ESI must be in readable format or not. In *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd and Another (WCC)*,[42] the court found that tapes on which a company backed up its electronic information were discoverable. Parties may also request courts to direct the discovery of ESI.[43]

Rule 23(1) of Magistrates' Courts Rules provides that a notice requesting discovery by one party may require the other party to discover all documents and tape, electronic, digital and other forms of recordings relating to any matter in question in such action, whether such matter is a matter arising between the above-mentioned parties which are or have been in the possession or control of such other party. Thus, rule 23 facilitates the discovery of electronic and digital forms of recordings. Rule 23 is a step in the right direction. However, rule 23 has been criticised for not adequately addressing the discovery of ESI.[44]

4.2 *Electronic Communications and Transactions Act* 25 of 2002 *(ECT Act)*

The *Electronic Communications and Transactions Act* 25 of 2002 (*ECT Act*) was introduced to address the use of electronic evidence in criminal

40 See Van Dorsten 2012:36.

41 *Le Roux v The Honourable Magistrate Mr Viana* case number 494/06, dated 30 November 2007.

42 *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd and Another (WCC)*. Unreported case number 10264/10, dated 19 August 2011.

43 See *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services: In re Masetlha v President of the Republic of South Africa and Another* 2008 SA 31 CC 41F-42B.

44 According to Van Dorsten (2012:36), Magistrates' Courts Rule 23 does not address the discovery of ESI. It only addresses electronic and digital recordings.

cases.[45] It was introduced to primarily address cybercrime. Although this is an omnibus *Act*, dealing with everything from electronic signatures to domain names, it also incorporates some very important sections on admissibility of evidence. The admissibility of a printout in court in terms of the *Computer Evidence Act* 59 of 1983 provided much legal uncertainty, and practitioners found this *Act* to be cumbersome. This led to the promulgation of the *ECT Act*, which aims, *inter alia*,

> 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 for electronic communications, transactions and the use of electronic transactions by SMMEs; to prevent abuse of information systems and to encourage the use of e-government services.

The *ECT Act* introduced the concept of a "data message", which refers to data generated, sent, received or stored by electronic means.[46]

The *ECT Act* creates a rebuttable presumption that data messages or printouts are admissible in evidence.[47] It is submitted that written communication such as e-mails, electronic documents attached to e-mails, webpages and SMS messages fall under the concept 'data' in terms of the *ECT Act*. Therefore, the admissibility and evidential weight of such data can be determined in terms of the provisions of the *ECT Act*.[48] The *ECT Act* provides that the requirement of an original document is met if the person produces an electronic copy of a data message.[49] However, the method of generating the electronic form of that document must provide a reliable means of assuring the continued integrity of the information in that document.[50] The question also arises as to whether document metadata

45 Due to technical difficulties with electronic evidence, a need for new legislation arose. See South African Law Reform Commission 2010:21.

46 See sec. 1 of the *ECT Act*, which defines a data message as data generated, sent, received or stored by electronic means. See also Collier 2005:7.

47 See secs 14 and 15 of the *ECT Act*. Sec. 14 addresses the integrity of a data message or electronic document. Sec. 15 provides that the rules of evidence must not be used to deny admissibility of data messages on the ground that it is not in its original form. See *Ndlovu v Minister of Correctional Services and Another* 2006 4 All SA 165 W, where the court used its discretion to admit documents in terms of its statutory discretion to admit hearsay evidence rather than sec. 15 of the *ECT Act*. See also Collier (2005:7-8) for a discussion about the case.

48 See also Hughes 2012:24.

49 See secs 14 and 17 of the *ECT Act*.

50 Hughes 2012:25.

constitutes the best evidence.[51] The *ECT Act* is considered to be the most important piece of legislation affecting digital evidence.[52]

The *ECT Act* has impacted on the Uniform Rules of Court by facilitating service of documents through the electronic medium.[53] Rule 4A of the Uniform Rules incorporates some provisions of the *ECT Act* by requiring service by facsimile or electronic mail. It is no longer necessary for service to be effected by the sheriff, who usually explains to a party the nature and contents of a document being served. Service may thus be effected by hand, registered post, facsimile, and electronic mail. However, it is still necessary for the originals of documents to be filed with the Registrar in terms of rule 4A.[54]

4.3 The *Protection of Personal Information Act 4* of 2013 (POPI)

The *Protection of Personal Information Act* 4 of 2013 *(POPI)* was signed into law during November 2013, although it has not yet been enacted in its entirety. Certain regulatory or administrative sections such as sec. 1, Part A of Chapter 5, secs 112 and 113 have been enacted.[55] *POPI* promotes, *inter alia*, the protection of personal information processed by private and public bodies; provides for the protection of the rights of persons regarding unsolicited electronic communications; provides for the introduction of certain conditions so as to establish minimum requirements for the processing of personal information, and regulates the flow of personal information across the borders of South Africa.[56] *POPI* regulates the

51 The best evidence rule originates from the English law of evidence, and involves the practice of admitting the best alternative to evidence, which has been lost or destroyed. This alternative evidence is now regarded as the "best evidence" under the given circumstances. It should be noted that the best evidence rule is found in sec. 15(1) of the *ECT Act*, which prohibits the "rules of evidence" from excluding the admissibility of a data message on the grounds that it is not in its original form if it represents the best evidence that the person adducing it could reasonably be expected to obtain. See Van der Merwe *et al*. 2016:119-120. Regarding metadata, refer to 2 above. See also Hughes (2012:25-26), who discusses the importance of metadata to litigation lawyers. See also Bacon 2003:19-20.

52 Hughes & Stander 2016.

53 See rule 4A of the Uniform Rules. Rule 4A addresses service of all documents and notices not falling under rule 4(1)(a) on a party to the litigation at the chosen address of the party in terms of the rules of court for service of such documents and notices. The documents and notices so excluded refer to processes directed at the sheriff, which initiates application and action proceedings.

54 It should be noted that the original documents may be filed with the registrar by way of hard copies and not by facsimile or the electronic medium.

55 See GK Government Gazette 2014:25 (37544). These sections came into effect on 11 April 2014. It is submitted that a majority of the sections of *POPI* will only commence at a later date to be proclaimed by the President.

56 See *inter alia*, chapters 3, 9 and 11 of *POPI*. Chapter 3 regulates the conditions for the lawful processing of personal information; chapter 9 regulates trans-

manner in which personal information may be processed by establishing conditions prescribing minimum standards for the lawful processing of personal information.[57] *POPI* defines 'personal information' as "information relating to an identifiable, living natural person and where applicable, an identifiable, existing juristic person",[58] and 'data subject' as the "person to whom personal information relates".[59] The term 'processing' refers to any operation or activity or set of operations, whether or not it takes place by automatic means, relating to personal information, and it includes, *inter alia*, the collection, receipt, recording, storage, retrieval or use of information, whereas the term 'record' refers to any recorded information regardless of the form or medium.[60] It is submitted that both confidential legal data and client personal information may be stored in the cloud. Thus, it may be argued that *POPI* (which protects personal information) may be used to protect sensitive client information stored in the cloud.

POPI places obligations on companies to process personal information responsibly.[61] *POPI* also requires data collectors to register with the Information Regulator.[62] Individuals can request companies to provide information free of charge as to whether or not they hold personal data of the individual and to whom such data was disclosed.[63] Companies including Internet service providers and providers of cloud-computing services will have to implement appropriate, reasonable and organisational measures

---

border information flows, and chapter 11 regulates offences, penalties and administrative fines. It should be noted that sec. 72 specifically regulates the transfer of personal information outside South Africa.

57 See sec. 2(b) of *POPI*.

58 It should be noted that the term 'electronic communications' refers to any text, voice, sound or image message sent over an electronic communications network, which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient. See chapter 1 of *POPI*.

59 It is submitted that the term 'personal data' may refer to electronic representations of personal information. A 'data collector' could refer to the 'operator' who processes the personal information of the natural or juristic person in terms of a contract or mandate.

60 It is submitted that the term 'processing' may incorporate the use and storage of personal information by traditional or conventional means (such as written format) and electronic means. See chapter 1 of *POPI* for a detailed definition of key terms.

61 See sec. 19 of *POPI*. To illustrate this, companies cannot collect personal information without the prior consent of the individuals and they cannot divulge or sell personal information to other companies for marketing purposes. See secs 19 and 69 of *POPI* in this regard.

62 The Information Regulator refers to a juristic person established in sec. 39 of *POPI*. Sec. 40 sets out the duties and functions of the Regulator, which include, *inter alia*, providing education on the *Act* to private or public bodies and data subjects; monitoring and enforcing compliance by private and public bodies regarding the *Act*, and handling complaints about alleged violations of the *Act*. It should be noted that the National Assembly only approved members of the Information Regulator during September 2016. Advocate Pansy Tlakula has been appointed as the chairperson. See Anonymous 2017.

63 See sec. 23 of *POPI*.

to prevent the unauthorised use of personal information, and invest in new technologies such as encryption and access control.[64] A written agreement should be concluded between the service provider and the lawyer who requires the service provider to establish and maintain reasonable measures to protect the security, integrity and confidentiality of sensitive client information. Sec. 21 places an obligation on companies such as Internet service providers to notify the individual of any unauthorised use or disclosure of personal information to afford the individual to take protective measures.[65] Internet service providers have to appoint Information Protection Officers to ensure compliance with provisions of the *Act*.[66] *POPI* prescribes fines of R10 million or imprisonment of 10 years if companies (such as Internet service providers) do not respect personal information and handle it with utmost care and responsibility.[67] Data subjects whose personal information has been breached have recourse to civil remedies in terms of sec. 99 of the *Act*.[68]

It has been mooted that, while *POPI* establishes safeguards for the confidentiality and integrity of personal information, its provisions reflect lawyers' professional obligations to maintain the confidentiality and integrity of their client information.[69] It is, therefore, important for lawyers to understand *POPI* in order to protect the confidentiality and integrity of client information processed in electronic form.

4.4 Case law

Courts have taken a progressive approach towards the impact of technology on the law. In the case of *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens*,[70] the court granted leave for a notice to discover to be served by way of substituted service[71] and directed that service be effected by way of a Facebook message addressed to the defendant. It should be noted that this was an exceptional case and its application was

64 See sec. 19 of *POPI*.

65 To illustrate this, the theft of an employee's computer must be disclosed to every person whose data is at risk.

66 See sec. 55 in chapter 5 of *POPI* regarding duties and functions of such officers.

67 See secs 107, 108 and 109 of *POPI*.

68 The Information Protection Regulator may pursue civil actions for damages for breach of *POPI's* provisions, and a court hearing the matter may award a just and equitable amount including payment of damages as compensation for patrimonial and non-patrimonial loss suffered by the data subject.

69 Heyink 2015:31. See also LSSA Guidelines 2013:1-49.

70 *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens.* Unreported case, KwaZulu-Natal High Court, Durban case number 6846/2006, dated 3 August 2012.

71 Substituted service is an extraordinary method of service, since it deviates from the normal method of service provided for in the rules. An application is made to the High Court for leave to sue by substituted service where a person is believed to be within the Republic, but service cannot be effected on him/her in terms of the Rules, because it is not known precisely where such person is living/residing.

not restricted to summonses. In *Le Roux and Others v Viana and Others*,[72] the court found that books and documents recorded on a computer drive fell within the contemplation of sec. 69(3) of the *Insolvency Act* 24 of 1936; thus, recognising the relevance of electronic storage of documents. It was advocated that courts should either refuse to order discovery if the request does not specifically address the discovery of relevant information, or shift the costs to the requesting party when electronic discovery imposes an undue burden or expense on the producing party.[73] One needs to examine the intention behind the request and the question of burden or expense to the producing party in awarding costs in electronic discovery.

The above cases demonstrate the progressive approach of courts towards advancing technology.

4.5 Summary

An exploratory study to determine the status and challenges of e-discovery in South Africa indicated that e-discovery is not commonly used by lawyers, and that the major challenges are the lack of knowledge and education among lawyers and their clients.[74] Many lawyers perceive e-discovery as a costly exercise rather than a legal necessity, although some lawyers are aware of the procedures.[75] It appears that lawyers need to be more educated about the process and benefits, and be more prepared about the process.[76] According to Heyink, lawyers are reticent about embracing the information revolution and recognising the benefits it holds for the profession.[77] However, a recent study by the Law Society of South Africa indicated that South African lawyers are increasingly using online services, using technology 'smartly' and undertaking digital research regularly in their practices.[78]

The above discussion demonstrates that lawyers in South Africa are aware of the procedures involving technology such as e-discovery and cloud-computing technology. Legislation is in place to address the impact of technology such as e-discovery and the protection of sensitive client information. The question arises as to whether the legislation is adequate to address the challenges posed by advancing technology.

72 *Le Roux and Others v Viana and Others* 2008 2 SA 173 SCA. This case related to the winding up of a property where the liquidator took over the property.
73 Cilliers *et al*. 2009:813.
74 Hughes & Stander 2016.
75 Hughes & Stander 2016.
76 Hughes & Stander 2016.
77 Heyink 2015:31.
78 Law Society of South Africa Report 2016:1-45. It should be noted that this study examined the evolution of South African law firms as they responded to challenges facing the profession in 2016.

5. The position in the United States of America (USA)

5.1 Legislation

In 2006, the Federal Rules of Civil Procedure (FRCP) were substantially revised in order to make discovery of ESI more manageable. This entails that ESI is now a relevant aspect of discovery requests and responses.[79] The revised Rules also require the requesting party to specify the form in which ESI is to be produced.[80] Rule 34 of the FRCP refers to the production of documents and ESI.[81] The use of the phrase "electronically stored information" is considered to be broad enough to cover all present types of computer-based information and flexible enough to address future changes and developments.[82] The revised Rules place emphasis on "reasonable accessibility" to control e-discovery burdens, which means that the responding party has to show that a particular source of information is not reasonably accessible when asked to produce the information.[83] Rule 26 imposes a specific limitation on the discovery of ESI, namely the precondition of reasonable accessibility.[84] Rule 26 encapsulates the duty to disclose and contains provisions governing discovery.[85] The court has the final discretion to order the production of such documents, but it may impose certain conditions.[86] One can minimise preservation disputes by addressing them at the outset of the litigation, such as at planning conferences.[87] A great deal of emphasis is thus placed on early communications between the parties to resolve disputes. It should be noted that Federal Rule 502 addresses privileged and work-product protected information.[88] Rule 37 of the FRCP contains the sanction provisions for failure to make disclosures or to co-operate in discovery requests. Rule 37(e) specifically addresses the failure to preserve ESI. The

79 Brown 2011:18. See also Foggo *et al*. 2007:2.
80 See Federal Rule of Civil Procedure 34(b)(1)(C).
81 Federal Rule 34(a)(1) refers to discovery of "data compilations from which information can be obtained". Rule 34(a) thus facilitates the request for production and inspection of any ESI in any medium.
82 Araiza 2011:7.
83 Federal Rule 26(2). See also Brown 2011:18; Noyes 2007:53.
84 Basset 2010:438. See also Foggo *et al*. 2007:2.
85 Rule 26A(ii) refers to ESI.
86 Federal Rule 26(b)(2)(B).
87 See Federal Rule 26(f). It should be noted that Federal Rule 26(f) applies to both state proceedings and federal court-mandated arbitration proceedings.
88 Rule 502(e) facilitates agreements that permit parties to produce ESI with little or no preproduction review and to return any privileged documents produced without any waiver. A party may request the court to make the agreement an order to safeguard it (Federal Rule 502(d)). Federal Rule 502(d) is regarded as a valuable tool to minimise the risks of discovery. Brown 2011:19.

above rule requires courts to examine the intent of the parties in order to prescribe the relevant sanction.

As stated earlier, lawyers also need to be educated about information storage in order to ascertain what information is or is not reasonably accessible.[89] It has been mooted that a lawyer's clear and accurate explanation of how his/her client's computer system works can be persuasive in any e-discovery dispute.[90] Lawyers also need to anticipate discovery requests and preserve ESI as soon as a claim seems likely in order to avoid discovery sanctions. To this end, lawyers should act professionally and co-operate in discovery requests. The above guidelines will assist a lawyer in "reining in e-discovery".[91]

5.2 Relevant case law

The *Zabulake v UBS Warburg LLC* case[92] is regarded to be the leading American case on e-discovery. The issue arose regarding the discovery of e-mail messages archived on back-up tapes and the question of who was responsible for the costs of recovering the tapes. The court concluded that some of the electronic information stored on back-up tapes was not reasonably accessible. However, it ordered the restoration and production of a sample of back-up tapes that would provide "tangible evidence".[93] E-discovery requests require additional reasonableness standards such as reasonable accessibility for production, reasonable care in preservation, and disclosure of evidence.[94] It has been mooted that American courts should employ an objective reasonable standard to fulfil the aim of FRCP 26, which was introduced to accommodate e-discovery and technological developments.[95]

The issue of proportionality has been raised in American case law. Rule 26(b)(2) of the FRCP grants courts the power to limit discovery if the proposed discovery is found to be more burdensome or expensive than the likely benefit. This means that judges may use their discretion to limit discovery if it is clear that costly and burdensome discovery will unlikely lead to the disclosure of relevant information.[96] The balancing exercise involves weighing the burden over benefit of electronic discovery. In *Kaufman v Kinko Inc*,[97] the defendant argued that the burdens of the retrieval process outweighed any evidentiary benefit that the plaintiff

89 See Federal Rule 34. This can be done with the aid of technical support staff.
90 Brown 2011:20.
91 Brown 2011:20.
92 *Zabulake v UBS Warburg LLC* 217 FRD 309 (SDNY 2003). It should be noted that the case was decided before the amended FRCP. See also Coumbe (2004:130-133) for a discussion about the case.
93 *Zabulake v UBS Warburg LLC*:324.
94 Basset 2010:436.
95 Basset 2010:453-454.
96 Wall & Lange 2003:32.
97 *Kaufman v Kinko Inc* Civ. Action No 18894-NC (del. Ch Apr 16 2002).

would obtain from the documents requested. The court found this to have no persuasive force. The court granted the plaintiff's motion to compel the defendant's production of certain e-mail messages retrieved from the back-up system, and thus the court found in favour of a good faith request to examine the relevant information.[98] It should be noted that the proportionality analysis also applies even to non-parties.[99] The question arises as to whether lawyers can avoid rule 26(b) by ensuring that their requests are just and not burdensome. The courts provided some guidance in *Tulip Computers International v Dell Computer Corp*,[100] where the plaintiff's electronic proposal requesting the defendant to list e-mails and show compliance with privilege and confidentiality disclosures, was found to be fair, efficient and reasonable.

Federal and state courts have uniformly ruled that information stored on electronic media is discoverable.[101] The American experience shows that Congress and the judiciary are demonstrating a strong commitment to preserving records that could be relevant in future lawsuits or governmental proceedings.[102] To illustrate this, in *Antioch v Scrapbook Borders Inc*,[103] the court ordered the defendant to preserve all data on the computer at issue, and requested the defendant to appoint a neutral computer expert to collect electronic evidence.

5.3 Cost implications

Electronic discovery can be expensive. The traditional view was that the responding party is responsible for the expense of complying with a discovery request. However, the courts have shifted some or all of the expense obligations to the requesting party.[104] The spiralling costs of electronic discovery were examined in *Rowe Entertainment Inc v William Morris Agency Inc*,[105] where the court shifted the cost of discovery to the requesting party, basing its decision on the needs of justice and the resources of the parties. The court adopted an eight-factor balancing test

98 *Kaufman v Kinko Inc* Civ. Action No 18894-NC (Del. Ch Apr 16 2002).

99 See *Braxton v Farmers Insurance Group* 2002 WL 31132933 (ND Ala. Sept 13 2002). This case involved a class action suit in terms of the *Fair Reporting Act*, where e-mail correspondence from a non-party insurance agent was sought. The court agreed with Farmers Insurance that the non-party insurance agents would be subjected to an undue burden, and it instead followed a more proportional approach of having the defendant locate and produce relevant e-mail, newsletters, and other relevant electronic correspondence.

100 *Tulip Computers International v Dell Computer Corp* 2002 WL 818061 (D. Del Apr 30 2002).

101 Bacon 2003:18. See also *Linnen v AH Robbins Co Inc* 1999 Mass. Super Lexis 240 at 16.

102 Wall & Lange 2003:31.

103 *Antioch v Scrapbook Borders Inc* 2002 WL 31387731 (d. Minn. Apr 29 2002).

104 Wall & Lange 2003:33; Foggo *et al*. 2007:2-3.

105 *Rowe Entertainment Inc v William Morris Agency Inc* 205 FRD 421 (SDNY 2002). See also 2003 US Dis LEXIS 12643 (SDNY 24 July 2003).

involving the following criteria: the availability of data from other sources; the parties' financial resources; the type of request; the likelihood of success for data retrieval; the reason for data retention; the benefit of production; the total costs, and the availability and incentive to control costs.[106] Similarly, in *Zabulake*, the court adopted a seven-factor cost-shifting test.[107] Thus, in the United States of America, the courts have compelled the requesting party rather than the producing party to bear the costs of discovery. Parties have also been sanctioned for "bad-faith manoeuvring or rule violations".[108] Therefore, parties must exercise due care and caution in complying with discovery requests.

5.4 Summary

The above provisions demonstrate the importance of electronic discovery in the United States of America, with amended FRCP encompassing ESI. Rule 502, which applies to privilege and waiver in e-discovery, is regarded as a valuable tool to minimise the risks of discovery. The wide definition given to ESI is encouraging, as it can address future changes and developments in technology.

The American experience demonstrates the wide and flexible approach towards electronic information. However, the Federal Rules of Civil Procedure have been criticised for not effectively addressing the use of cloud technology.[109] The American courts provide some useful guidelines regarding cost-shifting, which could be invoked by South African courts.

106 *Rowe Entertainment Inc v William Morris Agency Inc* 205 FRD 421 (SDNY 2002).

107 The seven factors encompassed the following issues: the extent to which the request is specifically tailored to discover relevant information; the availability of such information from other sources; the total cost of production *versus* the amount payable; the total cost of production compared to the available resources; the ability of each party to control the costs and its incentive to do so; the importance of issues at stake in the litigation, and the relative benefits to the parties to obtain the information. It was held in a subsequent decision that the responding party must bear the costs of reviewing and producing electronic data once it has been converted into an accessible form. See 2003 US Dis LEXIS 12643 (SDNY 24 July 2013).

108 Wall & Lange 2003:33.

109 Araiza 2011:18.

6. The position in the United Kingdom (UK)

6.1 Legislation and case law

The UK Court Rules were amended during October 2005 to include new requirements for the disclosure of electronic documents.[110] In terms of the UK Civil Procedure Rules, the word 'document' is defined as "anything in which information of any description is recorded".[111] The definition of 'document' includes electronic documents, including e-mail and other electronic communications, word-processed documents, databases, documents stored on servers and back-up systems, documents that have been deleted, and metadata.[112] Thus, the definition is fairly wide and comprehensive and includes documents stored on portable devices such as memory sticks and mobile phones. The reason for the wide definition is said to encourage and assist parties to reach agreement in relation to disclosure of electronic documents in a proportionate and cost-effective manner.[113] The Civil Procedure Rules relating to discovery were also amended to reflect the importance of metadata. The definition of 'document' in the Rules now specifically includes "additional information stored and associated with electronic documents known as metadata".[114]

The English courts place emphasis on electronic disclosure and any failure may amount to gross incompetence.[115] The English courts also consider the criterion of proportionality in achieving justice, scrutinising the importance of documents, the amount in dispute, the ease and cost of production, and the financial resources of the parties. This has resulted in the limitation of the scope of electronic disclosure by the courts, with parties required to specify the scope of their searches for electronic documents and to prove the necessity of such production in order to ensure fair disposal of the case.[116] As in the United States of America, parties also need to preserve documents from the outset of the litigation process; case management conferences are held to resolve disagreements

110 Foggo *et al*. 2007:5.
111 See rule 31.4.
112 See rule 31.4. It is submitted that documents stored on servers could include documents stored in the cloud.
113 See Anonymous 2016. It should be noted that the Practice Directions relate to civil litigation only.
114 See United Kingdom Civil Procedure Rules "Practice Directions 31 A-Disclosure and Inspection" Part 31A 2A, and Part 31B-Disclosure of electronic documents.
115 See *Earles v Barclays Bank PIC* [2009] EWHCI (Mercantile Court). See also Van Dorsten 2012:34.
116 See Foggo *et al*. (2007:5) regarding how the parties approach electronic disclosure. See also *Digicel (St Lucia) v Cable Wireless* [2008] EWHC 2522 (Ch) (23 October 2008) regarding what constitutes "reasonable search".

between parties.[117] Courts give directions where parties are unable to reach agreement regarding disclosure.[118]

In the United Kingdom, the "loser pays regime" is followed. The losing party has to pay the winning party the costs of disclosure and inspection.[119] This has resulted in less frequent cost-shifting orders in the United Kingdom; however, the courts have a wide discretion regarding awarding costs. To this end, the court can order the disclosure of specific electronic data including inaccessible data and order that the receiving party pay some or all of the disclosing party's costs of production.[120]

6.2 Summary

The UK experience demonstrates that a wide definition is given to the word 'document' in the Civil Procedure Rules to address the disclosure of electronic information; the definition includes the concept of "metadata"; the adherence to the principle of proportionality by the courts to achieve fairness and justice in disputes; the use of case management conferences to facilitate resolution of disagreements, and the use of the "loser pays regime" in the UK has resulted in fewer cost-shifting orders.

7. Conclusion

Discovery seeks to appraise parties to a trial of the relevant documentary evidence, and to facilitate the administration of justice. It is important in the current electronically driven world for discovery to include ESI, as the use of e-mails and electronically stored data has transformed the discovery process. Clients and opposing parties keep a significant amount of information on their computers and electronic devices. Therefore, it is important for attorneys to learn about the basics of electronic discovery in order not only to educate their clients about the effect of electronic discovery, but also to assist attorneys in effectively presenting their cases. It has introduced new strategies and trial tactics that could lead to a party winning or losing a case. Lawyers should also anticipate potential discovery problems and co-operate with opposing attorneys to expedite the matter. Lawyers should no longer use excuses such as technological ignorance, antiquated systems and delays with obtaining discovery to avoid using electronic discovery, but embrace advancing technology. Indeed, judges expect lawyers to seek technological solutions for the problem that technology poses.[121] Therefore, lawyers must keep abreast of advancing technology and become more technically savvy in this information or digital age. They must examine more efficient ways to best serve their clients'

117 Foggo *et al*. 2007:6.
118 Foggo *et al*. 2007:6.
119 Foggo *et al*. 2007:6.
120 Foggo *et al*. 2007:6.
121 Wall & Lange 2003:33.

interests. They must also use cloud-computing technology cautiously and ensure that their service contracts include safeguards to protect sensitive client data.

It is submitted that South Africa does have legislation in place to address the impact of technology such as the Uniform Rule 35, the Magistrates' Courts Rule 23, the *ECT Act*, and *POPI*. However, there is room for improvement, as the definition of 'electronic document' in the Rules is not wide enough to include all types of possible electronic information or incorporate future changes or technological developments. Neither do our Rules adequately address the discovery of ESI. Therefore, South Africa can learn from the approaches in the United States of America and the United Kingdom. Our Rules need to be amended to, *inter alia*, reflect the following: greater preservation of electronic evidence; widen the definition of 'electronic document'; address the discovery of ESI; include the need for early conferences between parties at the outset of litigation to facilitate resolution of disputes; our courts should follow the principle of proportionality in achieving fairness and justice in trials involving electronic information, and our Rules should incorporate the guidelines set out in *Rowe* and *Zabulake* regarding the cost-shifting regime.

There is an urgent need for better and cheaper legal services in order to keep pace with the demands of a rapidly globalising world. There has been a growth in the use of information and communication technologies in South African legal practices over the past few years, as demonstrated in the 2016 Law Society Report. It is important to make technology work for all participants in the justice system, as it enhances access to justice for all citizens. The use of advancing technology should reduce rather than increase the justice gap. Our lawyers should learn to understand relevant law such as the *ECT Act* and *POPI*, and embrace appropriate technologies more enthusiastically, yet responsibly, in their practices.[122] Lawyers should learn new skills or amend their current skillset to adjust to the changing legal landscape, and to fulfil their professional responsibilities and duties to their clients, thus ensuring compliance with the time-honoured standard of a litigant's right to a fair trial.[123]

122 See also Heyink 2015:32.

123 Moseneke DCJ in *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services: In re Masetlha v President of the Republic of South Africa and Another* 2008 5 SA 31 CC 41F-42B.

Bibliography

ANONYMOUS

2016. *CPR Rule and Directions.* https://www.justice.govt.uk/courts/procedures-rules/civil/rules/Part 31 (accessed on 30 September 2016).

2017. *Information Regulator* (South Africa). https://www.justice.gov.za/inforeg/index.html (accessed on 16 February 2017).

ARAIZA AG

2011. *Electronic discovery in the cloud*. Duke Law and Technology Review 10(1):1-18.

BACON G

2003. *The fundamentals of electronic discovery*. Boston Bar Journal 47:19-20.

BASSET DL

2010. *Reasonableness in e-discovery*. Campbell Law Review 32(3):435-454.

BENNET SC

2011. *E-discovery meets the cloud*. NYSBA Journal May:45-46.

BROWN GS

2011. *Reining in e-discovery*. Litigation 37(4):18-20.

CASSIM F

2013. *Use of electronic evidence in South African law*. In Jaishankar K and Ronel N (eds) 2006:85-93.

CILLIERS AC, LOOTS C & NEL HC

2009. *Discovery, inspection and production of documents*. In Herbstein J & Van Winsen LdV 2009:810-813.

COLLIER D

2005. *Evidently not so simple: Producing computer printouts in court*. Juta's Business Law 13(1):6-9.

COUMBE G

2004. *E-Discovery. The New Zealand Law Journal* April:130-134.

FOGGO G, GROSSO S, HARRISON B & RODRIGUEZ-BARRERA JV

2007. *Comparing e-discovery in the United States, Canada, the United Kingdom and Mexico.* American Bar Association 8(4):1-7.

HERBSTEIN J & VAN WINSEN LDV

2009. *The civil practice of the High Courts of South Africa and the Supreme Court of Appeal of South Africa*. 5th ed. Volume 1. Cape Town: Juta.

HEYINK M

2015. *Why are South African lawyers remaining in the dark with POPI?* De Rebus August:30-33.

HUGHES B

2012. *The rise of electronic discovery*. De Rebus January/February:24-26.

HUGHES K & STANDER A
2016. *E-discovery in South Africa and the challenges it faces*. Paper presented at the Second International Conference on Information Security and Cyber Forensics. Cape Town, November 2015. https://www.researchgate.net/publication/284173757 (accessed on 3 March 2016).

JAISHANKAR K & RONEL N (EDS)
2006. *Global criminology: Crime and victimization in the globalized era*. Boca Raton, FL: CRC Press Taylor and Francis Group.

LAW SOCIETY OF SOUTH AFRICA REPORT
2016. *Attorneys' profession in South Africa*. Durban: LexisNexis.

LSSA GUIDELINES
2013. *Protection of personal information for South African law firms*:1-49.

2015. *Use of internet-based technologies in legal practice*:1-12.

NELSON SD & SIMEK JW
2005. *Preparing for electronic discovery*. GPSolo:42-47.

NOYES HS
2007. Good cause is bad medicine for the new e-discovery rules. *Harvard Journal of Law and Technology* 21(1):50-96.

SOUTH AFRICAN LAW REFORM COMMISSION
2010. *Review of the law of evidence* (Electronic evidence in criminal and civil proceedings: Admissibility and related issues). Issue paper 27: Project 126:18-46.

VAN DER MERWE DP, ROOS R, PISTORIUS T, EISELEN GTS & NEL SS
2016. *Information and communications technology law.* 2nd ed. Durban: LexisNexis.

VAN DORSTEN J
2012. *Discovery of electronic documents and attorneys' obligations.* De Rebus November:34-36.

WALL CD & LANGE CS
2003. *Recent developments: Electronic discovery*. Washington Lawyer March:31-33.