Case Comments

Electronic Wills with an Aura of Authenticity: *Van der Merwe v Master of the High Court and Another*

SYLVIA PAPADOPOULOS
University of Pretoria

1 Introduction

We live in what has been termed 'a quicksilver technological environment'. Regardless of perceived ethical or enforcement limitations, laws have become increasingly significant in applying general principles to the electronic environment. Some people will argue that 'technology can be just as powerful as the law in constraining or regulating digital activity' (F Fitzgerald et al *Internet and E-Commerce Law: Technology, Law, and Policy* (2007) at 1–2).

In line with our own 'quicksilver' technological environment, Van Staden and Rautenbach convincingly argue that the formality requirements of the Wills Act 7 of 1953 for validly executing a will have not kept up with technological advances, and that there is an increasing need for this statute to provide for electronic wills. This is relevant because technology such as electronic signatures significantly reduces the possibility of fraud. By using and understanding technology, the integrity and genuineness of an electronically executed will can be ensured (André R van Staden & Christa Rautenbach 'Enkele Gedagtes oor die Behoefte aan en die Toekoms van Elektroniese Testamente' (2006) 39 *De Jure* 586; cf DP van der Merwe 'How Standards (such as XML) Accomplish Electronic Authentication in Web Services' (2005) 26 *Obiter* 665). I support this view.

The Electronic Communications and Transactions Act 25 of 2002 ('ECTA') stipulates that it must not be interpreted to give validity to the execution, retention and presentation of a will or codicil (s 4(3) read with Sched 1 and s 4(4) read with Sched 2). Yet in some circumstances the courts are prepared to condone electronic wills under s 2(3) of the Wills Act (*Macdonald and Others v The Master and Others* 2002 (5) SA 64 (O); *Van der Merwe v The Master and Another* 2010 (6) SA 544 (SCA)). In this respect, legislation clearly needs to reflect the reality of the increased use of technology. What is even more serious is that electronic wills are being condoned without reliance on the safety mechanisms built into the 'functionally equivalent' provisions of

Cite as: (2012) 24 *SA Merc LJ* 93–106.

ECTA (due to the exclusions) and without reference to technology that could ensure the integrity and genuineness of a will in the form of a data message.

2 Executing a Valid Will

For a will to be validly executed, it must be signed at the end by the testator or by some other person in his presence and by his direction (s 2(1)(*a*)(i) of the Wills Act). The signature must be made by the testator or by such other person or be acknowledged by the testator and, if made by such other person, also by that other person, in the presence of two or more competent witnesses present at the same time (s 2(1)(*a*)(ii)). The witnesses must attest and sign the will in the presence of the testator and of each other and, if the will is signed by such other person, also in the latter's presence (s 2(1)(*a*)(iii)). If the will consists of more than one page, each page other than the page on which it ends must also be signed by the testator or by such other person anywhere on the page (s 2(1)(*a*)(iv)). And if the will is signed by the testator by making a mark or by some other person in the presence and by the direction of the testator, a commissioner of oaths must be present and certify that the formalities have been met (s 2(1)(*a*)(v)).

The references to pages of the will (s 2(1)(*a*)(iv) and 2(1)(*a*)(v)), and the requirement that it must be signed by the testator in certain specified places (s 2(1)(*a*)(i) and 2(1)(*a*)(iv)), imply that the will must be in the form of a written document (Juanita Jamneck et al *The Law of Succession in South Africa* (2009) at 66).

The reason for the formality requirements for a valid will as set out in s 2(1) of the Wills Act is that in

> 'ancient law the execution of a will was regarded as a solemn act and was vested with a high degree of formality. The retention of a measure of formality in modern law is designed to curtail opportunities for fraud and to ensure as far as possible that wills reflect the genuine and voluntary disposition of the testator' (MM Corbett et al *The Law of Succession in South Africa* 1 ed (1980) at 36)'.

Section 2(1)(*a*) of the Wills Act prescribes that a will must be in writing, signed, and attested by two competent witnesses; and that the testator must sign every page. Under the condonation section of the Wills Act, the courts only have the ability to condone non-compliance with the formalities of s 2(1). Courts cannot, for instance, grant condonation to witnesses that are not qualified to inherit (MJ de Waal & MC Schoeman-Malan *Law of Succession* 4 ed (2008) at 67). For a court to exercise its power to condone, three requirements have to be proved on a balance of probabilities:

- There is a document;
- That was drafted or executed by a person who has since died; and
- That was intended to serve as a last will of the deceased (s 2(3) of the Wills Act).

The third requirement is seen as the most important. It must be clear from the surrounding circumstances that the testator wished the specific document

to serve as his or her last will and testament (De Waal & Schoeman-Malan op cit at 70).

3 The Revolutionary Concept of Functional Equivalence

The Electronic Communications and Transactions Act took its cue from the United Nations Commission for International Trade Law Model Law on Electronic Commerce adopted on 12 June 1996 with the additional article 5 *bis* adopted in 1998 (the UNCITRAL Model Law). This Model Law introduced and reinforced what was a revolutionary concept at the time – functional equivalence. This approach was based on an analysis of the purposes and functions of traditional paper-based requirements and their adaptation for electronic commerce (see *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 With additional article 5 bis as adopted in 1998* at 20 ('the UNCITRAL Guide'), available at *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf* (visited on 15 October 2010)).

The UNCITRAL Guide identified a paper document as serving the following functions:

- to provide that a document is legible by all;
- to remain unaltered over time;
- to allow for reproduction of the document so that each party would hold a copy of the same data;
- to allow for authentication of the data by means of signature; and
- to provide a document in a form that would be acceptable to public authorities and the courts (par 16 at 20).

Significantly, the Guide (at 21) also noted that, as regards all these functions of paper, electronic records can at least provide an equal level of security, and in most cases a much higher degree of reliability and speed, especially for identification of the source and content of the data, provided that a number of technical and legal requirements are met.

The Electronic Communications and Transactions Act establishes its sphere of application in s 4, and applies to any electronic transaction or data message. An 'electronic transaction' is not defined in s 1 of ECTA. However, a 'transaction' is either of a commercial or a non-commercial nature and it includes the provision of information and e-government services. Looking at the s 1 definitions for the phrases 'electronic agent', 'electronic communication' and 'electronic signature', with data as the common denominator, one could surmise that electronic transactions include transactions where the use of data, or electronic representations of information in any form, is intrinsic to the transaction.

This Act also applies to transactions that are concluded in the form of 'data messages'. 'Data messages' are described in s 1 as data that is generated, sent, received or stored by electronic means, and that includes a voice where it is used in an automated transaction and a stored record.

The implementation of the functional equivalent approach in our law is evident in ECTA provisions such as the following:

- legal recognition of 'data messages' (s 11(1));
- compliance with an 'in writing' requirement (s 12);
- 'electronic signatures' (s 13);
- the requirement that information be presented in an 'original' form (s 14);
- the 'admissibility and evidential weight of data messages' (s 15);
- 'notarisation, acknowledgement and certification' of documents (s 18); and
- the formation of valid agreements by way of data messages (s 22).

In the light of the requirements for the valid execution of a will ('mainly in writing' and 'signature'), the two functionally equivalent ECTA provisions most relevant to this discussion are s 12 and s 13.

A legal requirement that a document or information must be in writing is met under s 12 of ECTA if the document or information is in the form of a data message and it is accessible in a manner that is usable for subsequent reference.

As regards the signature requirement, s 13 of ECTA states that if the law does not specify the type of signature required, the requirements in relation to a data message are only met if an advanced electronic signature is used.

An advanced electronic signature is an electronic signature that results from a process which has been accredited by the Authority as provided for in s 37 (s 1 of ECTA). Certain criteria that must be met before the Accreditation Authority can accredit an electronic signature service or product. These criteria include the following, that the signature:

- is capable of identifying the user;
- is uniquely linked to the user;
- is created using means that can be maintained under the sole control of the user;
- will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable; and
- is based on the face-to-face identification of the user (s 38 of ECTA).

The South African Accreditation Authority (SAAA) released accreditation regulations in *Government Gazette* No 2995 on 20 June 2007 so that the applications for advanced electronic signatures accreditation could commence. According to the SAAA website, one service provider's product has been accredited so far (see *http://www.saaa.gov.za* (last visited 21 August 2012)).

Despite these provisions, when it came to wills and codicils Parliament unfortunately opted to remove wills from the ambit of ECTA. Sections 11 to 16 and 18 to 20 of ECTA do not apply to the Wills Act (s 4(3) of ECTA read with Sched 1). Most notably, these are the provisions that give legal effect to 'data messages' and provide functional equivalence to concepts such as in

'writing' and 'electronic signatures'. Furthermore, ECTA must not be interpreted so as to give validity to any transaction listed in Schedule 2 of the Act (s 4(4)). This list in Schedule 2 includes the execution, retention and presentation of a will or codicil as defined in the Wills Act.

The reason for specifically excluding wills and codicils from ECTA's sphere of application is not clear. It suffices to say that wills were almost universally excluded from the ambit of e-commerce legislation worldwide (cf ch 10, s 2(4)(*a*) of the British Columbia Electronic Transactions Act, S.B.C. 2001 (available at *http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_01010_01*); s 2(3)(*a*) of the Uniform Law Conference of Canada's Uniform Electronic Commerce Act 1999 (available at *http://www.ulcc.ca/en/us/index.cfm?sec'1&sub'1u1*); and the American Electronic Signatures in Global and National Commerce Act (E-SIGN), PL 106–229, 14 stat 464 Title 15 chpt 96 adopted in 2000 §7003 (available at *http://www.law.cornell.edu/uscode/15/usc_sec_15_00007003–000-.html*). A notable exception is the Nevada statute: Title 12 Wills and Estates of Deceased Persons Chapter 133 NRS 133.085 (available at *http://www.leg.state.nv.us/nrs/NRS-133.html NRS133Sec085* (last visited 11 May 2011)).

When it came to the issue of accepting video or filmed wills as valid under the Wills Act, the South African Law Commission decided that because the Master's procedure for controlling estates and wills did not allow for this type of digital expression of intention, they could not accept these wills as valid in our law (*Review of the Law of Succession* Project 22 (1991) at 167). Corbett simply states that these wills were not acceptable to the Commission because at the time this step was regarded as too revolutionary (Corbett et al op cit at 57; James Thomas Faber & Pierre Jacques Rabie 'Van Tikmasjien tot Rekenaar: 'n Ondersoek na die Ontwikkeling van die Suid-Afrikaanse Erfreg in die Tegnologiese Era' 2005 *Tydskrif vir die Suid-Afrikaanse Reg* 767 at 777).

So it seems that when the exclusions in ECTA were drafted, the approach of functional equivalence was new to the law, and technological aspects were treated with caution. It seems to have been too extreme to allow electronically represented wills or wills in the form of data messages to be considered functionally equivalent to a validly executed paper-based will.

Since then, however, although ECTA states that it should not be interpreted so as to give validity to the execution, retention and presentation of a will or codicil as defined in the Wills Act, the Supreme Court of Appeal has been prepared to condone an unsigned will in the form of a data message under s 2(3) of the Wills Act (*Van der Merwe v Master of the High Court* (supra)). This judgment is critically analysed in the light of its broader implications for our law and compared to an earlier decision (*Macdonald v The Master* (supra)). I will argue that this exclusion should be revised for the sake of legal certainty.

4 Condonation under s 2(3) of the Wills Act and *Macdonald v The Master*

Macdonald v The Master was the first case to condone a will in the form of a data message. It was decided before ECTA came into operation. The deceased, an information technology specialist, left a note indicating that his will was located on his personal computer at his workplace. He also left specific instructions, including relevant passwords on how and where to retrieve the document (supra at 67–9).

To reach the conclusion to condone the will, the Court also considered a number of objective factors. These included the following: the documents clearly indicated the deceased's intention; there was no suspicion of fraud; they were protected by a password; and, on the facts, only the deceased could have typed the document (at 72C–F). The Court held (at 71I–J):

> 'The deceased's will was indeed a document that was stored in his computer in accordance with his instructions. On a flexible interpretation of s 2(3), it may be regarded as having been drafted by him personally.'

The documents were also drafted by the deceased, who had since died, and they were intended to be his will (at 71I–J, 72C–F).

Much was written in reaction to the *Macdonald* decision. Most commentators cautiously approved of it. So, for instance, Steve Cornelius remarked that this case

> 'can be construed as setting a precedent in terms of which documents stored on electronic media can be condoned as wills in terms of section 2(3) of the Wills Act. . . . However, while the liberal and technology-friendly approach of the court in this case should be welcomed, care should be taken not to view this case as introducing such sweeping reforms' ('Condonation of Electronic Documents in terms of Section 2(3) of the Wills Act 7 of 1953' 2003 *Tydskrif vir die Suid-Afrikaanse Reg* 208 at 210).

Faber and Rabie (op cit at 780) remarked that

> 'dit behoort klaarblyklik in die lig van wat hierbo opgemerk is oor die relatiewe onbelang van die medium waarin die wilsuiting vervat is. . . . Daar word toegegee dat 'n riskante gebied betree word, maar soos aangedui sal word, behoort die vereiste van omringende omstandighede hier 'n belangrike rol te speel'.

And MC Wood-Bodley said:

> '[N]otwithstanding Hattingh J's reliance on the now discredited liberal approach to s 2(3) in rescuing Macdonald's will, I submit that the outcome of *Macdonald* can still be supported and is to be welcomed ('*Macdonald v The Master*: Computer Files and the ''Rescue'' Provision of the Wills Act' (2004) 121 *SALJ* 34 at 42–3; see also idem 'Wills, Data Messages, and the Electronic Communications and Transactions Act' (2004) 121 *SALJ* 526).

Even more has been written on interpreting s 2(3) of the Wills Act, which is in itself controversial. (See MM Corbett et al *The Law of Succession in South Africa* 2 ed (2002) at 58–65; JT Faber & PJ Rabie 'Die Behoefte aan 'n Wyer Artikel 2(3) van die Wet op Testamente 7 van 1953 (soos gewysig): 'n Kritiese Beskouing' (2004) 29 *Tydskrif vir Regswetenskap* 198; JT Faber & PJ Rabie 'Praktiese Wenke met die Opstel en Verlyding van Testamente en die Kondonering van Vormgebrekkige Dokumente' 2006 *Tydskrif vir Boedelbeplanningsreg* 72; MC Schoeman-Malan 'Kondonasie vir die Opstel en Verlyding van 'n Testament Ingevolge Artikel 2(3) van die Wet op Testamente

7 van 1953' (2003) 36 *De Jure* 414; and JC Sonnekus 'Kondonering van Vormgebrekkige Testamente? Vergeet Dit!' (2003) 14 *Stellenbosch LR* 337.)

These controversies resurfaced in *Van der Merwe v Master of the High Court* (supra). I predict that the issues surrounding electronic wills will continue to come before courts, perhaps in increasing numbers.

5 *Van der Merwe v The Master of the High Court*

5.1 Facts and Decision

Van der Merwe, the appellant, was a very close friend of the deceased. The two friends had decided that they would each execute a will making the other the sole beneficiary of their respective deceased estates. So the deceased, Van Schalkwyk, sent Van der Merwe an e-mail on 26 July 2007, containing the contested will with Van der Merwe as the sole beneficiary. Van der Merwe reciprocated and drafted his own will, naming Van Schalkwyk the sole beneficiary.

The deceased did not execute the document e-mailed to the appellant. Nor did he meet any of the formalities under s 2(1)(*a*) of the Wills Act. The document was still stored on his computer when he died. The appellant was also the sole beneficiary of the deceased's pension fund. An earlier, validly executed will dated 23 September 2004 had bequeathed the entire estate to the Society for the Prevention of Cruelty to Animals (the second respondent) (*Van der Merwe v Master of the High Court* (supra) pars 2–6).

After Van Schalkwyk died, the appellant applied to the South Gauteng High Court to have the e-mailed document declared the deceased's last will and testament under s 2(3) of the Wills Act (par 7). The Court a quo dismissed the application. Tsoka J held that as regards the e-mailed document, in the absence of a signature it would be

> 'impossible to link a document alleged to be a Will, to the testator. In this instance one cannot speak of a Will, otherwise any document as long as it contains the particulars of the testator, may be characterized as a Will' (par 9).

The Supreme Court of Appeal considered two questions (par 15): did the deceased draft or execute the document? If so, did he intend it to be his last will and testament?

The Court unanimously held that a lack of signature had never been a complete bar to a document being declared a valid will in terms of s 2(3) of the Wills Act. The very object of this section 'is to ameliorate the situation where the formalities have not been complied with but where the true intention of the drafter of a document is self-evident' (par 16).

The Court then examined several objective factors leading it to conclude that the Court a quo had erred in dismissing the application, that the document was drafted by the deceased, that it had not been amended, and therefore that the Master should be directed to accept the document drafted by the deceased as the deceased's last will and testament for the purposes of the

Administration of Estates Act 66 of 1965. These factors included the following (pars 17–9):

- There was proof that the document had been sent to Van der Merwe by the deceased;
- The document still existed on the deceased's computer;
- The document had a bold heading reading 'Testament';
- The deceased nominated Van der Merwe as the sole beneficiary of the pension fund proceeds: this was important because it accorded with an intention that the appellant should be the sole beneficiary;
- There was no other immediate family;
- The previous will indicated that the deceased had no intention of benefitting remote family members; and
- The appellant, in response to receiving the e-mailed document, had executed a will nominating the deceased as his sole beneficiary (ie, further proof of their mutual agreement).

6 Commentary

6.1 What about the ECTA exclusion?

This was the second time that the courts condoned, through s 2(3) of the Wills Act, a will that only existed in the form of a data message. It is clear from both cases that the courts were influenced by the surrounding circumstances (objective factors) when deciding to condone the wills.

On the topic of s 4(3) and s 4(4) of ECTA read with Schedules 1 and 2, the specific exclusion, Wood-Bodley, relying on the interpretation clause s 3 of ECTA, noted that '[a]lthough the ECT Act does not authorize the execution of a valid will in electronic form, there is nothing in the Act that would prevent the application of the rescue provision of section 2(3) of the Wills Act to a will that exists as a data message' (op cit (2004) *SALJ* 526 at 527).

This is the dichotomy we now confront. Because of the realities of the computer age, the court is prepared, on a case-by-case basis, and taking into account the surrounding circumstances, to accommodate wills in the form of data messages, despite the possible effect that the ECTA exclusion may have on these documents. As more of these cases reach the courts it may be possible to argue that the ECTA exclusion has been reduced to the point where it is redundant in our 'quicksilver' technological age. The question is therefore: would it not be more judicious to use the ECTA provisions in so far as they may assist in confirming the authenticity and integrity of these documents?

6.2 The 'in Writing' Requirement

6.2.1 Legibility and reproduction

The first requirement of s 2(3) of the Wills Act – that there be a document – indicates that at a minimum it must be in writing (De Waal et al op cit (2008)

at 70; MC Schoeman & A van Der Linde 'Artikel 2(3) en 2A van die Wet op Testamente – Kondonasiebevoegdheid van die Hof – Verlyding en Herroeping van Testamente' (1995) 58 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 517 at 523; Corbett et al op cit (1980) at 58; Faber & Rabie op cit 2005 *Tydskrif vir die Suid-Afrikaanse Reg* at 775). This is also true for the valid execution of a will in terms of the requirements in s 2(1).

The main functions served by a written document are inter alia to provide that (1) a document is legible by all; (2) that it remains unaltered over time; (3) that it can be reproduced so that each party would hold a copy of the same data; (4) to allow for authentication of the data by means of signature and (5) to provide a document in a form that would be acceptable to public authorities and the courts (UNCITRAL Guide to Enactment of the Model Law op cit at 20).

Wood-Bodley argues that the High Court decision in *Macdonald* (supra), decided before ECTA was in operation, did not depend on the actual recognition of the data message or computer file (a series of binary numbers stored on a hard drive) as a document in writing, for the purposes of s 2(3) of the Wills Act, because the document was printed out and presented to the Court in its hard-copy format. Therefore it was the written, printed-out, hard copy of the document that was recognised as the last will and testament of the deceased (op cit (2004) 121 *SALJ* at 39 and 43). This was most likely because no legal recognition of data messages as 'writing' existed before ECTA was promulgated.

By contrast, *Van der Merwe* (supra) was decided by the Supreme Court of Appeal when ECTA was applicable. Similarly, though, this decision centred on whether the printed-out, unsigned, written, hard-copy document could be declared the will of the late Mr van Schalkwyk and not on the recognition of the data message itself, as a valid will.

De Waal and Schoeman-Malan accept that the 'in writing' requirement could include a document in the form of a data message. They rely on an analysis of dictionary meanings attributed to the word 'writing' and refer to s 3 of the Interpretation Act 33 of 1957 (De Waal et al (2008) at 70; MC Schoeman-Malan & A Van der Linde 'Kondonasie vir die Opstel en Verlyding van 'n Testament Ingevolge Artikel 2(3) van die Wet op Testamente 7 van 1953' (2003) 36 *De Jure* 414 at 420–2).

Wood-Bodley (op cit (2004) 121 *SALJ* at 41) engages in a similar exercise in respect of the word 'document' and concludes that

> '[a] theme common to most of these definitions is the function of storing information or evidence, the material on which this may be stored varies . . . and therefore does not appear to be crucial . . . [The] increasingly widespread use of computers and computer files to perform this function can arguably justify the inclusion of such computer files within the meanings of the term document. . .'.

Most would, I think, agree that a document or will in the form of a data message would meet the functions of legibility and reproduction, and that if all the functions listed above in points (1) to (4) were accommodated, then the

document would be one step closer to being acceptable to the courts and public authorities. The UNCITRAL Guide considers this to be the lowest level of the 'in writing' requirement. The Guide also notes that: 'The requirement that data be presented in written form (which can be described as a ''threshold requirement'') should thus not be confused with more stringent requirements such as ''signed writing'', ''signed original'' or ''authenticated legal act''' (at 35–6).

In this respect at least, s 12 of ECTA provides that if the document or information is in the form of a data message and it is accessible in a manner that is usable for subsequent reference, it meets the requirement of 'in writing'.

Thus it leaves meeting the functions of remaining unaltered and being available for signature as significant stumbling-blocks to recognising wills in the form of data messages as valid.

6.2.2 Remaining Unaltered Over Time

In *Macdonald* (supra) a great deal of care was taken to ensure that the parties could clearly show that the integrity of the data message had been maintained, with a number of objective factors that the Court could rely on (at 68D–69B).

In *Van der Merwe* (supra) it is not evident from the judgment which methods, if any, were employed to ensure that the integrity of the data message had been maintained. The judgment merely mentions that there was proof that the deceased had sent the document to Van der Merwe (presumably a printout of the e-mail) and that it still existed on the deceased's computer. Presumably, it had not been deleted or perhaps the contents of the e-mailed will were compared to the document on the deceased's computer hard drive to ensure that they were identical. Nevertheless, the Supreme Court of Appeal held that as the appellant had provided 'proof' that that the will had been sent to him by the deceased via e-mail, and that it lent 'the document an aura of authenticity' (par 17).

I submit that at the very least, the Court should have referred to the ECTA provisions aimed at assisting in the determination of:

(1) whether the integrity of the data message was retained;
(2) the testator's intention to communicate the document as his will under the rules of attribution in terms of s 25 of ECTA; and
(3) the fact that it was sent by the testator and received by the beneficiary before the testator's death by referring to the deceased's computer and information system used to communicate the will.

In maintaining the integrity of a data message, ECTA stipulates that in any legal proceedings, information in the form of data messages should be given its due evidential weight. In assessing the evidential weight of a data message, ECTA requires that regard must had to the reliability of the manner in which the data message was generated, stored or communicated, the reliability of the

manner in which the integrity of the data message was maintained, the manner in which the originator was identified, and any other relevant factor (s 15(1)–(4)).

These subsections stipulate that a data message can be considered an 'original' if the integrity of the information has been maintained from the time when it was first generated in its final form as a data message and it is capable of being displayed or produced. The integrity of a data message has to be assessed 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 or display; in the light of the purpose for which the information was generated; and having regard to all other relevant circumstances (s 14; cf s 17 regarding the production of a document or information).

As regards the retention of data messages, the information contained in the data message must be accessible so as to be usable for subsequent reference; the data message must be 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 the origin and destination of the data message and the date and time it was sent or received must be capable of being determined (s 16).

It is trite that the Supreme Court of Appeal or any other court adjudicating on cases such as these is not bound to follow these specific systematic steps to ensure that the integrity of a data message will has been maintained, because s 4(3) of ECTA read with Schedule 1 ensures that these evidentiary sections designed to assist with functional equivalence do not apply to the Wills Act. But this does not mean that the court is not bound to apply all other applicable rules of evidence: it merely means that the legitimate benefit of these sections is foregone, when condoning a will that only exists as data message at the time of the testator's death. Compare also *Ex parte Porter and Another* 2010 (5) SA 546 (WCC), where a proper case for relief under the common law could be made out that an executed codicil to a will had been lost, and the Court was satisfied on the evidence that the reconstruction of the lost document through an e-mailed electronic record of the text of the document was both accurate and complete. In reaching this conclusion, the Court referred to *Ex parte Gowree* 1915 CPD 108; *Ex parte Ntuli* 1970 (2) SA 278 (W); and *Nell v Talbot* 1972 (1) SA 207 (D).

The UNCITRAL Guide (op cit at 49) suggests that provisions dealing with the attribution of data messages to the originator are intended to apply only where there is a question whether a data message was really sent by the person who is indicated as being the originator. The purpose of such a provision is not to assign responsibility, but rather to attribute the data messages, by establishing a presumption that, in certain circumstances, a data message would be or could be considered a message of the originator, unless the addressee knew or ought to have known that the data message was not that of the originator.

I return to the question of whether we can ensure that data messages remain unaltered over time, thus allowing the law to facilitate the recognition of data messages as validly executed wills. We can, through the use and understanding of metadata.

Metadata is usually described as data about data. Metadata includes contextual, processing and use information that is used to identify and certify the scope, authenticity and integrity of electronic information. Metadata is created automatically by a computer, and contains information such as the following: a file name, a file's location, file format, file type, file size and, most importantly, file dates such as the date on which the document was created, the date of last modification, the date on which the document was last accessed, or the date on which the last metadata modification took place. Metadata helps to establish the context of the content. But it does not conclusively prove the integrity of a data message, because it can be altered or removed. (See 'The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age' A Project of The Sedona Conference _ Working Group on Best Practices for Electronic Document Retention & Production (September 2005) at 80–2, available at *http://www.thesedonaconference.org/dltForm?did'TSG9_05.pdf*, and Lee H Rosenthal 'Metadata and Issues Relating to the Form of Production', available at *http://www.yalelawjournal.org/the-yale-law-journal-pocket-part/procedure/metadata-and-issues-relating-to-the-form-of-production/* (visited on 9 October 2010)).

In considering metadata, it is necessary to remember that the person seeking to introduce an electronic document in any legal proceeding has the burden of proving its authenticity in the manner provided. Where a data message's integrity is in dispute, it is also possible to consider the act of removing metadata as an indication of mala fides ('The Sedona Guidelines' op cit at 83). It has been stated that 'in the absence of credible metadata, the admissibility and evidential weight of any electronic document is not capable of proper assessment' (Infology *Comments and Submissions in response to Issue Paper 27 of SALRC*, of 8 July 2010, available at *http://www.infology.net/archive.php* (last visited on 16 May 2011)).

In neither of the above-mentioned cases was credible metadata a factor that was taken into account by the courts in their assessment of an electronic document purporting to be a will or codicil – a fact I find rather worrisome.

6.2.3 Available for Authentication by Means of Signature

Authentication is essentially a process of establishing whether a person or document is who or what it purports to be. Electronic authentication methods vary in their security and effectiveness from user names and passwords, which are easy to use but also not very secure, to the very secure digital certificates and electronic signatures with public key infrastructure (PKI) and biometric identification. Two frequently used processes of authentication include

analysing metadata (as discussed above) and using electronic signatures (Fitzgerald et al op cit at 543).

It has been argued that ECTA electronic signature provisions cannot meet the requirements for signature in terms of the Wills Act because this statute requires multiple signatures and parties need to sign in specific places within the document (ie, the testator must sign every page and witnesses must sign on the last page (Jamneck et al op cit at 66–7)). But I submit that this reasoning falls short of the functional equivalent approach of ECTA and the UNCITRAL Model Law as well as the inherent function of a signature in or on a document, whether it is electronic or paper-based.

The requirement of signature encapsulates that the signatory is aware of the content above the signature, signifies agreement to be bound to that content, awareness that the signature is a sign of intent; and it shows an unalterable permanent record of the event (Fitzpatrick et al op cit at 542).

Under the broadest definitions, electronic signatures are simply an electronic confirmation of authenticity (ibid). This is wide enough to include all forms of electronic identification from the very informal (such as insecure initials at the end of an e-mail) to the very formal and secure forms (such as iris scans and other biometric identification methods).

Under s 1 of ECTA, 'electronic signatures' are defined as data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature, while 'advanced electronic signatures' are electronic signatures that have passed a process of accreditation in terms of ss 37 and 38.

Section 38 of ECTA sets a number of criteria for accreditation. So, for instance, the advanced electronic signature must uniquely link to the user. It must be capable of identifying the user with certainty. It must be created by using a means that falls under the sole control of that user, and it must be linked to the data or data message to which it relates in such a manner that any subsequent change to the data can be detected.

Digital signatures use encryption to guarantee authenticity. The two main methods of encryption are public key cryptography and a one-way hash function. The public key cryptography method uses two different but mathematically related keys known as a key pair. One key is used to encode and the other to decode, and they are therefore used to verify the authenticity of a data message. On the other hand, the one-hash function method uses an algorithm that is not related to any other algorithm, and it guarantees that the simple text has not been altered. Either of these methods can used to create a unique, verifiable mark of authenticity (Fitzpatrick et al op cit at 558–9; cf Van der Merwe op cit at 665–86). For the technical requirements that accredited advanced electronic signatures must meet in South Africa, see chapter III of the final Accreditation Regulations published in the *Government Gazette* No 29995 of 20 June 2007, in particular, reg 13.

At a technological level, therefore, advanced electronic signatures have been designed to ensure the authenticity and integrity of a data message.

Unlike handwritten signatures, once produced they cannot be copied or falsified. They can therefore fulfil the same functions as a handwritten signature, such as authentication, integrity and non-repudiation, and they attach to the electronic document, ie binary code, in its entirety (ie, every single page, word or letter (Fitzpatrick et al op cit at 557, 558, 560 and 570)). Furthermore, multiple electronic signatures can be attached to a single document, with each signatory being given a unique and secure electronic signature which will also record date and time stamps (see *http://www.docusign.com* (visited on 26 October 2010)).

7 Conclusion

The Court's willingness to embrace technology has to be commended and welcomed as progressive and forward thinking. Its decision should be seen as a catalyst to review the exclusion of wills from the ambit of ECTA.

Further arguments raised in respect of potential problems that may arise in the execution of electronic wills, such as the dangers of interference by viruses and hackers, accidental or deliberate deletion and the inability to trace a will (Jamneck et al op cit at 66), are not unique to wills created in the form of data messages. Paper-based wills are equally susceptible to loss or destruction in a myriad of ways for all the same ulterior motives that apply in an electronic world. The distinct advantage, however, of a digital document is that there is a better chance of recovering it than if it was, say, only in paper form and burnt (Allison Stanfield *Computer Forensics, Electronic Discovery and Electronic Evidence* (2009) at 89).

The leap from excluding wills to including them within the ambit of ECTA is made infinitely easier through the courts' ability to recognise the integral role played by computers in people's lives as well as an understanding of the technology available and the appropriate use of the available legislation.