ICT and the profession

The Law Society of South Africa (LSSA) held an information communication technology (ICT) session on 15 August. The aim of the strategic session was to develop a holistic approach to ICT in the legal profession by looking at the interests of the profession.

The conference focused on the impact of ICT on the attorneys' profession going into the future, as well as the actions needed to be taken by the profession in the next five years.

Discussion topics included information security, privacy and confidentiality; social media and the profession; legislation, rules and codes affecting the use of ICT within the attorney's practice; as well as paperless practice and e-signatures.

Speakers included co-chairperson of the LSSA, Max Boqwana; attorney and member of the LSSA's e-law committee, Brendan Hughes; attorney and chairperson of the LSSA's e-law committee, Gavin McLachlan; attorney and information security consultant, Mark Heyink, and attorney and media law consultant, Emma Sadleir.

Mr Boqwana gave the welcome address. He said that the legal profession was changing rapidly and that it was influenced by advances in technology. He added that the use of social media must not compromise security.

Mr Boqwana said that South Africa must start thinking about e-filing and serving documents electronically, as this is where the country should be going. He suggested that maybe the South African justice system should start with a pilot project at the labour courts.

Information security

Speaking on information security Mr Heyink said that attorneys are custodians of constitutional rights. He said that the internet has changed everything, including what we do on a daily basis; it changes how we communicate, how businesses' target markets, as well as the law due to new legislation being developed, such as laws dealing with cybercrime.

Mr Heyink added that the market was changing and questioned whether South Africa's legal profession was ready to change with the times. 'Do we understand our market and are we ready to give them what they need?' he asked.

Mr Heyink stressed that information security was imperative as confidentiality is a professional responsibility. He said that electronic signatures are critical to attorneys as they are a 'stamp' that states that the documents are what they are. Mr Heyink explained that advanced electronic signatures lock the documents. He concluded by saying that privacy was impossible without security.

Overview of legislation

Mr Hughes gave an overview of legislation, rules and codes affecting the use of ICT in legal services. He said that the pervasive reach of technology has an impact on legal practice and institutional functioning.

He noted that judicial recognition of the impact of technology on law and society had already been given by South African courts. For example, he said, in *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD) KwaZulu-Natal High Court Judge Esther Steyn made history when she approved service of court documents via Facebook. In her judgment, Steyn J stated that 'Changes in the technology of communication have increased exponentially and it is therefore not unreasonable to expect the law to recognise such changes'. (See also 2012 (Nov) *DR* 30 and 2012 (Oct) *DR* 47).

Mr Hughes said that lawyers needed to adapt to technology because once customers have experienced a new and better way of doing things, they no longer tolerate any other way.

He quoted the example of the South African Post Office being forced to adapt to its own customers and introduce secure electronic communications services (including the provision of registered e-mail in the near future as provided for in s 19(4) of the Electronic Communications and Transactions Act 25 of 2002 (ECT Act)).

He said that public bodies had institutional power to introduce change as stated in ss 27 and 28 of the ECT Act which provides as follows –

*'*27. Acceptance of electronic filing and issuing of documents – Any public body that, pursuant to any law
(*a*) accepts the filing of documents, or requires that documents be created or retained;
(*b*) issues any permit, licence or approval; or
(*c*) provides for a manner of payment, may, notwithstanding anything to the contrary in such law –
(i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages;
(ii) issue such permit, licence or approval in the form of a data message; or
(iii) make or receive payment in electronic form or by electronic means.
28. Requirements may be specified – (1) In any case where a public body performs any of the functions referred to in section 27, such body may specify by notice in the *Gazette* –
(*a*) the manner and format in which the data messages must be filed, created, retained or issued;
(*b*) in cases where the data message has to be signed, the type of electronic signature required;
(*c*) the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message;

(*d*) the identity of or criteria that must be met by any authentication service provider used by the person filing the data message or that such authentication service provider must be a preferred authentication service provider;
(*e*) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and
(*f*) any other requirements for data messages or payments.'

Mr Hughes gave an overview of the court's responses to technological changes. He said that following amendments to the rules promulgated in 2012, r 19(3)(*c*) now provides that the defendant may request the consent of the plaintiff to consent to the exchange or service of documents and notices by e-mail. 'Rule 19(3)(*d*) now also provides that if the plaintiff fails to provide its consent, the court may, on written application by the defendant, grant such consent and on such terms as to costs as may be just and appropriate in the circumstances. Rule 4A(3) of the High Court Rules expressly provides that Chapter 3 Part 2 of the ECT Act is applicable to service by e-mail. However r 4A(5) also says that the filing of originals with the registrar may not be done by e-mail,' he said.

Mr Hughes said that the Magistrate's Court Rules essentially mirror the provisions of the High Court Rules. He added that the only court rules that expressly permit the filing of documents electronically are the rules of the Supreme Court of Appeal, where r 4(1)(*b*) provides that documents may be submitted to the registrar electronically provided the 'original' document is filed within ten days. This means that even in this case, e-filing simply interrupts running of time periods and does not constitute formal delivery of a document, he said.

According to Mr Hughes, there is a need for the legal profession to adapt to technology. He said that the value of litigation compared to the net possible result against the time, risks and monetary costs involved were not on par.

Mr Hughes looked at the risks of not adapting. He said: 'Currently under South African law, the admissibility and/or evidential weight of any document that was generated, sent, received or stored by electronic means that is produced at court in paper format may be challenged on the basis that –
• the "original" was not produced in terms of s 14 of the ECT Act;
• the "best evidence" was not produced in terms of s 15(1)(*b*) of the ECT Act; and
• the "integrity" of the information was not capable of passing assessment in terms of s 15(3) of the ECT Act.'

He added that this significant risk arises for virtually every party to litigation because –
• s 15(2) of the ECT Act provides that the rules of evidence must not be applied so as to deny the admissibility of a data message 'if it is the best evidence that the person producing it could reasonably be expected to obtain';

• s 15(3) of the ECT Act expressly provides that the evidential weight of a data message must be assessed by having regard to, *inter alia*, the reliability of the manner in which the document was generated, stored or communicated and the reliability of the manner in which the integrity of the document was maintained; and
• s 14(2) of the ECT Act provides further that the integrity of a data message must be assessed by considering, *inter alia*, whether the information presented has remained complete and unaltered since it was created.

'Quite simply, neither of these assessments can be conducted against paper print outs of electronic documents such as e-mails,' he said.

Mr Hughes indicated that the admissibility and evidential weight of data messages (including ordinary e-mails, attached electronic files and electronically stored records) depends on an integrity assessment, which can be properly assessed only from an electronic copy of the document containing file metadata, such as, information contained in the electronic copy that typically evidences when, and by whom, an electronic document was originally created, whether it was revised or edited, to whom it may have been sent and when it was received.

'Internationally, discovery rules have been amended to address these issues by catering for the proper discovery and production of electronic documents before trial,' he said.

Mr Hughes recommended that r 35(1)(*a*)(*b*) of the the uniform rules of court dealing with the discovery, inspection and production of documents, should read:
'(*a*) such documents and tape recordings in his possession or that of his agent other than the documents and tape recordings mentioned in paragraph (*b*) and the electronic format, if any, in which any such documents and tape recordings exist.'

And 35(6) should read:
'(6) Any party may at any time by notice as near as may be in accordance with Form 13 of the First Schedule require any party who has made discovery to make available for inspection any documents or tape recordings disclosed in terms of subrules (2) and (3) and the electronic format, if any, in which such documents or tape recordings are to be made available. Such notice shall… .'

Cloud computing

According to Mr Hughes cloud computing offers flexible, affordable technology that directly addresses a business's objectives and goals by providing required functionality, reduced expenditure and increased mobility and convenience.

He added that the general consensus internationally was that the use of cloud computing architectures in legal practice do not violate any ethical duty (and in many instances may go some way towards upholding them) provided that reasonable care is taken effectively to minimise any risks to the confidentiality and security of client information and client files. In other words, he said, lawyers must take reasonable steps or reasonable protective measures to minimise any risks to the confidentiality and security of client information. He added that lawyers should exercise due diligence before utilising a third-party service provider for purposes of storing or processing confidential information offsite.

Duties of attorneys

According to Mr Hughes, the general ethical duties of an attorney relating to the use of ICT and cloud computing include to –

• understand and guard against the risks inherent in the cloud by remaining aware of how and where data is stored and what the service agreement says, namely, the duty of competence;
• keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology;
• have a reasonable understanding of technology and using it, or seek assistance from others who have the necessary proficiency;
• keep abreast of, and understand, any advances in technology that genuinely relate to competent performance of the lawyer's duties to a client;
• ensure that service providers and the technology they use support the lawyer's professional obligations;
• conclude an agreement with the provider/operator of the services, where the information to be processed is personal information, to ensure that appropriate security for the protection of personal information is established and maintained; and
• implement and provide appropriate information security for the information and communications processed by the attorney.

E-signatures

Speaking on a paperless practice and e-signatures, Mr McLachlan said that paper-based signatures or traditional signatures are readily understood in commerce and law. He added that paper is an effective means of transmitting information and that this methodology will remain in use for the foreseeable future.

'That being said, in today's tightly regulated legal and financial services market, paper-based document retrieval, management and storage is time consuming and costly. Another obvious negative is the ease with which a paper signature can be forged and it can, at times, be difficult to conclusively prove a signature in a legal process,' he said.

Mr McLachlan said that there are two types of electronic signatures in South African law – the electronic signature and the advanced electronic signature.

• *Electronic signature:* This is electronic data that the sender intends to serve as a signature. As with the traditional method of signature, this can be done in any number of ways – typing your name at the end of an e-mail, for example, will serve as an electronic signature.
• *Advanced electronic signature:* This is an electronic signature, the provider of which has been accredited by the accreditation authority in terms of the provisions of the ECT Act. In its accreditation the provider must meet globally accepted security in security encryption and authentication standards and is subject to an annual audit to ensure that these standards are maintained.

Mr McLachlan said that there were only two accredited providers of advanced electronic signatures at the time of the strategic session – the South African Post Office and Lawtrust (Pty) Limited.

Social media

Ms Sadleir spoke on social media and risks for the profession. She highlighted recent case law involving employees being fired or getting into trouble with their employers for their posts on social media platforms such as Facebook.

Ms Sadleir urged judges to sign up on social media websites. 'How can judges decide on matters dealing with Facebook, for example, if they are not aware of what goes on on Facebook or how to use it?' she asked.

Ms Sadleir noted that there are no guidelines on tweeting in court, except in *S v Kotze and Others* (GNP) (unreported case (C119/12, 15-7-2013) (Bam AJ) – the *Modimolle* case – where tweeting was banned. She noted that these days all you need to know is which journalists are in court covering a certain case, and the hashtag they are using, to be able to follow court proceedings as if you were in court yourself.

Ms Sadleir warned delegates to avoid tweeting when angry, drunk or emotional. 'Once you tweet, that is it; it is out there. Even if you delete it, people usually retweet so quickly, someone is bound to read your tweet,' she said, adding that the disclaimer which reads 'I tweet in my personal capacity' is not a magic wand that gets one out of trouble for 'wrong' tweets.

Ms Sadleir highlighted the fact that as long as your profile indicates where you work, you cannot distance yourself from your employer in your tweets.

She concluded by making a few recommendations for the legal profession:
• Guidelines on social media for legal practitioners. *
• A social media policy.*
• A policy or rules on social media as evidence.
• Guidelines on tweeting from court.
• Social media training for judges.

*The LSSA's guideline and draft social media policy for law firms can be accessed on the LSSA website at www.LSSA.org.za under 'Resources for attorneys'.

• See also 2013 (April) *DR* 7; 2013 (Jan/Feb) *DR* 17 and see page 28 of this issue.

Nomfundo Manyathi-Jele,
nomfundo@derebus.org.za