A paper presented in the 16th International Conference on Sustainable Development at the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) Bangkok, Thailand, 2022.

Forensic inquiries: Evidencing the reliability and admissibility of digital communication

Werner Uys[1] **, Kobus Joubert**[2]
[1] Department of Taxation, University of South Africa, South Africa,
[2] Department of Auditing, University of South Africa, South Africa,
[2] Corresponding author: joubek@unisa.ac.za

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at http://www.ssrn.com/link/OIDA-Intl-Journal-Sustainable-Dev.html

Abstract: This article discusses several requirements for the admissibility and relevance of digital evidence, for the unacquainted forensic investigator, including social media statements, in criminal and civil investigations. Any criminal or civil investigation must not misapply the rules of evidence to deny the admissibility of data messages as digital evidence or electronic communication. According to the Electronic Communications and Transactions (South African) Act, 25 of 2002 (hereinafter "the ECTA"), the relevant and admissible requirements for digital evidence must reflect this purpose. The Cybercrimes (South African) Act, 19 of 2020 (hereinafter "the Cybercrimes Act") was promulgated with the intention of outlawing the disclosure of information that is detrimental to the cyber environment. A unique law in South Africa, the Protection of Personal Information (South African) Act 4 of 2013 (hereinafter, the "POPI Act"), defines "electronic communication" as "any text, voice, sound, or image message sent over an electronic communications network". A common-sense approach is often needed for the workings of the machinery of the law and the use of technology. To secure admissible digital evidence, forensic investigators need to understand that different industries require different approaches. The banking industry, for instance, is governed by bank laws, while intentional tax evasion and tax fraud are governed by tax laws.

Forensic investigators need to be familiar with both the requirements and pitfalls of the legislation above. Particular attention should be paid to how original records or copies of originals must be submitted as digital evidence in court. Furthermore, this study summarizes techniques available to forensic analysts in determining the admissibility and relevance of electronic evidence in the form of emails and text data messages such as Short Message Service (SMS) and WhatsApp. To analyse court rulings on the admissibility of evidence in digital form, which is documented in court cases, a literature review has been conducted, making use of the LexisNexis Electronic database as well as the Southern African Legal Information Institute (hereinafter the SAFLII database), and analysing South African case law as well as research literature available online. In court proceedings, digital evidence is seldom inspected for authenticity. The study shows that the ECTA and the Cybercrimes Act allow for access to data stored in the cloud or even when data breaches are detected. Forensic investigators rarely possess the knowledge or skills required to investigate digital evidence that would be most likely to be admissible as well as having probative value in a trial court. Generally, at the outset of an investigation, forensic investigators or forensic analysts should use the techniques available for generating digital evidence, which is deemed relevant in terms of South African legislation and the common law. This article refers to forensic analysts which include forensic investigators or forensic accountants and refers to electronic or digital evidence used interchangeably for easy identification of relevant concepts. The question is answered whether emails, SMS and social media messages (including WhatsApp) such as tweets will stand up to scrutiny in legal proceedings as admissible electronic evidence.

Keywords: Admissibility, Cybercrimes, Electronic Evidence, Forensic Analyst.

Introduction

One of the famous quotes by United States Supreme Court Justice Potter Stewart, "I know it when I see it" in *Jacobellis v Ohio* [1], is a proverbial description of the inescapable requirement for any communication or form of information presented as electronic evidence before a court or tribunal by a forensic analyst, is to pass the test of what is deemed "admissible" evidence. In the proverbial "eyes of the law," and as stipulated in section 15(1) of the Electronic Communications and Transactions (South African) Act, 25 of 2002 (hereinafter "the ECTA") [2], data messages can be presented in criminal or civil proceedings as evidence and cannot be denied on the basis that it is a *data* message or that it is not in its original form (that is, to confirm its truthfulness). Section 15(2) of the ECTA contains the *data message* definition – that is – *information* electronically created, sent, received, or stored, including voice messages.

For any *information* or form thereof, to be formally recognised and admitted as electronic evidence in court, the forensic analyst should lawfully collect such information from the original source and present it in the required form or format acceptable, or admissible, to the judiciary. For the successful prosecution of a white-collar crime offender, for example, a cyber-fraudster, the forensic analyst should focus on collecting relevant evidence, such as e-mails or data messages, data breaches, breaches of privacy, or identifying and reporting on cyberattack activities. These pieces of digital evidence should only be related to the crime at hand and ought to prove beyond a reasonable doubt in criminal cases, the guilt of the alleged offender. This can be difficult as the work of the forensic analyst is both abstract and conceptual in nature. It, therefore, requires the forensic analyst to coordinate abstract concepts in a meaningful way during the forensic investigation and proving them with hard evidence. For this article, these activities will not be discussed including the admissibility of video material submitted in evidence.

Apart from the main criminal proceedings legislation, namely, the Criminal Procedure (South Africa) Act, 51 of 1977 (hereinafter the CPA") [3] and the ECTA [2], other legislation has been promulgated in South Africa affecting access to digital information. The Cybercrimes (South African) Act, 19 of 2020 (hereinafter "the Cybercrimes Act") [4] provides for the investigation of suspected cybercrimes and the admission of digital evidence regarding the commission of cybercrimes by granting investigators access to digital information stored on a network or a database. This is necessary as a forensic investigator must be able to access a network or database (the information is stored in the cloud) to obtain digital evidence, for use in a trial court through the assistance of a designated Point of Contact (section 52 of the Cybercrimes Act). Section 3 of the Protection of Personal Information (South African) Act 4 of 2013 (hereinafter, the "POPI Act") [5] governs offences associated with personal information such as the misuse thereof to commit cybercrime (Williams, Fourie and Siyaya 2021) [6]. Both the Cybercrimes Act and the POPI Act allow for electronic evidence to be effectively collected for use in court. Clough (2014:734) [7] argues that countries affiliated with the Council of Europe Convention on Cybercrime/Budapest Convention [8] must have harmonised national laws to prevent cybercrime on a global scale. As a signatory to the Budapest Convention (Council of Europe 2020) [8], South Africa endorsed the Protocols of the Budapest Convention. Considering the extent of global digital communication, Swales (2018:2) [9] believes that digital evidence will play a growing role in future court proceedings.

Digital evidence

Digital evidence includes data messages and electronic records and is allowed as evidence in criminal law proceedings. Defining "electronic evidence" is not easy as terms such as "digital evidence" or "computer evidence" are also used but also relate to mobile forensics (evidence obtained from cell phones). This is evident in the fact that the ECTA was promulgated to assist in clearing up the legal uncertainty of these terms and overcome legal obstacles attributed to the evidential weight of this type of evidence (such as scanned reproductions of digital evidence). For this article, the terms "electronic evidence" or "digital evidence" will be used to refer to information having probative value, which is stored or transmitted in binary form that may be relied on in a trial court (*S v Brown* in para [16]) [10]. This definition implies that the digital evidence must be relevant and admissible, and legally recognisable as data messages (section 11 of the ECTA). It must be continuously considered by the forensic analyst that documents in electronic format have characteristics that affect the test for authenticity as well as the chain of custody requirements to be met to ensure admissibility in court. As cybercrimes occur swiftly, a critical element of the forensic analyst's work is to respond swiftly to the crime and to use appropriate techniques to verify fraudulent activities, i.e., immediate verification of banking details in the case of bank crimes. There are techniques that are used to analyse electronic evidence to ensure its admissibility as evidence in court. Four techniques are considered (McKemmish 2008) [11]:

- The meaning of the electronic evidence should not be altered;

- Any errors in the admissibility of the electronic communication must be identified and explained to the satisfaction of the court;
- Analysis processes should be available for independent verification for delivering comparable results; and
- The forensic analyst performing the analysis should have relevant and comprehensive experience.

The role of the forensic analyst in this regard is to gather, analyse and present electronic evidence that is relevant to the case, and which is admissible as evidence in a court, without compromising its integrity or credibility of the required standard for the admission of evidence (Ngomane 2010) [12]. The term used to describe the said actions is computer forensics and is the practice of collecting, analysing and reporting evidence in a way that is legally admissible in "open court" or "public" as part of the criminal investigation process (Haidarevic and Dzaltur 2015) [13]. Criminal proceedings are dealt with in terms of the CPA and acquaintance with those rules is essential for the forensic analyst. According to a survey by AlixPartners (2022) [14], the greatest threat faced by legal and compliance officers in organisations in the United States, Europe and Asia, is data breaches or cyberattacks.

For the unacquainted forensic analyst, the collection of legally relevant evidence can be a difficult exercise. According to Klein AJ in *Fourie v Van der Spuy and De Jongh Inc. And Others* in para [25] [15], "the rate at which cybercrime occurs makes the internet a very unsafe working area". Any method to assist the unacquainted forensic analyst in building a *prima facie* case, therefore, becomes invaluable. The forensic analyst, when analysing information or evidence implicating a person in a crime or workplace misconduct, cannot look at pieces of evidence in isolation but must examine all the other evidence linked or available to him, even if such evidence may expulse the alleged offender from the charges. To mitigate cybercrime risks, the forensic investigator can, for instance, inquire about verification methods for electronic fund transfers (EFTs), such as email or telephone verification of bank accounts.

A judge admitting digital evidence could make the mistake of automatically assuming that digital evidence is reliable. A well-prepared case can be spoiled by the littlest of overseen detail. For instance, according to Mitchell (2022) [16], a British Virgin Islands court (unpublished) approved the freezing of crypto wallets when a company applied for urgent relief against hackers that stole crypto tokens kept in cryptocurrency wallets (this is called digital property). The company provided "cross-chain bridging" to cryptocurrency companies (it is a computer process that synthetically transfers cryptocurrency tokens between different blockchains) and it was hacked on at least one occasion. The court allowed interim relief only based solely on the perpetrators being identified through the theft of the crypto wallets. Jack J requested the identified respondents to come to court to prove otherwise, but on the due court date, they neglected to appear before the court, with the court eventually granting relief to the applicants. This matter highlights the fact that even though the crypto property was never stolen directly from the applicants, the court granted relief because of the tarnished reputation of the applicants caused by the theft of the cryptocurrency. This article sets out criteria for the forensic analyst to consider when gathering, analysing, and presenting electronic evidence in court.

Research Methodology

The research methodology entailed a literature review and incorporated a systematic literature review as described by Kirkevold (1997) [17]. The review method consisted of a content analysis of legislation, common law principles, court decisions and sources related to the subject under discussion. The relevant provisions of the CPA, Law of Evidence Amendment (South Africa) Act, 45 of 1988 [18], the ECTA, the Constitution of South Africa, 1996 [19] and the common law together with court decisions, which relate directly to the objective of this article, were analysed in relation to requirements imposed on the diverse types of evidence by the judiciary. The court cases were selected from different databases, namely the Lexis Nexis Electronic Library, as well as the Southern African Legal Information Institute (hereinafter "SAFLII") [20]. This form of systematic analysis was deemed the most suitable method to congregate the various aspects covered by the research into a comprehensive whole. It is necessary to take note that the 2022 proposals to amend the ECTA are not discussed, including voice and short messaging service (hereinafter "SMS"), fraudulent Subscriber Identity Module (hereinafter "SIM") swap and number porting, state of disaster protocols, data services, educating end-users about cybersecurity and protection of personal information, and 3G and 4G service quality.

Literature review

According to Ernst and Young (2022) [21], an organisation's cybersecurity depends on controls that are based on people, processes, and technology. If these controls are implemented, organisations are better prepared against organised cyber-attacks, accidental information breaches, or human error in the use of electronic resources. These

types of controls ensure that previous electronic communication is easily accessible by the forensic analyst for use as digital evidence. Once digital or electronic communication has been formally admitted in court, it can be described as "evidence" (Bellengere *et al*. 2013) [22]. Evidence can be defined, from a legal perspective, as real, documentary, or verbal evidence presented to a court to assist in proving the truth (ACFE 2016) [23]. This type of evidence may include electronic communication such as a "data message". As defined by the Cybercrimes and Cybersecurity Bill [24], the forerunner of the Cybercrimes Act, a data message is any information that has been generated, sent, received, or stored by electronic means, and whose output is comprehensible.

This definition was adopted into legislation with the enactment of the Cybercrimes Act in 2020. This type of "evidence" may either refute or support the truthfulness of any fact in issue for determination before the court, especially as the Cybercrimes Act criminalises certain electronic activities such as the hacking of email accounts, where electronic tracks exist in cyberspace. However, documentary evidence of crimes against information networks or computer systems is on the rise and evidence may be difficult to obtain. Therefore, in line with the new Cybercrimes Act, new methods, techniques, tools, processes, and protocols are required for extracting evidence of computer crimes. For example, to help strengthen cybersecurity and cybercrime investigations in Argentina, a High-Tech Cybercrime Investigation Centre was created to detect cybercrime and criminal activities against computers, information systems and computer networks (Peruzzotti & Sorrentino 2022) [25]. Similarly, South Africa introduced a "Point of Contact" initiative through legislation (adopted in 2020) to assist South African companies with cybercrimes (section 52 of the Cybercrimes Act), but this procedure is not yet operational and is mentioned as an incidental note for further research purposes.

Digital evidence in the form of data messages means data that are generated, sent, received and stored by electronic means and includes voice (Watney 2009) [26]. Electronic records are information created and stored in an electronic medium and the South African Courts have introduced a new CaseLines system whereby pleadings by parties are submitted electronically (Mabeka 2021) [27]. The term "electronic evidence" includes many forms of evidence, but this article concentrates on electronic mail (email), SMS and online social media as sources of evidence as an introduction to "digital evidence". A note on cryptocurrency assets: where an applicant approaches a court with any form of digital evidence obtained from a cryptocurrency investment platform – say for instance in the case of theft of cryptocurrency – the evidence submitted before the court must leave the judge with little difficulty in deciding to accept it as digital evidence in trial proceedings before the court. Fortunately, this process is supported in terms of the Cybercrimes Act and unacquainted forensic investigators should take note of the legislation enacted in the Act.

Emails

There is a high rate of incorrect collection of digital evidence, as Nortje and Myburgh (2019) [28] suggest. This is true for documentary evidence as it could include correspondence that often takes place by electronic mail (email) and therefore, should qualify as admissible documentary evidence before being admitted in court. Emails are messages that are composed electronically by special-purpose software (Mason & Seng 2016) [29]. Special-purpose software is designed to enable a user to perform specific tasks (Mason & Seng 2016) [29]. Emails are an important source of electronic evidence due to the nature of the information contained therein. Emails are used to, inter alia, negotiate business transactions, and exchange information about transactions, dealings or the parties involved and implicated in a transaction. The problem that arises when emails must be presented as evidence is for the forensic analyst to prove that the emails were sent (authentication) by the parties under investigation. Authentication, however, needs to be established to ensure the sender is the one whose name appears on the email because a sender's identity can easily be concealed. The admissibility of emails as evidence is often wrongly assumed impossible because emails can easily be forged. Such a view loses sight of the reality that almost all forms of evidence, including paper-based evidence, can also be forged. The challenge remains to test the authenticity of any type of evidence, including electronic evidence (Mason & Seng 2016) [29].

Authentication of email as evidence

To be able to establish authentication of the parties involved in the communication by email, the forensic analyst needs an understanding of various protocols used for the transmission of emails. Each of the protocols has unique features that affect their authentication. The most popular email protocols will be discussed with specific reference to the authentication issues facing forensic analysts that may affect the admissibility of the emails into evidence. The first protocol under discussion is the Post Office Protocol (hereinafter "POP"), a computer-networking tool. This protocol, when used for receiving emails, downloads the emails to the user's computer and deletes them from the server while leaving a copy intact on a backup server. The forensic analyst's only avenue to establish authentication is to gain access to the backup server to obtain evidence of the sender and receiver. The information available on

such a server will contain the username and password used to access the emails on the server, which is important for the authentication required by the forensic analyst (Chhabra & Bajwa 2015) [30].

The second protocol to be discussed is the Internet Message Access Protocol (hereinafter "IMAP"). This protocol works differently from the POP protocol by leaving the emails on the server. When emails are sent using this protocol, it attaches a header containing the current time and date, like a post office "stamp", to the email. Another element of importance included in the header is the internet protocol (hereinafter "IP") address of the computer sending the email (Gupta, Gupta & Singla 2016) [31]. Servers also keep logs by whom and when emails were opened. This leaves a trail for the forensic analyst to follow even if all emails have been deleted from the user's computer. Knowledgeable users can remove the information contained in the header attached to the email, but the forensic analyst may still be able to extract other metadata associated with the email (Mason & Seng 2016) [29].

Chain of custody for emails

The chain of custody principle means that the forensic analyst must be able to prove that the electronic evidence that is presented before the court, has not been changed in any way after the alleged offender's last access thereto. Various forensic software solutions exist to take care of custody (Giova 2011) [32]. The procedure to seize the evidence is to secure, in the presence of the alleged offender and a police official or officer of the court, an image of the medium on which the evidence is stored. Such an image contains a hash total that will change if any content forming part of the image is altered. The image also contains important metadata (data about data) that provide additional authentication information of use to the forensic analyst. By proving in court that the hash total of the evidence presented before the court is equal to the hash total at the time of the seizure, the forensic analyst can prove that the chain of custody requirement was met.

Judgements previously adduced by the judiciary are important indicators and predictors of how the Courts view the chain of custody. For illustration purposes, although the way a warrant was obtained to access emails on an alleged offender's computer was irregular at law, a court will nevertheless sanction the mirroring of the hard drive, if it will allow for direct access to evidence such as emails (*Page and Others v Additional Magistrate, Somerset West and Others*) [33]. A respondent was not allowed to deny receiving an email during court proceedings since the respondent ought to have knowledge of the content of such an email even if it was sent to his colleague (*General Council of the Bar of South Africa v Jiba and Others*) [34]. Thus, the chain of custody can extend to a series of emails and investigating the history of an email is vital for the forensic analyst.

SMS

SMS messaging is a popular media of communication, which include social response platforms such as "WhatsApp". These platforms, like SMS messaging, could also be used for illegal purposes. Additionally, since they are part of day-to-day life, forensic analysts solving legal disputes can use SMSs as evidence. Since a cellular phone might be accessible to people close to the owner, it is important to establish the fact that the sender of the message is indeed the owner of the phone (Chang *et al*) [35]. The vast application abilities of smartphones offer additional information to forensic analysts, for example, their global positioning system (hereinafter "GPS") abilities. The GPS position of the phone is included in the metadata that can be extracted from the phone and can be used to determine if the phone was in the same location as testified to by the accused (Peters *et al*) [36].

However, although the procedural aspect of admissibility of the SMS could be successfully fulfilled, the unreasonable and self-serving construction of the contents or text message by a party to a dispute itself will only draw the ire of the court – as in this case – the Supreme Court of Appeal (*T v T* in para 22) [37], with the appeal dismissed with costs because of the conduct of the appellant. An appellant that does not act *bona fide* but abuses the court's process because of his or her superior economic position, may be punished with a punitive cost order (*T v T* in para 23).

Authentication of SMSs as evidence

To establish if it was indeed the accused that sent an SMS, which the forensic analyst will present as evidence in a court, is more complex than the authentication techniques applied to emails. The main difference is that the contents of SMS messages are not stored on a server by the cellular service provider that enables subsequent access and analysis. The techniques that are available to the forensic analyst are first, stylometry, secondly, the N-Gram method and thirdly, the probabilistic evaluation technique. These methods will be explained in the following two paragraphs.

The first technique, namely stylometry is a technique whereby SMS are analysed to determine a pattern of language and vocabulary used by the sender to establish authorship. The SMSs that are presented as evidence in court are then compared with the established pattern derived from other SMSs created by the accused. Studies have been successfully undertaken to prove authorship using stylometry (Mitchell 2013) [38]. The stylometric method is accepted as evidence in various jurisdictions such as the UK, the US and Australia (Ragel, Herath & Senanayake 2013) [39].

The second technique under discussion is the N-Gram method (Altamimi, Clarke, Furnell, & Li 2019) [40] which is also used to detect the authorship of an SMS with usable accuracy by measuring the similarity between a block of characters and the profile of the author, was proven more reliable than the stylometry method (Ragel, Herath & Senanayake 2013) [39]. Although this method might be adequate for text classification tasks such as SMS, it, however, falls short in analysing highly diverse data such as documents (Tuarob *et al*. 2014) [41].

The third technique for determining the authorship of SMSs is probabilistic evaluation. This technique relies on features such as the richness of the sender's vocabulary, the digit ratio and the average character number. A study by Ishihara (2013) [42] found that this method outperformed the N-gram method.

Chain of custody for SMSs

The purpose of preserving smartphone data is for the forensic analyst to ensure its admissibility as evidence in court. According to Dlamini, Olivier and Grobler [43], to preserve the evidence, that is, in addition to using forensic software to produce an image of the smartphone, various methods can be applied, such as:

- Upload the data to a cloud storage facility; and
- Copying smartphone data to a compact disc (hereinafter "CD") or secure digital (hereinafter "SD") card.

The benefit of these methods is that chain of custody remains in the hand of the forensic analyst and such a person can testify about the process and the validation of the electronic information transfer from the original form or source to its storage in the cloud or use of computer technology to transfer information (CDs as a digital storage device).

Social media tweets

Hanekom v Zuma [44] is a stern warning for those individuals making use of tweets on Twitter and other social media platforms such as WhatsApp, Facebook and Instagram not to impair the dignity of others and to safeguard against *crimen injuria* (harming someone's dignity). In this matter, the applicant, Mr Hanekom – a previous South African Minister of government and politician – had sued Mr Zuma for alleging him to be an apartheid spy. Mr Zuma's allegation (his electronic message) was posted on his Twitter account, a social platform with 517 million users worldwide. By default, tweets are publicly visible (*Netshipise v Munnick and Others*) [45] and because they are published online, can cause immense harm if it remains there without censure. As a result, the message by Mr Zuma caused harm to Mr Hanekom since he received insulting messages from other online users referring to him as an "…[a]skari and an impimpi" in para [2], a derogatory remark implying Mr Hanekom to be an apartheid spy.

As the court noted in para [11], the sender of a social message, in this case, Mr Zuma, "…[r]eserves the right to justify his tweet as being true, fair comment or falling within the limits of the right to freedom of expression in section 16 of the Constitution". Thus, the words expressed must be analysed and it must also be in the public's interest that the words are published, as was held in *Heroldt v Wills* in para [27] [46]. Rumpff JA distinguished in *Publication Controls Board v William Heineman Ltd and* Others [47] that what is in the public's interest will however depend on the convictions of the community (*boni mores*). The court stated in para [80] in *Hanekom v Zuma* that the matter is determined by objective evidence by defining the false narrative by testing the facts stated by the defendant. Legally, the defendant has the burden of rebuttal if the defamatory statement is not in dispute, in other words, to prove the facts that dispel its wrongfulness (*Du Toit v Coetzee* in para [16]) [48].

The test for the forensic analyst to determine whether a statement falls foul and should be pursued for its "subjective" defamatory inclination, however, remains an objective one. *Hanekom v Zuma* in para 8 determined an objective approach to be followed by the court. Firstly, one must ask and should answer what is the natural or ordinary meaning of the statement. Secondly, to determine *prima facie* the wrongfulness of a statement made on social media, the forensic analyst must establish:

- the alleged defamatory context of the message which must amount to a general comment and not be a fact;
- the comment must be unfair;

- the statement must be untrue, and
- the facts must not be in the public's interest (according to the moral convictions of the community). It is suggested that the forensic analyst pursue a legal opinion before using the statement as evidence.

The court in *Hanekom v Zuma* held that the four key requirements for a crime of defamation to be established, are wrongfulness, intention, publication, and the defamatory statement by the accused or conduct about the claimant in para [6]. According to section 242 of the CPA, the publication of the defamatory matter or a statement shall be admissible in evidence without further proof of the publication of their publication. Thus, any defamatory statements are considered evidence when they can be linked *(nexus*) to a specific person. In the case of an employee, the defamatory statement should be considered in conjunction with the employer's in-house legal counsel and the employer's labour policies before any formal disciplinary proceeding is initiated or should rather be treated as a criminal act. Whistle-blower evidence provided to an employer or company that was sent by WhatsApp should be treated with care and the necessary privacy as there could be potential victimization of the claimant. Information obtained in this regard should be tested for authenticity as untrue information would affect the person's integrity about whom the complaint is lodged.

A brief note about cybercrimes

Cybercrime can take many forms, from hacking to stalking. There is no universal definition of the term, but it involves committing an act via a computer network or the internet (Media Defence 2020:2) [49]. In *Msomi v* S [50] the court stated in para [34] that cybercrime seems somewhat less ethically reprehensible than fraud or theft, but that these crimes nevertheless have far-reaching effects on a country's economy, the global economy, and the public at large. To justify this proposition, different types of cybercrimes are criminalized under the Cybercrimes Act. The Cybercrimes Act is not specifically discussed in this article as the interposition between the various aspects of the legislation requires a substantial discussion of its own. However, forensic analysts dealing with computer fraud should be aware of the provisions stipulated in the Cybercrimes Act.

Results

Emails

Its admissibility and evidential weight as data messages are analogous as evidence for both email and SMS. In *Jafta v Ezemvelo KZN* Wildlife [51] the court had to decide if the email and SMS sent by the plaintiff were admissible as evidence in establishing a valid contract of employment. The court found that an SMS is as effective a method of communication as an email or a written document. In view of those findings, the court concluded that a valid contract of employment had come into existence, and therefore the weight of evidence apportioned to an SMS is sufficient. Emails were accepted as evidence in *Du Plessis v Independent Regulatory Board for Auditors and* Others [52]. The authenticity or chain of custody in this matter was not questioned and the emails were presented as evidence since none of the parties objected to its admissibility. Should the respondent have subjected the evidence to further scrutiny, additional expert testimony would have had to be relied upon. Emails exchanged between the parties were accepted as evidence and their authenticity was not questioned (*Konsult One CC v Strategy Partners (Pty) Ltd*) [53].

The authenticity of the emails between the parties to the dispute was not questioned in court, suggesting that this form of (data) communication does not necessarily diminish its evidentiary weight. If the email had bounced back from the respondent's server, the email would not have been received nor would constitute evidence. In terms of the ECTA, an email delivered on the server of the recipient would constitute a delivered document, even if not opened by the recipient. The law is however unclear on the malfunction of communication systems where the email is neither delivered by some fault in the system nor is bounced back to the sender. In *Jafta v Ezemvelo KZN Wildlife* the court found an email that was sent but due to technical problems was not received on the server of the defendant, inadmissible evidence.

An alleged offender may raise an argument that he or she was not aware of the misuse of emails in respect of their employer's policy. This was the case in *Woolworths v Commissioner Matlala NO and Others* [54]. Although it was stated that an abuse of the employer's email system could result in dismissal, the employer failed in treating its employees equally for the same offence. For the forensic analyst, it is important to carefully study and interpret the employer's email policy. In formulating the charges, the forensic analyst must take note of the policy rules in respect of any electronic communication transgression and the way evidence is presented.

In *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash* [55] the Supreme Court of Appeal had to deal with several emails sent in series, which purported the cancellation of a franchise agreement. The Court applied the following measures in terms of the ECTA to allow emails as evidence:

- that the emails are in writing (section 12);
- insofar the emails are signed by the author (section 13);
- that the emails satisfy the requirements of writing (section 12); and
- that the requirement of the signature is satisfied by the writing of a name at the end of the email (section 13(1).

In terms of section 15(1) of the ECTA, which deals with the admissibility of data messages, the mere fact that evidence is in the form of a data message, will not exclude it as evidence. If not in its original form, it must be proved by a person adducing it that it is the best alternative reasonably expected to be found. This section however does not specifically exclude provisions of the Law of Evidence Amendment Act [18] or the common law principles applicable to prove a case, and it is suggested that it may still be challenged based on documentary authenticity.

Where both parties enter emails into the bundle of documents, the court ordinarily accepts it as evidence (*Jepson NO v Lezar*) [56]. This follows the legal position established by section 22(1) of the ECTA, which provides that "[A]n agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages". Courts do not ordinarily challenge the validity of emails if both parties do not raise questions of authenticity (*Myburgh v Equestrian Valley (Pty)* Ltd [57]; *Mnyandu v Padayachi* [58]; *Ramaridili v MTN SA Innovation* Centre [59]; *Samtoy CC v Haffenden Groves (Pty) Ltd* [60]; *Charioteer Trading CC v Fontis Holdings (Pty) Ltd* [61]).

SMS

The question before the court in *Democratic Alliance v African National Congress* [62] was concerned with the truth of the SMS under discussion. The court was not asked to rule on the authenticity of the SMS, but on whether the message conveyed by the SMS was true or false. Unless the author makes it clear that the SMS is an expression of opinion or comment, its contents can't be protected by a plea of fair comment. For the forensic analyst, it is clear to establish at the outset whether the text contents of the SMS are true before submitting it as evidence.

As an additional consideration, the court must decide on the weight (relevance) of evidence in the form of data messages such as SMSs (section 15(3) of the ECTA). The factors considered by the court are:

- reliability of generated, stored or communicated messages;
- reliability of message maintained;
- manner how originator was identified, and
- other relevant factors.

These factors are eminent in court proceedings itself. Although the court did not utilise any of the metadata on the cell phone to prove the whereabouts of the accused, cell phone records obtained from a service provider were considered admissible evidence of the whereabouts in question (*S v Shange and Others*) [63]. For the forensic analyst, these factors are not the only considerations. The final test is that electronic information (data messages), when presented as evidence in court, in its present form, is sufficient proof of the issue for determination and is also rebuttable proof of the facts contained in such record. It must be probative, on its mere production, and admissible in evidence against an individual in criminal, civil or even disciplinary matters.

Social media

There is a dearth of case law about social media and the background between the parties to a dispute about the posting of defamatory statements is usually a good indicator of inappropriate motive (*H v W* in para [9] [64]). A person can institute an action for damages for defamation or *injuria* as was the case in *Hanekom v Zuma* based on the evidence of a tweet. The elements of defamation or injuria must be proved. A two-stage inquiry is followed, namely establishing the ordinary meaning of the words expressed in the statement and secondly, whether the remarks are defamatory insofar as they caused injury to the dignity of a person (*Hanekom v Zuma*; *Du Toit v Coetzee* in para [11]). "Fake news" campaigns can cause considerable harm to both individuals and organisations. Tracing a person who submitted fake news anonymously on a computer can be challenging, and it is imperative to establish firstly the identity of the sender (Iyer 2018:127) [65]. The Cybercrimes Act currently forces companies to keep evidence of criminal cyber activities at their own cost (Michaelsons 2021) [66]. In addition, employers should

integrate an online social media policy into their terms and conditions of employment, providing clear guidelines for unacceptable social media use by employees. It is suggested that this is an opportunity for forensic analysts to assist in developing sustainable policies and procedures for current employers and for future generations of employees.

Conclusion

This article explains that electronic communication such as data messages, collected lawfully by the forensic analyst and his or her team, taking all the factors mentioned above into consideration, are admissible as evidence in legal proceedings. The requirements for admissibility of each of the two types of data messages discussed in this article, namely emails and SMSs, are unique to establish authentication and adhere to the chain of custody requirements. The judiciary does not enforce these requirements in all cases unless challenged by a party to the dispute. Data messages, such as WhatsApp or tweets, are also not denied as evidence in terms of the requirements of the Law of Evidence Amendment Act. These requirements are determined in terms of the provisions of the Cybercrimes Act, ECTA, the Law of Evidence Amendment Act and the common law.

Its admissibility and evidential weight as data messages are analogous as evidence for both email and SMS. Emails exchanged between parties are accepted as evidence. This similarly applies to SMS, WhatsApp, tweets, or other social media technology. Data messages are not merely excluded as evidence in any legal proceedings because of their electronic nature. However, a court would consider several factors to determine its relevance as determined by section 15(3) of the ECTA. The form in which data messages are to be presented in court must conform to section 15 of the ECTA. For the forensic analyst, success lies in gathering information (electronic evidence), adhering to the chain of custody of evidence and complying with the admissibility requirements of evidence against any person in criminal, civil or disciplinary matters. Such success will aid in serving justice against white-collar criminals and send a strong message to those who intend to commit fraud. Prevention is better than cure and adding robust cybersecurity protocols to an organisation's digital network will go a long way in protecting people, processes and technology to ensure the organisation's survival. As is now up to a company to keep evidence of cybercrimes at their own cost, it pays to minimise risks and to put in place policies and protocols to prevent cybercrimes.

Acknowledgement

This research was supported by the efforts of research, finance and ethical committees and personnel at the University of South Africa and by the organisers, reviewers, and administrative personnel of the Ontario International Development Agency.

Bibliography

[1] Jacobellis v Ohio 378 U.S. 184 (1964); https://www.thefire.org/first-amendment-library/decision/jacobellis-v-ohio/

[2] Electronic Communications and Transactions (South Africa) Act, 25 of 2002, Pretoria: Government Printer. https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

[3] Criminal Procedure (South Africa) Act 51 of 1977, Pretoria: Government Printer. https://www.justice.gov.za/legislation/acts/1977-051.pdf

[4] Cybercrimes (South African) Act, 19 of 2020, Pretoria: Government Printer. https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

[5] Protection of Personal Information (South African) Act 4 of 2013, Pretoria: Government Printer. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

[6] Williams, G, Fourie, T and Siyaya, S. (2021). The newly enacted Cybercrimes Act and what it means for South Africans. https://www.golegal.co.za/newly-enacted-cybercrimes-act/

[7] Clough, J.A. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation Monash University Law Review 40(3) 698-736 https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf

[8] Council of Europe. (2022). The Budapest Convention (ETS No.185) and its Protocols. https://www.coe.int/en/web/cybercrime/the-budapest-convention

[9] Swales, L. (2018). An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: Suggestions for reform – Part one. PER/PELJ 2018(21)1-30 https://perjournal.co.za/article/view/2916

[10] S v Brown (CC54/2014) [2015] ZAWCHC 128 (17 August 2015). http://www.saflii.org/za/cases/ZAWCHC/2015/128.html

[11] McKemmish, R. (2008). When is digital evidence forensically sound? Advances in digital forensics IV 3-15. https://link.springer.com/chapter/10.1007/978-0-387-84927-0_1

[12] Ngomane, A.R. (2010). The use of electronic evidence in forensic investigation. Magister Technologiae. The University of South Africa (UNISA). https://uir.unisa.ac.za/bitstream/handle/10500/4200/dissertation_ngomane_a.pdf

[13] Hajdarevic, K. and Dzaltur, V. (2015) An approach to digital evidence collection for successful forensic application: An investigation of blackmail case. Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2015 38th International Convention. 1387-1392 IEEE. https://www.academia.edu/27037800/An_Approach_to_Digital_Evidence_Collection_for_Successful_Forensic_Application_An_Investigation_of_Blackmail_Case

[14] Alixpartners. (2022). Alixpartners' 2022 litigation and corporate compliance survey. https://docs.alixpartners.com/view/1050469772/

[15] Fourie v Van der Spuy and De Jongh Inc. And Others (65609/2019) [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP) (30 August 2019) http://www.saflii.org/za/cases/ZAGPPHC/2019/449.html

[16] Mitchell, D. (2022). BVI Court freezes Crypto Wallets. https://www.lexology.com/commentary/banking-financial-services/british-virgin-islands/ogier/bvi-court-freezes-crypto-wallets

[17] Kirkevold M 1997 'Integrative nursing research – an important strategy to further the development of nursing science and nursing practice' Journal of Advanced Nursing 25 977–984 https://doi.org/10.1046/j.1365-2648.1997.1997025977.x

[18] Law of Evidence Amendment (South African) Act 45 of 1988, Pretoria: Government Printer. https://www.gov.za/sites/default/files/gcis_document/201505/act-45-1988.pdf

[19] Constitution of the Republic of South Africa, 1996. https://www.gov.za/documents/constitution-republic-south-africa-1996

[20] Southern African Legal Information Institute. http://www.saflii.org/

[21] Ernst & Young. (2022). How cyber governance and disclosures are closing the gaps in 2022. https://www.ey.com/en_sy/tmt/how-cybersecurity-framework-implementation-can-transform-from-standard-to-innovative

[22] Bellengere, A., Palmer, R., Theophilpoulos, C., Whitcher, B., Roberts, L., Melville, N., Picarra, E., Illsey, T., Nkutha, M., Naude, B., Van der Merwe, A. and Reddi, M. (2013). The Law of Evidence in South Africa Oxford University: Press Oxford.

[23] Association of Certified Fraud Examiners (ACFE). (2016). Fraud examiners manual 2016 International Edition Austin TX National Association of Fraud Examiners. https://www.pdfdrive.com/fraud-examiners-manual-international-edition-2014-e189212955.html

[24] Cybercrimes and Cybersecurity Bill (2016), as introduced in the National Assembly (proposed section 75), Pretoria: Government Printer. https://www.gov.za/sites/default/files/gcis_document/201703/b6-2017cybercrimes170221a.pdf

[25] Peruzzotti, M. and Sorrentino, B. (2022). Ministry of Security publishes regulation to strengthen cybersecurity and cybercrime. Lexology. https://www.lexology.com/commentary/tech-data-telecoms-media/argentina/ojam-bullrich-flanzbaum/new-cybersecurity-and-it-regulations

[26] Watney, M. (2009). Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position. *Journal of* Information, Law & Technology. http://go.warwick.ac.uk/jilt/2009_1/watney

[27] Mabeka, N.Q. (2021). An analysis of the implementation of the CaseLines system in South African Courts in the light of the provisions of section 27 of the Electronic Communications and Transactions Act 25 of 2002: A beautiful dream come true in Civil Procedure. PER 2021(24). https://perjournal.co.za/article/view/8707

[28] Nortje, J.G.J and Myburgh, D.C. (2019). The search and seizure of digital evidence by forensic investigators in South Africa. PER 22(1). http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812019000100015#back_fn125

[29] Mason, S. and Seng, D. (2016). Electronic evidence. Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, *University of London*, 2017. https://doi.org/10.14296/97819115070 79

[30] Chhabra, G.S. and Bajwa, D.S. (2015). Review of E-mail System, Security Protocols and Email Forensics. International Journal of Computer Science & Communication Networks, 5(3) 201-211. file:///C:/Users/uyswr/Downloads/paperEmailForensics-IJCSCN.pdf

[31] Gupta, S., Gupta, K. and Singla, A. (2016). E-Mail Header-A Forensic Key to Examine an E-Mail. https://www.irjet.net/archives/V3/i2/IRJET-V3I2110.pdf

[32] Giova G 2011 Improving chain of custody in forensic investigation of electronic digital systems. International Journal of Computer Science and Network Security 11(1) 1-9 http://paper.ijcsns.org/07_book/201101/20110101.pdf

[33] Page & Others v Additional Magistrate, Somerset West and others (11275/2015) [2016] ZAWCHC 63; 3 All SA 619 (WCC) (20 April 2016) http://www.saflii.org/za/cases/ZAWCHC/2016/63.html

[34] General Council of the Bar of South Africa v Jiba and Others (23576/2015) [2016] ZAGPPHC 833; [2016] 4 All SA 443 (GP); 2017 (1) SACR 47 (GP); 2017 (2) SA 122 (GP) (15 September 2016) http://www.saflii.org/za/cases/ZAGPPHC/2016/833.html

[35] Chang, C.P., Chen, C.T., Lu, T.H., Lin, I.L., Huang, P. and Lu, H.S. (2013). Study on constructing forensic procedure of digital evidence on smart handheld device. System Science and Engineering (ICSSE) 2013 International Conference 223-228 IEEE. https://ieeexplore.ieee.org/document/6614664

[36] Peters, M.T., Price, D.L., Riordan, J.C., Vennam, B.M. and Vennam, R. (2016). International Business Machines Corporation (2016). Recommending sites through metadata analysis US Patent 9390323.

[37] T v T (287/2021) [2022] ZASCA109; 2022 (2) SACR 233 (SCA) (15 July 2022) https://www.saflii.org/za/cases/ZASCA/2022/109.html

[38] Mitchell, C.S. (2013). Investigating the use of forensic stylistic and stylometric techniques in the analysis and authorship on a publicly accessible social networking site (Facebook) Pretoria: UNISA https://uir.unisa.ac.za/handle/10500/13324

[39] Ragel, R., Herath, P. and Senanayake, U. (2013). Authorship detection of SMS messages using unigrams. Industrial and Information Systems, 2013 8th IEEE International Conference on Communication Software and Networks 387-392 IEEE. https://ui.adsabs.harvard.edu/abs/2014arXiv1403.1314R/abstract

[40] Altamimi, A., Clarke, N., Furnell, S. and Li, F. (2019). Multi-Platform Authorship verification. In proceedings of the Third Central European Cybersecurity Conference. https://dl.acm.org/doi/abs/10.1145/3360664.3360677

[41] Tuarob, S., Tucker, C.S., Salathe, M. and Ram, M. (2014). An ensemble heterogeneous classification methodology for discovering health-related knowledge in social media messages http://www.sciencedirect.com/science/article/pii/S1532046414000628

[42] Ishihara, S 2013 Probabilistic Evaluation of SMS Messages as Forensic Evidence: Likelihood Ratio Based Approach. Emerging Digital Forensics Applications for Crime Detection, Prevention and Security 138. https://www.igi-global.com/gateway/chapter/75669#pnlRecommendationForm

[43] Dlamini, I., Olivier, M.S. and Grobler, M.M. (2016). The smartphone evidence awareness framework for the users 11th International Conference on Cyber Warfare and Security: ICCWS2016 439 Academic Conferences and publishing limited. http://toc.proceedings.com/30046webtoc.pdf

[44] Hanekom v Zuma (D6316/2019) [2019] ZAKZDHC 16 (6 September 2019) https://www.saflii.org/za/cases/ZAKZDHC/2019/16.html

[45] Netshipise v Munnick and Others (29585/2018) [2018] ZAGPJHC 547 (14 August 2018) http://www.saflii.org/za/cases/ZAGPJHC/2018/547.html

[46] Heroldt v Wills [2014] JOL 31479 (GSJ) https://lawblogsa.files.wordpress.com/2013/10/heroldt-v-wills.pdf

[47] Publication Controls Board v William Heineman Ltd and Others 1965 (4) SA 137 (A)

[48] Du Toit v Coetzee (A122/2021) [2022] ZAFSHC 105 (2 June 2022) https://www.saflii.org/za/cases/ZAFSHC/2022/105.html

[49] Media Defence (2020) Cybercrimes module 7: Summary Modules on litigating digital rights and freedom of expression online. https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercrimes.pdf

[50] Msomi v S (39/2018) [2019] ZAECGHC 80; 2020 (1) SACR 197 (ECG) (3 September 2019) http://www.saflii.org/za/cases/ZAECGHC/2019/80.html

[51] Jafta v Ezemvelo KZN Wildlife (D204/07) [2008] ZALC 84; [2008] 10 BLLR 954 (LC); (2009) 30 ILJ 131 (LC) (25 September 2009) http://www.saflii.org/za/cases/ZALC/2008/84.html

[52] Du Plessis v Independent Regulatory Board for Auditors and Others (8572/2016) [2017] ZAWCHC 49; [2017] 3 All SA 137 (WCC) (26 April 2017) https://www.saflii.org/za/cases/ZAWCHC/2017/49.html

[53] Konsult One CC v Strategy Partners (Pty) Ltd (2607/10) [2013] ZAWCHC 55 (19 March 2013) http://www.saflii.org/za/cases/ZAWCHC/2013/55.html

[54] Woolworths v Commissioner Matlala NO and Others (JR2915/08) [2010] ZALC 188 (8 December 2010) http://www.saflii.org/za/cases/ZALC/2010/188.html
[55] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash (725/13) [2014] ZASCA 178, 2015 (2) SA 118 (SCA) (21 November 2014) http://www.saflii.org/za/cases/ZASCA/2014/178.html
[56] Jepson NO v Lezar (6453/2007) [2009] ZAFSHC 49 (9 April 2009) http://www.saflii.org/za/cases/ZAFSHC/2009/49.html
[57] Myburgh v Equestrian Valley (Pty) Ltd (15986/2012) [2016] ZAWCHC 6 (4 February 2016) http://www.saflii.org/za/cases/ZAWCHC/2016/6.html
[58] Mnyandu v Padayachi (AR162/2014) [2016] ZAKZPHC 78; [2016] 4 All SA 110 (KZP); 2017 (1) SA 151 (KZP) (1 August 2016) http://www.saflii.org/za/cases/ZAKZPHC/2016/78.html
[59] Ramaridili v MTN SA Innovation Centre (05951/2012) [2014] ZAGPJHC 118 (3 June 2014) https://www.saflii.org/za/cases/ZAGPJHC/2014/118.html
[60] Samtoy CC v Haffenden Groves (Pty) Ltd (49507/12) [2014] ZAGPPHC 336 (14 April 2014) http://www.saflii.org/za/cases/ZAGPPHC/2014/336.html
[61] Charioteer Trading CC v Fontis Holdings (Pty) Ltd (1500/2012) [2014] ZANWHC 38 (21 August 2014) https://www.saflii.org/za/cases/ZANWHC/2014/38.html
[62] Democratic Alliance v African National Congress (CCT 76/14) [2015] ZACC 1; 2015 (2) SA232 (CC) (19 January 2015) http://www.saflii.org/za/cases/ZACC/2015/1.html
[63] S v Shange and Others (CC169/07) [2012] ZAKZPHC 69 (29 June 2012) http://www.saflii.org/za/cases/ZAKZPHC/2012/69.html
[64] H v W (12/10124) [2013] ZAGPJHC 1; 2013 (2) SA 530 (GSJ); 2013 (5) BCLR 554 (GSJ); [2013] 2 All SA 218 (GSJ) (30 January 2013) http://www.saflii.org/za/cases/ZAGPJHC/2013/1.html
[65] Iyer, D. (2018). An analytical look into the concept of online defamation in South Africa. Speculum Juris Vol 32(2) 125-134. http://www.saflii.org/za/journals/SPECJU/2018/10.pdf
[66] Michaelsons. (2021). The practical impact of the Cybercrimes Act on you. https://www.michalsons.com/blog/the-practical-impact-of-the-cyber-bill-on-you/25300

About the authors:

Name: Werner Uys
Email: uyswr@unisa.ac.za
Tel No +27124294385

Name Kobus Joubert
Email: joubek@unisa.ac.za
Tel No +27124294068

Mailing address:
UNISA Main Campus
Preller Street
Muckleneuk Ridge
Pretoria
South Africa
0003