http://go.warwick.ac.uk/jilt/2009_1/nieman

Journal of Information, Law and Technology

Cyberforensics: Bridging the Law/ Technology Divide[1]

Dr. Annamart Nieman
Director: Deloitte and Touche, South Africa
annamart@telkomsa.net

***Lex Informatica* Conference, 21st – 23rd May 2008**
Pretoria, South Africa

This is a **Commentary** published on 28 May 2009-06-04

Citation: Nieman, A., 'Cyberforensics: Bridging the Law/Technology Divide', 2009(1) *Journal of Information, Law & Technology (JILT)*
<http://go.warwick.ac.uk/jilt/2009_1/nieman>

Abstract

New technologies are known to challenge existing legal concepts. The conversion of binary data into electronic evidence, and the collection of such electronic evidence with appropriate legal and technical tools, is but one of the manifold challenges presenting legal practitioners with an opportunity to explore the law/technology divide. Cyberforensics provides the contemporary and internationally accepted converter of choice by means of which to translate binary data into electronic evidence. It entails the process of unearthing evidence from computer media in order to support legal proceedings. Anti-cyberforensic techniques refer to the intentional or accidental changing of data that can obscure the data, encrypt it or hide it from forensic tools. This paper is aimed at elucidating basic concepts underscoring cyberforensics as a means to an end; the end being the collection and analysis of electronic evidence in such a way that it enables the successful admission of this evidence into a court of law, whilst optimally preserving its evidential weight. These concepts are explored by means of a technical contextualisation and within the parameters of the South African legislative framework. South Africa is a signatory to the Cybercrime Convention, which is currently the only existing internationally accepted benchmark, *inter alia*, for the procedural powers aimed at the collection of electronic evidence. Reference will accordingly also be made to the Cybercrime Convention.

Keywords

Electronic evidence; cyberforensics/computer forensics; digital anti-forensics/anti-cyberforensics; cyberlaw; information technology law; procedural powers; Cybercrime Convention.

1. Introduction

It has been said that the ostrich that buries its head in the sand has a bigger problem than limited vision: its rear end becomes an enormous target. By analogy to contemporary computing contexts, this sentiment clamours for, at the very least, an appreciation of the risks associated with doing business in the Third Wave of Change (as opposed to the Agricultural First Wave and the Industrial Second Wave).

New technologies, including the Internet, the World Wide Web (WWW), Electronic Mail (Email), Short Message Service (SMS), Multimedia Messaging Service (MMS), Voice over Internet Protocol (VoIP) and Instant Messaging (IM) have radically changed, and continue to change, the way we engage each other and go about conducting our business. There is no doubt that these technologies have become indispensable personal and business tools.

The exponential growth of information technology infrastructures such as computer networks and information superhighways not only creates increasing numbers of opportunities for potential offenders, but also, at the very least, an equal number of risks for potential victims (Moore, p.1). In South Africa, the risks associated with electronic data have only recently begun to receive the attention they warrant. Some of these risks include:

a) Failure by the Board of Directors to identify and address risks accompanying the use of information technology (IT) and/or failure by company management to implement Board decisions with regard to IT security. Such failure could render the Board

liable under governance related legislation such as section 424 of the Companies Act 61 of 1973.

b) Risks associated with the use of electronic communications by employees (such as criminal or civil liability resulting from email or SMS spam sent by employees; unauthorised disclosure of trade secrets or confidential information via email; privacy infringement attributed to unauthorised disclosure of third party personal information via email; the unauthorised monitoring of employee communications; and damage to a third party's computer network due to a virus unwittingly attached to an employee's email).

c) External security risks such as the unauthorised access of a company's computer network resulting in the loss of important data, the disclosure of personal information, intellectual property breaches, a slow down or down time of the company's network.

d) Risks associated with websites and *e*-commerce, examples of which include: liability for intellectual property infringement when a feature used on a company's website infringes third party content; failure to provide online consumers with an opportunity to review and withdraw from *e*-commerce transactions; failure to ensure a safe and secure website payment gateway resulting in the disclosure of personal or financial information and liability for email or SMS spam.

e) The shift in the focus of crime from physical objects to intangibles, targeted by anonymous or pseudonymous individuals, irrevocably changed the risk management environment. The spread of computer technology into almost all areas of life, as well as the interconnection of computers via international computer networks, has made computer crime more diverse, more dangerous, more international and more challenging to fight than its physical counterparts, where such counterparts exist. In addition, the growing use of computers renders the successful investigation and prosecution of even traditional crimes all the more dependent on evidence stored or processed by means of modern information technology (Mobrien.com, 2006, par 146, pp.1-8 <http://www.mobrien.com/computer_crime4.htm>).

It is evident that the ubiquity of the Internet and the connectivity of virtually every workstation to this global community have ramifications that have yet to be worked out. The mitigation and management of the risks ushering in the Information Age are typically facilitated by a combination of technical, legal and governance mechanisms. It is imperative that the most potent cocktail of these mechanisms be mixed in order to best serve the context that it is customised for and directed at.

The plot thickens intriguingly so when, in practice, one endeavours to explore the multidisciplinary approach necessitated to enable the mixing of this risk management cocktail. Suffice it to say that the relationship between the law and information technology can be better understood in the light of a Chinese curse that expresses the wish that the addressee should 'live in interesting times' (Lloyd, 2004, p. xlvx).

2. Bridging the Law/Technology Divide – A Small Step or a *Quantum Leap* for Lawyers?

New technologies are known to challenge existing legal concepts and there has always been a significant lag between the development of technology and the development of the law. Legal

mechanisms are often regarded as mustard after the (technological) meat. As both the online and offline worlds are grappling with the effects and consequences of risks gone awry in a globally interlinked economic environment, new laws have only recently emerged to establish the ground rules.

Three of the most important legislative interventions in this respect in South Africa, of course, include the Electronic Communications and Transactions Act 25 of 2002 (the ECT Act), the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (the RICPCIA) and the Electronic Communications Act 36 of 2005. Also, the current voluntary regime governing the collection of private and personal information obtained by means of electronic transactions, in future, will be substituted by privacy and data protection legislation of which due cognisance has to be taken.

Making technological sense of these new ground rules can be a daunting task. An age-old reliance on tangible evidence, hard fact and understanding of human motivation are considered some of the primary reasons why lawyers are held to be members of one of the most technophobic professions on earth (Grant, 1995, p.1):

> One thing lawyers like is certainty. Computers seldom give it. If anything, they show that we live in a universe where uncertainty rules, and if your livelihood depends on your predictability, that's a hard thing to stomach.

However, in analogous terms, being stuck in a world where bartering is the dominant mode when attempting to manage risks in contemporary financial markets will leave one clueless: a basic appreciation of payment systems and legal tender is essential. Similarly, some handle on the technicalities underlying the legalities (and vice versa) is non-negotiable.

The breathtaking pace of change and the sometimes startling complexity of the exceedingly complex technologies involved in computers and networks have important ramifications for the legal process and its protagonists. The conversion of binary data into electronic evidence, and the collection of such electronic evidence with appropriate legal and technical tools, is but one of the manifold challenges offering practitioners with an opportunity to rise to the occasion when exploring the law/technology divide.

In as much as Confucius's journey of a thousand miles began with a single step, an understanding of the technicalities intertwined with the collection of electronic evidence begins with knowing that you know not. This notion, coupled with the aspiration to remain relevant and meaningful in the Third Wave, could challenge lawyers to their very (stereotypically arrogant) core and set them afoot on a truly humbling experience that requires enormous perseverance. This article aims to assist legal practitioners by introducing the following concepts underscoring an understanding of this challenge:

a) binary data and electronic evidence;

b) cyberforensics and anti-forensic techniques;

c) legal electronic evidence collection mechanisms.

These concepts will be explored by means of a technical contextualisation and within the parameters of the South African legislative framework. In November 2001 South Africa signed the Council of Europe's Cybercrime Convention Budapest 23.XI.2001 CETS No: 185 (the Cybercrime Convention) <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>. At present, the Cybercrime Convention is the only existing internationally accepted benchmark, *inter alia*, for the procedural powers aimed at the collection of electronic evidence. Section 39(1)(b) of the Constitution of the Republic of South Africa 1996, furthermore contains the express command that a court, tribunal or forum must consider international law when interpreting the Bill of Rights. Reference will accordingly also be made to the Cybercrime Convention.

3. Mining the Forensic Gold: From Binary Data to *E*-Evidence

It is important to note that when collecting electronic evidence, hardware is not simply transported from an evidence collection point to an evidence storage facility. Similarly, when the production or preservation of information in electronic format is requested, the process does not merely involve the handing over or isolation of hardware. On the contrary, when searching and seizing, intercepting and monitoring, preserving or producing information collected from computing environments, one enters the business of browsing or busting the binary in search of electronic evidence. This essentially entails a transition from the tangible to the largely intangible realm.

Information has become digitised and dematerialised. In contemporary computing, 'data' refers to information that has been translated into a form that is convenient to process. In respect of today's computers and transmission media, data is information converted into a digital form (Whatis.com searchStorage.com Definitions 'Data', 2001, pp.1-2 <http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211894,00.html>).

'Digital' refers to the use of binary code to represent information (Google 'Definitions of Digital on the Web', 2004. pp.1-3, <http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=define%3Adigital>). All computer data is ultimately a series of zeros and ones and can therefore be represented as binary numbers. Binary data that has been broken down into the smallest unit that a computer is capable of representing and/or recognising is called a 'bit' (derived from binary digit). A bit represents one of two values, on or off, since most computers are electronic devices powered by electricity, which also has only two states, on or off (Shelly, Cashman and Vermaat, 2002, p.4.15).

Computer data, as the object of evidence collection interventions, therefore encompasses any electronic representation of information that is suitable for processing by a computer and, as such, is capable of being reduced to binary.

Computer data may exist in two forms, namely static, recorded or stored; or fluid, in flux or movement or in the process of communication (Council of Europe 'Explanatory Report to the Convention on Cybercrime (ETS No 185)', 2001, pp.1-68 <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>) [the Council of Europe's Explanatory Report to the Cybercrime Convention]. The definition of computer data typically includes three specific types of communications data, namely content data; traffic data or

communication-related information; and subscriber information. It is important to distinguish between different types of computer data, because different legal collection regimes dictate the collection of each type of data. The applicability of an evidence collection mechanism (such as an interception and monitoring direction; a search and seizure, production or preservation order) to a particular type or form of data depends on the nature and form of the data that is to be collected.

Whereas computer data encompasses any binary representation of information that is suitable for processing by a computer, information is the organised, meaningful and useful end product of data processing. Information is converted into evidence when it becomes admissible as evidence in a court of law.

Broadly defined, electronic evidence is electronically stored information that can be used as evidence in any legal action (Volonino, 2003, p.7). This includes any information of probative value that is either stored or transmitted in a binary form, by means of, for example, cellular phones, digital fax machines, digital audio and digital video (Whitcomb, 2002, p.4). *E*-evidence constitutes the ultimate objective of an evidence collection intervention directed at computing environments. The final objective of computer forensics is to collect and analyse computer evidence in such a way that it enables the successful admission of this evidence in a court of law.

Generally, there are two types of electronic evidence, namely physical and logical electronic evidence. In many cases, both of these leave 'bread crumbs' behind on a crime scene. Most computer criminals appear to reuse the same machinery and hard drives, and these constitute the physical evidence. Evidence that resides in log files, embedded in software, in memory or within the file system, is considered logical evidence. Along with the physical and logical evidence, there is a subclass of volatile and non-volatile information. Volatile information may only exist for a short time or may disappear. Volatile evidence is often the most useful for making a case, but it is also the most difficult to preserve and collect, sometimes at the expense of other information or all the evidence contained on the device itself (Rittinghouse, and Hancock, 2003, p.389). The most prevalent types of electronic evidence are mined from email, background information and data files.

Electronic evidence that could be mined from background information includes (Feldman, 2003, pp.4-5, <http://www.forensics.com/pdf/Essentials_of_Discovery.pdf>):

a) non-printing information (such as the date and time stamp that the operating system puts on every file, revisions of documents and hidden comments);

b) access control lists that limit the rights of users to access, view and edit files; and

c) audit trials and computer logs that leave an electronic trial regarding, inter alia, network and computer usage (such as how, when, where and how long a user was on the system and information pertaining to the programs used, the files accessed, email sent and received and websites visited).

Electronic evidence that could be mined from data files includes:

a) active data that is readily available and accessible to users;

b) replicant data (such as automatically backed-up file clones);

c) backup data that provides a historical snapshot of the data stored on the system on the particular day that the backup was made; and

d) residual data that appears to be gone, but is still recoverable from the computer system (such as deleted files that are still extant on a disk surface and data existing in other system hardware, examples of which include the buffer memories of printers, copiers and fax machines).

Electronic evidence encapsulated in computer records containing text are often divided into two categories, namely computer-generated records and computer-stored records. The difference hinges upon whether a person or a machine created the record's contents. Computer-stored records refer to documents that contain the writings of some person or persons and that happen to be in electronic form, including email messages, word processing files and Internet chat room messages. By contrast, computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records and ATM receipts are all computer-generated records (USA CCIPS 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations', 2002, p.101 <http://www.cybercrime.gov/s&smanual2002.htm>) [USA CCIPS].

With reference to the Cybercrime Convention and the South African legislative framework, the procedural measures introduced in section 2 of the Cybercrime Convention for purposes of the collection of electronic evidence in general refer to all types of data. Such data may exist in two forms, namely as stored data or data involved in a process of communication. The applicability of a particular evidence collection procedure to a particular type or form of electronic data depends on the nature and form of the data and on the nature of the procedure, specifically described in each of the articles set out in the Cybercrime Convention that allows for the acquisition of that particular type of data (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.24).

Article 1(b) of the Cybercrime Convention defines 'computer data' as

> … any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

This definition of computer data is built on the definition of data proposed by the International Standards Organisation (ISO) of the United Nations, with specific reference to the terms 'suitable for processing'. The term 'computer data', as introduced by the Cybercrime Convention, must be understood as data in an electronic form or in another directly processable form. The electromagnetic emissions emitted by a computer during its operation are not considered data in terms of the definition in article 1 of the Cybercrime Convention. However, data can be reconstructed from such emissions (the Council of Europe's Explanatory Report to the Cybercrime Convention, pp.6-12).

Automatically processed computer data may be the target of one of the criminal offences defined in the Cybercrime Convention (i.e. illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and

neighbouring rights). Such data may also be the object of the application of one of the investigative measures created by the Cybercrime Convention. The domestic investigative measures created by the Cybercrime Convention are the following: search and seizure of stored computer data; production orders; the expedited preservation of stored computer data; the expedited preservation and partial disclosure of traffic data; the real-time collection of traffic data; and the interception of content data. The transborder investigative measures proposed by the Cybercrime Convention are the following: the expedited preservation of stored computer data; the expedited disclosure of preserved traffic data; mutual assistance regarding the accessing of stored computer data; transborder access to stored computer data with consent or where publicly available; mutual assistance regarding the real-time collection of traffic data; and mutual assistance regarding the interception of content data.

Section 1 of the ECT Act defines data as 'electronic representations of information in any form'. The real currency of the ECT Act is, however, 'data messages', which are defined in section 1 as

> …data generated, sent, received or stored by electronic means and [this] includes voice, where the voice is used in an automated transaction; and a stored record.

Computer data therefore encompasses any electronic representation of information that is suitable for processing by a computer, including communications data (considered in more detail below).

3.1 Communications Data: A Special Type of Computer Data

An 'electronic communication' is defined in article 1 of the ECT Act as 'a communication by means of data messages'. Section 1 of the Telecommunications Act 1996, defines 'telecommunication' as the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio or other electromagnetic waves, or any agency of a like nature, whether with or without the aid of tangible conductors.

In general, the procedural measures introduced in article 2 of the Cybercrime Convention refer to all types of data. This includes three specific types of communications data, namely content data, traffic data and subscriber data. The latter may exist in two forms, namely stored or in the process of communication (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.24). The RICPCIA uses the term 'communication-related information' instead of 'traffic data'.

It is important to differentiate between different types of communications data, because the Cybercrime Convention and the RICPCIA introduce different legal regimes for each type of communications data. The applicability of a procedure to a particular type or form of data depends on the nature and form of the data and the nature of the procedure to be used. Accordingly, within a particular set of circumstances, any type of communications data may constitute the object of a search and seizure, production or preservation intervention. The different types of procedural powers (interception and monitoring, search and seizure, production, preservation and retention) that may be directed against computer data, including the different categories of communications data, will be elaborated upon below.

The meanings of the terms content data, traffic data, real-time and archived communication-related information and subscriber information warrant further attention. They are therefore defined below.

3.1.1 Content Data

'Content data' is not defined in the Cybercrime Convention. It is, however, generally understood to refer to the communication content of the communication. The communication content of a communication is the meaning or purport of the communication, or the message or information being conveyed by the communication. It is everything that is transmitted as part of the communication that is not traffic data (the Council of Europe's Explanatory Report to the Cybercrime Convention, pp.40-45).

Article 1(1) of the RICPCIA provides that the term 'contents', when it is used in respect of any communication, includes any information concerning the substance, purport or meaning of that communication.

3.1.2 Traffic Data

Computers generate traffic data in the chain of communication, in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.7). Article 1(d) of the Cybercrime Convention defines 'traffic data' as

> …any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Although not all categories of traffic data are always technically available, capable of being produced by a service provider or necessary for a particular criminal investigation, the definition of 'traffic data' in the Cybercrime Convention exhaustively lists the categories of traffic data that are treated by a specific legal regime in the Cybercrime Convention. These categories are (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.7):

a) the 'origin', which refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services;

b) the 'destination', which refers to a comparable indication of a communications facility to which communications are transmitted; and

c) the 'type of underlying service', which refers to the type of service used within the network, for example, file transfer, e-mail, or instant messaging (IM).

The RICPCIA introduces the more detailed term 'communication-related information'. This term encompasses the Cybercrime Convention's concept of traffic data. Section 1(1) of the RICPCIA defines 'communication-related information' as

> …any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system.

The RICPCIA also discerns between archived and real-time communication-related information. 'Archived communication-related information' is defined as

> …any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30(1)(b) for the period determined in a directive referred to in section 30(2)(a), beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates.

'Real-time communication-related information' is defined as

> …communication-related information which is immediately available to a telecommunication service provider before, during, or for a period of 90 days after, the transmission of an indirect communication; and in a manner that allows the communication-related information to be associated with the indirect communication to which it relates.

3.1.3 Subscriber Information

Subscriber information includes various types of information about the use of a service and the user of that service. Subscriber information is defined in section 18(3) of the Cybercrime Convention as any information contained in the form of computer data or any other form and held by a service provider relating to subscribers of its services, other than traffic data or content data, which can be used to establish

a) the type of communication service used, the technical provisions taken and the period of service;

b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; and

c) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Section 1 of the RICPCIA defines a 'customer' as any person to whom a telecommunications service provider provides a telecommunications service; or who has entered into a contract with a telecommunications service provider for the provision of a telecommunications service, including a pre-paid telecommunications service.

Chapter 7 of the RICPCIA details the duties of telecommunications service providers and customers. A telecommunications service provider may obtain any information that it deems necessary, for the purposes of the RICPCIA, from a person who enters into a contract with such a provider for the provision of a telecommunications service. The procurement of a minimum threshold of information is obligatory. In the case of a natural person, the following information must be obtained: full names, identity number, residential and business or postal address (whichever is applicable) and a certified photocopy of the person's identification document on which her photo, full names and identity number (whichever is applicable) appear. In the case of a juristic person, the following information must be obtained from the person representing that juristic person: full names, identity number, residential and postal address (whichever is applicable); the business name and address and, if registered as such in terms of any law, the registration number of the juristic person; a certified photocopy of the identification document on which the photo, full names and identity number (whichever is applicable) of the person representing the juristic person appear; and a certified photocopy of the business letterhead of, or other similar document relating to, the juristic person. Telecommunications service providers must ensure that proper records are kept of the information.

4. The Collection of Electronic Evidence

Legal tools enabling the collection of electronic evidence (such as interception and monitoring directives; search and seizure, production and preservation orders) infringe upon the right to privacy. The most embryonic of protections in respect of the right to privacy currently exists in the area of information acquisition, retention and dissemination. Buttressing the need for the protection of information is the move toward targeted policing and the creation of databases of knowledge as tools of crime control (Sharpe, 2000, pp.1 and 220).

In most jurisdictions, the powers of interception and monitoring of communications have traditionally been seen as more intrusive than the powers of searching and seizing. This resounds locally in South Africa, for example, in the fact that interceptions and monitoring are only allowed in respect of certain serious offences, as set out in the Schedule to the RICPCIA and in the definition of a 'serious offence' in article 1 of the preceding Interception and Monitoring Prohibition Act 1992). Content data is generally also more jealously guarded than, for example, traffic and subscriber data (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.40). In its turn, the powers to request and/or order the production or preservation of information could, arguably, be considered less infringing to the right to privacy than the powers of search and seizure. Consequently, the law has evolved gradually into different legal powers, emanating from different legal regimes, so as to extend protection to the different facets of the right to privacy.

The question arises whether (and if so, to what extent) the distinction between the facets of the right to privacy that are more and less worthy of protection remains relevant in contemporary computing contexts. So, for example, technology is challenging the legal

concepts of search and seizure and interception and monitoring, in that some of the traditional distinctions between these concepts overlap or become blurred in computing environments. Interconnected computer systems provide, for example, the possibility that the search of stored data can be carried out from remote terminals. Where the data is not transferred, but only surveyed or copied, this can be done without the knowledge of the owner or custodian of the data. In theory, this renders a search and seizure intervention as secretive as an interception or monitoring (Council of Europe 'Explanatory Memorandum to Recommendation 1995(13) on Problems of Criminal Procedural Law connected with Information Technology', 1995, p.12, <http://cm.coe.int/stat/E/Public/1995/ExpRep(95)13.htm>) [Council of Europe's Explanatory Memorandum to Recommendation 1995(13)].

Another example of technology forcing the convergence of legal concepts is attributable to the transmutable nature of computer data. Examples of such transmutation include cases where data are converted from an electromagnetic form to a paper printout, a visual representation on a monitor screen or an auditory simulation of human speech. Whereas a search is generally executed in respect of existing recorded data, an interception is aimed at data that is being processed into the form in which it is concurrently transmitted and intercepted. However, data within a computer system can change its form and it can be transmitted from one location to another. Previously recorded data may, accordingly, be transmitted in the same or another electronic format and may be intercepted during this period of transmission (Council of Europe's Explanatory Memorandum to Recommendation 1995(13), p.12).

The approach taken by the international legal community, as reflected in the Cybercrime Convention, is to develop, supplement and continue applying existing legal concepts.

The first principle in the Council of Europe's Recommendation No R(95)13 of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law connected with Information Technology [the Council of Europe's Recommendation 1995(13)] accordingly requires that the legal distinction between the search of computer systems and the seizure of data stored therein, as opposed to the interception of data in the course of transmission, be clearly delineated and applied (Council of Europe 'Recommendation No R(95)13 of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law connected with Information Technology', 1995, pp.1-4, <http://cm.coe.int/ta/rec/1995/95r13.htm>). The reason for this is, specifically, the fact that different legal powers, emanating from different legal regimes, in respect of different categories of computer data, are required in order to execute the actions of search and seizure as opposed to the actions of interception and monitoring. While the end result in both instances is the acquisition of data, the preconditions for using the accompanying safeguards and the scope of these two coercive powers differ (Council of Europe's Explanatory Memorandum to Recommendation 1995(13), p.11).

The differentiation between search and seizure and interception and monitoring is based upon the format and inertness of the data at the time of its gathering. Data that is static, recorded and stored, is acquired by means of a search and seizure intervention. However, if the data is fluid and in movement, acquisition is accomplished by means of an interception and monitoring intervention (Council of Europe's Explanatory Memorandum to Recommendation 1995(13), p.12).

The Cybercrime Convention not only adapts traditional search and seizure powers to the demands of the volatile technological environment, but has also created new measures to ensure the continued effectiveness of search and seizure legal devices or to provide less intrusive alternative powers. The production, preservation and partial disclosure mechanisms proposed by the Cybercrime Convention signal ways in which search and seizure mechanisms could be facilitated, supplemented or aligned to the dictates of technological progress.

A more detailed description (with specific reference to the Cybercrime Convention and the South African legislative framework) of the following electronic evidence collection mechanisms is provided below: interception and monitoring; search and seizure, production and preservation.

4.1 Interception/collection and Monitoring

Interception and monitoring in accordance with the Cybercrime Convention is directed at data that is fluid and in movement (the Council of Europe's Explanatory Memorandum to Recommendation 1995(13), pp.11-12). It entails the collection of data in currently generated communications collected at the time of the communication. Such data is, generally, in the process of being created at the time when it is gathered. The gathering of real-time data takes place during a certain period in respect of data that will be created or, if it has already been created and recorded, will be transmitted at a particular time or period in the future. Interception and monitoring is generally secretive or surreptitious and the physical presence of law enforcement officers is generally not necessary (the Council of Europe's Explanatory Report to the Cybercrime Convention pp.39-40).

Whilst operationally acknowledging that data is 'collected' in both situations, the Cybercrime Convention refers normatively to the collection of traffic data as 'real-time collection' and to the collection of content data as 'real-time interception'. The rationale behind this is to assist in recognising the distinction made by some states, including South Africa, between the real-time interception of content data and the real-time collection of traffic data. The common operational use of the term 'collect or record' in the Cybercrime Convention is intended also to recognise that some jurisdictions do not differentiate between the collection of traffic data and the interception of content data (Council of Europe's Explanatory Memorandum to Recommendation 1995(13), pp.40-41).

'Interception', in terms of section 1(1) of the RICPCIA, means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, in order to make some or all of the contents of a communication available to a person other than the sender, recipient or intended recipient of that communication. This interception includes monitoring any such communication by means of a monitoring device; viewing, examining and inspecting the contents of any indirect communication; and diverting any indirect communication from its intended destination to any other destination. 'Monitoring' includes listening to or recording communications by means of a monitoring device.

In South Africa, a communication is considered to have been intercepted if the interception is effected by conduct within the country and it is intercepted in the course of its occurrence

in the case of a direct communication; and in the case of an indirect communication, in the course of its transmission by means of a postal service or telecommunication system, as the case may be (RICPCIA, section 1(2)(a)). Importantly, the time during which an indirect communication is being transmitted by means of a telecommunication system includes any time when the telecommunication system that transmits or has transmitted such an indirect communication is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it. The interception of any indirect communication broadcast or transmitted for general reception is not considered the interception of a communication (RICPCIA, section 1(3)).

The RICPCIA distinguishes between the real-time interception of a communication and the provision of real-time communication-related information. Section 16 of RICPCIA makes provision for the application for, and issuing of, an interception direction. Section 17 of the RICPCIA makes available an application for, and the issuing of, a real-time communication-related direction. Section 18 contains a combined application for, and the issuing of, an interception direction, real-time communication-related direction and archived communication-related direction or interception direction supplemented by a real-time communication-related direction. Section 15 of the RICPCIA also explicitly brings the production of real-time communication-related information within the scope of section 205 of the Criminal Procedure Act (provided that the information is not provided on an ongoing basis).

Interception directions are directed at data in transit and not at stored computer data. Real-time communication-related information is described in section 1 of the RICPCIA as information which is immediately available to a telecommunications service provider before, during or for a period of 90 days, after the transmission of an indirect communication. Technically such 'real-time' communication-related information could thus have been stored by the telecommunications service provider for a period of 90 days already. This definition of real-time communication-related information obscures the meaning given to stored computer data in the Cybercrime Convention to some extent.

Real-time communication-related information could become the object of both a production order under section 205 of the Criminal Procedure Act (but not on an ongoing basis) and a real-time communication-related direction under section 17 of the RICPCIA. The latter provision allows for the ongoing provision of real-time communication-related information. In urgent or exceptional circumstances, an oral real-time communication-related direction can be issued under section 23(7) of the RICPCIA. In circumstances where it is not advisable to order the required real-time communication-related information from the telecommunications service provider, such information could also be collected by means of a search and seizure intervention. This would be the case where the service provider is, for example, collaborating with the suspect.

Provision is also made in the RIPCIA for the production of archived communication-related information, targeted at stored computer data.

4.2 Search and Seizure

Search and seizure in accordance with the Cybercrime Convention is directed at any computer data, including all forms of communications data, provided that such data is static, recorded and stored. Search and seizure is concerned with data that has been recorded or registered in the past, either in tangible or in intangible form, and the gathering of this data takes place at a single moment in time, in other words, the period of the search, and in respect of data that exists at that time, as opposed to interception and monitoring (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.36 and the Council of Europe's Explanatory Memorandum to Recommendation 1995(13), p.11). Law enforcement officers are generally physically present during the course of a search and seizure and the intervention is generally non-secretive in nature.

To 'search' in terms of the Cybercrime Convention means to seek, read, inspect or review data and it therefore allows for both the searching for and the searching or examining of data (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.37). The term 'similarly access', as introduced by article 19(1) of the Cybercrime Convention, more accurately reflects computer terminology, is said to have a neutral meaning and would include actions such as the mirror imaging of data or the diversion of a copy of the data for scrutiny at another location (as opposed to search) (the Council of Europe's Explanatory Report to the Cybercrime Convention p.38). To 'seize' means to take away the physical medium in which data or information is recorded and includes the use or seizure of programmes needed to access the data being seized. To 'seize' also means to make and retain a copy or image of data or information. The term 'similarly secure' is included in article 19(3) of the Cybercrime Convention to reflect other means by which intangible data is removed, rendered inaccessible or otherwise taken control over in computing environments. In order to secure stored intangible data, additional measures of maintaining the integrity or the chain of custody of the data are required. In this context, 'secure' means taking control over or taking away data (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.38). Data, albeit copied or removed, must be retained in the state in which it was found at the time of the seizure and it must remain unchanged during the time that the criminal proceedings take.

To seize or similarly secure data therefore allows both for gathering evidence (for example, by copying the data) and for confiscating evidence (for example, by copying the data and subsequently rendering the original version of the data inaccessible or by removing it, without necessarily implying a final deletion of the seized data) (the Council of Europe's Explanatory Report to the Cybercrime Convention, p. 38).

The flexible approach of using both the traditional notions of either 'search and seizure', or the new and more technology-oriented notions of 'access and copying', is adopted in the Council of Europe's Explanatory Report to the Convention on Cybercrime. This inclusive approach to the quest for appropriate terminology seeks to underscore the modernisation and the harmonisation of domestic laws for the purposes of international cooperation. It reflects the evolution of concepts in the electronic environment, whilst also identifying and maintaining the traditional roots of these concepts (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.38).

In the South African legal framework, a 'search' is regarded as any act whereby a person, container or premises is visually or physically examined with the object of establishing whether an article is in, on or upon such a person, container or premises (Joubert, 1999, p.305). Although the search of premises for, and the seizure of, a computer itself can be authorised under the Criminal Procedure Act, the South African Law Reform Commission has submitted that the same does not apply to the search of a computer and the seizure of information located on that computer (South African Law Reform Commission 'Discussion Paper 99 on Computer-related Crime', 2001, p.14) [South African Law Reform Commission's Discussion Paper 99 on Computer-related Crime]. It is argued that words such as 'article' and 'premises' denote that the criminal procedural provisions are intended to be applied in respect of physical items.

To the extent that communication-related information under the RICPCIA is considered real-time for a period of 90 days after its transmission, such real-time communication-related information can be obtained by means of a real-time communication-related direction or a production order under section 205 of the Criminal Procedure Act. Following the expiration of a period of 90 days after the date of transmission, the communication-related information is considered to be archived communication-related information and, as such, can be obtained by means of a search and seizure intervention, an archived communication-related direction or a production order under section 205 of the Criminal Procedure Act.

The Constitutional Court held that the word 'seizure' is not a term of art and should be given its ordinary and natural meaning (*Rudolph v. Commissioner for Inland Revenue* 1996 (7) BCLR 889 (CC) 11). The compulsion to produce a document on pain of a criminal sanction must be considered as much a seizure as when a document is physically removed by another person (*Bernstein v. Bester NO* 1996 (4) BCLR 449 (CC) 89). A seizure takes place when a person is effectively deprived of control over an object which falls within her sphere of privacy (Steytler, 2004, p.84). A limited interpretation of the word 'seize' to encompass the act of seizure only would render the search and seizure powers under chapter 2 of the Criminal Procedure Act worthless. Seizure accordingly refers not only to the initial seizure, but also to the continued detention of the article after the seizure (Du Toit, et al., 2005, p.2-2B).

4.3 Production

Production is the submission or handing over of data or information under legal compulsion. Production orders under the Cybercrime Convention are aimed, firstly, at specified stored computer data in a specific person's possession or control and, secondly, at subscriber information relating to such services in a particular service provider's possession or control. Data or information sought by means of a production order is limited to the data maintained by the person or service provider to whom the production order is addressed (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.33). Real-time traffic data and real-time content data cannot be acquired by means of production orders under the Cybercrime Convention.

In the South African legislative framework, provision is made in section 205 of the Criminal Procedure Act for general criminal procedural production orders. This mechanism, under

section 15 of the RICPICA, can also be directed at communication-related information, but not on an ongoing basis.

Sections 17 and 19, read with sections 13 and 14, of the RICPCIA allow for the production of real-time and archived communication-related information respectively. In addition, section 23(7) of the RICPCIA provides for the oral application for, and issuing of an oral direction or entry warrant for purposes of the provision of, *inter alia*, real-time communication-related information. Section 23(7) is not applicable to archived communication-related information. Sections 39(3) and 40(3) of the RICPCIA allow for the provision of limited information so as to facilitate making applications under the RICPCIA.

4.4 Preservation

Data preservation is the activity that keeps existing, stored data secure and safe. In order to 'preserve' data, data which already exists in a stored form must be protected from anything that would cause its current quality or condition to change or deteriorate. It requires that data be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be frozen, rendering such data or copies thereof inaccessible to legitimate users (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.28).

In relation to computer usage, data preservation must be distinguished from data retention. Data retention is the process of storing data. To 'retain' data means to keep data which is currently being generated (real-time data) in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future period (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.28).

The importance of the distinction between preserved and retained computer data in the Cybercrime Convention is evident from the fact that articles 16 and 17 only refer to data preservation and not to data retention. These articles provide for the expedited preservation of stored computer data, and the expedited preservation and partial disclosure of traffic data, respectively.

In South Africa, preservation is currently accomplished by means of search and seizure and production orders. No specific provision is made in South African law for mechanisms aimed solely at the preservation of computer data. The closest mechanism to such a preservation mechanism would be the civil law Anton Pillar order.

Section 30(1) of RICPCIA provides for data retention in the South African legislative framework. It obliges South African telecommunications service providers not only to provide a telecommunications service in which communications can be intercepted, but which can also store communication-related information.

Reference is also made to data retention in section 16 of the Electronic Communications and Transactions Act, which provides that where a law requires information to be retained, such a requirement is met in respect of data messages if

a) the information contained in the data message is accessible so as to be usable for subsequent reference;

b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

c) the origin and destination of that data message and the date and time it was sent or received can be determined.

It is important to distinguish between the different electronic evidence collection legal mechanisms as these mechanisms provide the legislative mandates in terms of which one can access certain types of stored or real-time data. When one deploys technical cyberforensic tools to engage a particular set of data, one first needs to ensure that the interrogation of such data is lawful in that the evidence collection mechanism must speak to the type and state of the data. Although the Internet is often referred to as the Wild West, evidence collection mechanisms typically do not provide full access to all data (section 6 of the RICPCIA is an example of a very broad legal mandate but is appropriately delineated with specific requirements to override any reasonable expectation to privacy).

5. Cyberforensics: A Means to an End

When collecting electronic evidence from computing environments, the ultimate goal remains to obtain evidence that is admissible as evidence in a court of law, and to preserve its evidential weight optimally. In the Council of Europe's Explanatory Memorandum to Recommendation 1995(13) on Problems of Procedural Law connected with Information Technology, the powers to obtain evidence from dynamic objects (such as computer systems and networks) were explored in parallel to those powers with regard to concrete, tangible and material objects. It was found that computer data is a new form of evidence that requires special rules in respect of its collection, preservation and presentation. The rationale for such special powers included the following computational technicalities (the Council of Europe's Explanatory Memorandum to Recommendation 1995(13), pp.5-6):

i. The essential nature of electronic evidence (aggravated by the possibilities of remote access) poses special problems with regard to its reliability, in that it can easily be accurately copied, or erased or destroyed in another way. The volatile character of computer data necessitates exceptionally efficient collection interventions, as well as the power to control the whole system for a certain time, in order to retain unimpeachable continuity and integrity.

ii. Given the gigantic quantity of data which can be processed and stored, as well as the nature of the logical computer operations during processing and storage, it may be practically impossible to identify and to access the data needed as evidence in multi-user systems.

In addition to these technicalities, a number of other technicalities were highlighted in the South African Law Reform Commission's Discussion Paper 99 on Computer-related Crime (pp.14-16):

i. Computer data may be subjected to encryption and/or other software protection techniques, rendering it inaccessible for evidentiary purposes in the absence of the required technological converter(s).

ii. Electronic evidence may be inextricably commingled with collateral information that is legally privileged or necessary for the day-to-day functioning of the business or the network itself.

iii. The increasing interconnectedness of computing environments, even spanning multiple legal jurisdictions, requires exceptionally efficient mutual legal assistance mechanisms and causes unique jurisdictional and double jeopardy problems.

Collecting electronic evidence tends to be more complicated than collecting tangible evidence in traditional realms. Some of the idiosyncrasies of computing environments include the fact that computer files consist of electrical impulses that can be stored on the head of a pin and moved around the world in an instant. A single file could be located anywhere on the planet, or could be divided up into several locations in different districts or countries. It may furthermore be impossible to learn this prior to the actual execution of the collection intervention. Files may be stored on a floppy diskette, in a hidden directory on a laptop, or on a remote server located thousands of miles away. The files may be encrypted, misleadingly titled, stored in unusual file formats, or commingled with millions of unrelated, innocuous and even statutorily protected files (USA CCIPS, pp.30-40).

Computing technologies also frequently force the collection of evidence in non-traditional ways. Some of the features of the Internet, for example, that render non-conventional approaches non-negotiable include its global and borderless nature, its anonymity, its potential to reach vast audiences easily, its potential as a force multiplier and the wealth of probative information produced by the routine storage of information (United States Department of Justice, the President's Working Group 'The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet', 2000, p.14 <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>).

Like any other evidence, electronic evidence must be authentic, accurate, complete, convincing and admissible in conformity with the common law and legislative dictates. This form of evidence, however, poses special problems in that computer data changes moment by moment and is invisible to the human eye as it can only be viewed indirectly after appropriate procedures have been followed. The very process of collecting computer data may furthermore change it in significant ways. The processes of opening a file or printing it out are, for example, not always neutral (Vacca, 2005, p.19).

The collection of stored intangible data therefore requires additional measures of maintaining its integrity (the Council of Europe's Explanatory Report to the Cybercrime Convention, p.38). The data, which is copied or removed, must be retained in the state in which it was found at the time of its collection and it must remain unchanged during the time of legal proceedings. Adequate safeguards must be taken to guarantee the integrity of data in the period between its acquisition and its presentation at court proceedings (the Council of Europe's Explanatory Memorandum to Recommendation 1995(13), p.33). The safeguarding measures must include keeping track of all the measures that have been taken in handling the data or to prevent its unauthorised use. These measures of ensuring the reliability of electronic evidence, by default, have consequences for powers to collect electronic evidence or the ways those powers are executed.

Cyberforensics provides the contemporary and internationally accepted converter of choice by means of which to translate binary data into electronic evidence. The final objective of

cyberforensics is to collect and analyse electronic evidence in such a way that it enables the successful admission of this evidence into a court of law, whilst optimally preserving its evidential weight.

Electronic evidence is different from paper-based documentary evidence in a number of ways. Computer evidence is more fragile than paper documentation. A copy of a document stored in a computer file is identical to the original. Other valuable information, such as the time and date of origin and the author's name, may be embedded in the electronic version of a document. Comparisons of computer backups to existing documents can be used to show that a critical document has been altered and when the event occurred. In the case of email, casual and candid correspondence may be 'frozen in time, like insects in amber (Feldman, 2003, p.1). Electronic documents thought to be lost or destroyed can be recovered. Deleted file information has been analogised with a fossil, that may miss a bone here or there, but the fossil remains unchanged until it is completely overwritten. One of the challenges of what has been termed electronic 'dumpster diving 'is accordingly to recover information that has been partially destroyed and to make sense of the discovered 'digital trash' (Farmer and Venema, 2005, p.12).

Electronic evidence used to mean a regular print-out from a computer. Many computer exhibits in court are just that. However, for many years now, legal practitioners (and law enforcement officers, in particular) have been seizing and relying on the ever smaller and ubiquitous actual data media and computers. Then practitioners began to generate their own printouts, sometimes using the original application program, sometimes using specialist analytical and examination tools. Recently, practitioners have found ways of collecting evidence from remote computers to which they do not have immediate physical access, provided such computers are accessible via a phone line or network connection. It is even possible to track activities across a computer network, including the Internet. These processes of methodically examining computer media for evidence form part of what is called cyberforensics (Vacca, 2005, p.3).

In the early days of cyberforensics, before imaging was widely available, most recovered electronic evidence was in the form of copied files or raw sectors. When imaging became the norm, the use of copying decreased. Imaging is commonly acknowledged to be the better solution as it enhances the continuity and integrity of the electronic evidence that has been found. However, copying does have some advantages over imaging. Some of these advantages include the following: copies can be viewed immediately; copying can be used when convenient or expedient or to recover evidence from unusual machines or evidence which is not suitable for imaging; there are no special equipment or software requirements; it carries no additional costs; little training is required and it applies to files only (Sammes, and Jenkinson, 2000, p.195).

In the South African legislative framework, chapter III of the ECT Act deals with the facilitation of electronic transactions. Sections 11 to 20 deal specifically with the legal requirements for the admission of data messages as evidence in court proceedings. The efficacy of these provisions has yet to be tested in court, but they are generally considered a vast improvement of the former muddled state of affairs governing the admissibility and weight of electronic evidence (emanating from the products of modern technology). It is anticipated that the provisions will allow for a more equitable approach to electronic evidence in both civil and criminal proceedings than was possible before. South African courts struggled to classify satisfactorily the products of modern technology as real evidence, documentary evidence or a *sui generis* type of evidence. In *S v. Mpumlo* 1986 (3) SA 485 (E) and *S v. Baleka* (1) 1986 (4) SA 192 (T), for example, it was decided that video and audiotapes should be treated as real evidence. However, in *S v. Singh*

1975(1) SA 330 (N) and *S v Ramgobin* 1986 (4) SA 117 (N), it was decided that tapes should be treated as documentary evidence. The contentious Computer Evidence Act 1983 arose directly from the case of *Narlis v. South African Bank of Athens* 1976 (2) SA 573 (A) and was confined to civil cases. The Electronic Communications and Transactions Act repealed this piece of legislation and brought about much-needed legal certainty in respect of the admissibility of electronic evidence (Schwikkard, and Van Der Merwe, 2002, pp.79-387; Zeffert, Paizes, and Skeen, 2003, pp.699-712).

Section 15 of the ECT Act provides for the admissibility and evidential weight of data messages. It states that the rules of evidence in any legal proceedings must not be applied so as to deny the admissibility of a data message in evidence on the mere grounds that it is either constituted by a data message or not in its original form, if a data message is the best evidence that the person adducing it could reasonably be expected to obtain. It also states that information in the form of a data message must be given due evidential weight. Evidential weight must be assessed by considering 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 its originator was identified; and any other relevant factor (article 15(3) of the Electronic Communications and Transactions Act 2002). Article 15(4) of the same Act furthermore creates a rebuttable presumption that the facts contained in a business document are correct once a business document is certified to be correct. This provision contains the co-called 'shopbook exception' that was inherited from English law. Section 15(4) does not appear in the UNCITRAL Model Law on Electronic Commerce, on which section 15 of the Electronic Communications and Transactions Act was based (UNCITRAL 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 bis as adopted in 1998', 1996, <http://www.uncitral.org/pdf/english/text/electom/05-89450_Ebook.pdf>). It is argued that the ordinary South African law on the admissibility of evidence (including the rules applicable to hearsay) applies to data messages except where the Electronic Communications and Transactions Act changes it (see *S v. Ndiki* (2007) 2 All SA 185 (Ck), where part of the electronic evidence was admitted as real evidence and Van Der Merwe, 2008, pp.103-133, for a current and insightful discussion of the South African position).

Cyberforensics ensures the admissibility and optimal evidential weight of electronic evidence. The term 'cyberspace' was coined by William Gibson in his science fiction novel Neuromancer to describe the 'original consensual hallucination' (Gibson, 1984, p.10). The word 'forensic' stems from the Latin word 'forum', meaning court of law. The word 'forensic' is defined in the Oxford English Dictionary as an adjective meaning '… used in, or connected with a court of law' and the term forensic science as 'a science that deals with the relation and application of scientific facts to legal problems.' Traditionally, forensic science has centred on the physical and applied studies (such as medicine, engineering, chemistry and ballistics). However, more recently social sciences (such as psychology and accounting), have been added to the forensic science armoury. The extension of forensic science now called computer or cyberforensics is, in essence, concerned with the unearthing of evidence from computer media in order to support legal proceedings (including civil, criminal, administrative and disciplinary proceedings) (Carr and Williams, 1994, p.146).

Although the field is relatively new to the private sector, it has been the mainstay of technology-related investigations in law enforcement and military agencies since the mid-1980s (Vacca, 2005, p.795). Computer forensic methods may, however, not be afforded the luxury of time in which to establish themselves, or the longevity that more traditional chemistry- and physics-based

forensics enjoys, as newness and obsolescence is the norm in computing contexts (Vacca, 2005, p.237). So, for example, as lawyers have educated themselves about the DNA analysis procedure, so challenges to the production of DNA-based evidence have become more widespread and the courts' attention has been directed to the flaws and weaknesses in the process. Similarly, with digital evidence, as lawyers become more aware of the possibilities for improper modification outside the audit systems, more appropriate challenges can be mounted and the courts can assess these dangers (Plowden, and Stockdale, 1998, p.432).

The 'continued mystery surrounding the computer systems environment in general' is precisely what makes computer forensics particularly appealing to some people (Herold, 2002, p.150). However, it has also been said that in the face of the intimidating challenge of unravelling this mystery, it is not surprising that 'parents, federal investigators, prosecutors and judges often panic when confronted with something they believe is too complicated to understand' (Hafner, 1992, p.11). Unwittingly guided by the subconscious credo that any sufficiently advanced technology is almost 'indistinguishable from magic' many legal practitioners seem reluctant to embrace technology (Hafner, 1992, p.10).

In its demystified sense, it is accordingly ironic that cyberforensics is, first and foremost, concerned with forensic procedures, rules of evidence and legal concepts, precedents and processes. Only in the second place, is it concerned with computers. Cyberforensics involves the preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis. It entails the process of extracting data from computer storage media and guaranteeing its accuracy and reliability. In contrast to all other areas of computing, where speed is the main concern, in forensics the absolute priority is therefore accuracy (Vacca, 2005, pp.6 and 795; Davis, Phillip and Cowen, 2005, p.6).

The cyberforensic methodology must ultimately be capable of standing up to legal scrutiny. The basic cyberforensic methodology consists of what has been described as the 'AAA of Computer Forensics', i.e. acquire the evidence without altering or damaging the original; authenticate that the recovered evidence is the same as the originally seized data; and analyse the data without modifying it (Kruse, and Heiser, 2002, pp.1 and 3). It must be shown that the evidence presented in court is exactly the same as the evidence that existed at the time that the evidence was collected. This is mainly achieved by means of different cryptographic hashing functions. These algorithms act like fingerprints or electronic tamper seals, allowing you to show mathematically that the evidence is the same today as on the day that it has been collected.

A more comprehensive methodology is the one designed by Andrew Rosen (the CEO of ASR Data), called the 'Six A's of Computer Forensics'. This process has been tested in both legal and technical aspects and is flexible enough to handle the diverse requirements posed by the investigation. The steps in the process entail the assessment, acquisition, authentication, analysis, articulation and archival of electronic evidence (Davis, Phillip and Cowen, 2005, p.13).

The objective in cyberforensics is quite straightforwardly to recover, analyse and present computer-based material in such a way that it is usable as evidence in a court of law. It is essential that none of the equipment or procedures used during the examination of the computer obviate this objective. Like any other forensic science, cyberforensics involves the use of sophisticated technology tools and procedures, which must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of processing results (Vacca, 2005, pp.6 and 295). These tools and procedures are briefly considered below.

Although certain hardware tools are used with important measure in the cyberforensic methodology, cyberforensic tools typically exist in the form of computer software. Cyberforensic specialists guarantee accuracy of evidence-processing results through the use of multiple forensic tools, developed by separate and independent developers. It is critical that the expert understands the tool and its fundamentals so as to verify the results herself. The use of different tools that have been developed independently to validate results is important to avoid inaccuracies introduced by potential software design flaws and software bugs. Cross-validations through the use of multiple tools and techniques are standard in all forensic sciences. Validation through the use of multiple software tools, computer specialists and procedures eliminates the potential for errors and the destruction of evidence. When this approach is not deployed, it creates advantages for opposing counsel who may challenge the accuracy of the software tool used and thus the integrity of the results (Vacca, 2005, p.795).

Examples of forensic toolkits include ASR Data <http://www.asrdata.com/SMART>, Paraben <http://www.paraben-forensics.com>, Access Data <http://www.accessdata.com>, The Sleuth Kit (<http://www.sleuthkit.org>), and New Technology Incorporated (NTI). The EnCase Forensic Edition, developed by Guidance Software <http://www.guidancesoftware.com>, contains a large suite of tools based on the requirements of law enforcement, government and corporations, spanning seven years. One of the strongest features of EnCase is its repeated industry and court validation and deep analysis capabilities. The EnCase Enterprise Edition greatly extends the capabilities of the EnCase Forensic Edition technology. Its secure network-enabled capability gives corporate and government investigators the ability to respond immediately and centrally to security breaches and to conduct proactive and reactive investigations. One of the key features of the EnCase Enterprise Edition is its ability to investigate a machine thoroughly without having to bring it offline, potentially disrupting business. The EnCase Enterprise Edition also has a feature called Snapshot, which quickly captures volatile data.

Cyberforensics is one of the most adversarial occupations in information technology. Every aspect of the technical competency and methods of the cyberforensic specialist will be scrutinised to its very core. As such, it is imperative to use a deterministic, repeatable process that is clear, concise and simple. Adherence to this process is the forensic examiner's greatest asset and will become her lifeline in court. A defined, proven process incorporates the following elements: cross-validation of findings with multiple toolsets; proper evidence handling and the safeguarding of the evidential chain of custody, completeness of the investigation so that no single piece of relevant evidence remains undetected; management of archives; technical competency; explicit definition and justification for the process; conducting the investigation in a manner that allows a forensic specialist to retrace every step in the process; legal compliance and flexibility. These elements are the difference between an effective, expedient investigation and playing around with a neat piece of software (Kruse, and Heiser, 2002, p.315; Davis, Phillip and Cowen, 2005, p.10; Earnshaw, 2003, pp.11-13; Harris, 2002, p.674).

An important feature of computer forensics is that it has changed the legal best evidence rule in respect of the processing of e-evidence (Vacca, 2005, p.795). The best evidence rule has in recent years seen the growth of a standard known as representational accuracy, which means that it is unnecessary to present the originals. If data stored by on a computer or similar device, any printout or other output readable by sight is shown to reflect the data accurately, it is considered an original (Vacca, 2005, p.237). The concept of representational accuracy allows investigators to gather forensic duplicates,[2] qualified forensic duplicates,[3] mirror images[4] and, to some extent, logical copies of the computer and data storage systems involved. A logical copy is used to refer

to the act of copying discrete files from the logical file system onto media during the collection process (Prosise, and Mandia, 2003, p.152). If at all possible, it is prudent to safeguard the original evidence media as they constitute the ultimate control samples of the forensic process.

6. Anti-Forensics: Another One Bytes the Rust[5]

Anti-forensic techniques refer to the intentional or accidental changing of data that can obscure the data, encrypt it or hide it from forensic tools (Davis, Phillip and Cowen, 2005, p.168). Two of the most prevalent anti-forensic techniques are obscurity methods (such as file extension renaming, encoding, compression obscurity methods, data stored in slack, unallocated, and free space) and privacy measures (encryption, steganography, evidence eliminators and disk-wiping).

An anti-forensic technique is any intentional or accidental changing of data that can obscure the data, encrypt it or hide it from forensic tools. As most contemporary forensic examination tools tend not to trust data, the concepts discussed below do not necessarily affect the efficiency of modern forensic tools. However, it is necessary to be familiar with these concepts, as they may become relevant during the course of legal proceedings. Two of the most prevalent anti-forensic techniques, namely obscurity methods and privacy measures, are explored below.

6.1 Obscurity Methods

An obscurity method is a method by which the true nature or meaning of some data is obscured. Data is typically obscured when the name or contents of a file is changed either intentionally or accidentally, resulting in a file that could be misinterpreted or disregarded in subsequent forensic analysis. File extension renaming can be countered by file signaturing in that some unique aspect of the file is compared to a database of signatures that relate to an extension. Several forensic tools can be used to determine a file's signature. EnCase, for example, has the ability to detect file types and carry out file signature analysis to detect modified file types (Davis, Phillip and Cowen, 2005, p.169).

Encoding is an obscurity method that changes a file's content in some way that can be easily reversed. A simple encoding mechanism is ROT-13, which rotates the characters 13 times. Such encoding can be detected by using ROT-13 decoders (Davis, Phillip and Cowen, 2005, p.172).

Compression obscurity methods allow a file's contents to be reduced in size for storage and transmission. Although it is not difficult to detect compressed files, most forensic tools do not allow direct access to compressed data during a search. FTK and EnCase both allow for searching data without virtually uncompressing the data. SMART and other systems require such files to be exported out of the image, decompressed and then searched using separate tools (Davis, Phillip and Cowen, 2005, p.173).

Data stored in slack space, unallocated space and free space may not be detected if an attempt is made to search a disk using non-forensic utilities. Operating systems arrange all data stored on a hard drive into segments called allocation units or clusters. Unallocated space is the area of the hard drive not currently allocated to a file. Fragments of deleted files are often strewn across unallocated space on a hard drive (Kruse, and Heiser, 2002, p.75). Free space is the portion of the hard drive media that is not within any currently active partitions (Prosise, and Mandia, 2003, p.275). Slack space is a remnant of data that exists within a sector of data that has been

overwritten. Specifically, slack space is the area of the sector that was not fully overwritten by a recent write to disk (Davis, Phillip and Cowen, 2005, p.800).

6.2 Privacy Measures

Some of the recognised anti-forensic techniques, such as encryption, steganography, evidence eliminators and disk wiping, are legitimate attempts to protect the privacy of the individual. It is, however, necessary to be able to identify and access such protected data during the course of a forensic examination.

Wiping is a real problem when it is done correctly, as any data that has been truly wiped from the disk has been overwritten at least once. Current software tools do not provide access to any data that has been overwritten. However, the data can be recovered by using an electron microscope to find the previous state of all the electrons on the disk, thus restoring the wiped information. This is an expensive and labour-intensive process; and very few forensic examiners have access to an electron microscope for analysis purposes. It is possible to determine whether wiping tools have been installed by reviewing the programs that exist and have existed on the disk. If the disk was received during the course of an investigation, legal sanctions may be filed against the person responsible for the wiping or the person may be ordered to produce any other data that may exist. Whether or not a preservation order exists in respect of such data, an opposing party is likely to be ordered to produce further evidence if it can be proved that some of the data that was provided was wiped (Davis, Phillip and Cowen, 2005, pp.181-184).

Other than wiping, encryption is the only true anti-forensic method that can defeat the forensic analysis of data. Cryptography is the art of secret writing and comprises a science of codes and ciphers that can be used to conceal the contents of a message. It transforms messages into unintelligible forms in order to hide its content, establish its authenticity and prevent undetected modification. Cryptography largely falls into two camps, namely symmetric or secret key cryptography and asymmetric or public key cryptography. The main difference between the two types of cryptography is that symmetric or secret key cryptography uses the same single key to both encrypt and decrypt, whilst asymmetric or public key cryptography uses one key to encrypt and another one to decrypt (Bharvada, 2002, pp.268.). Symmetric key encryption is only as strong as its key length and its ability to keep others from finding the key itself. Asymmetric key encryption is stronger than symmetric encryption, because not only does the length of the key protect it, but the private key that is used to decrypt the data must be found before the data can be accessed. Having the public key used to encrypt the data will not allow access to the original data. If data is encrypted, it is not possible to analyse or search its contents directly. Another method of identifying and accessing the data must then be found. Encrypted data is identified in two ways: either the file has an extension that is used by an encryption program to identify its files or it can be detected by means of a process known as entropy testing (Davis, Phillip and Cowen, 2005, pp.176-179).[6]

However, even encryption has its weaknesses, depending on the type used (Russell, 2004, p.7). For data to be encrypted, it must first exist on the disk in its unencrypted form. Although it is possible for someone to download a document in memory and encrypt it in memory before the data even touches the disk, this is very rare, except in the case of email. Instead, most people choose to encrypt a file that already exists on a disk. This means the data could still be stored at three locations: in the original file on the disk if it is still present, in the contents of the deleted file in the unallocated and slack space, or in the original file in the swap or pagefile. If data cannot be

accessed in this way, the suspect may be asked to supply the encryption key and the method by which she encrypted the data. Although this sounds simplistic and too good to be true, it often works. Alternatively, a court of law may order the production of the encryption key and the method used to encrypt the data (Davis, Phillip and Cowen, 2005, pp.175-180).

Steganography is the technique of hiding information in other data such as visual images, voice communication and music. The word is derived from the Greek word meaning 'covered writing ' and it refers to the science of hiding information inside something innocuous so that no-one suspects it is there in the first place. Secret messages written in invisible ink, micro dots and radio signals that resemble noisy static are examples of steganography used in the past. Using the steganography tools available today, suspects can even hide data inside an image and audio files. When a sophisticated suspect is being investigated and remnants of a steganography tool exist, it would be bad practice not to attempt to discover the existence of any hidden data.

Like all cryptographic techniques, steganography is fallible. Sophisticated programs are available to crack the algorithms. Criminals may prefer the use of steganography because of the fact that encrypting data is visible to prying eyes, while the use of steganography is invisible to authorities who may not even know that there is anything that needs decrypting. Steganography has yet to achieve the versatility of public key cryptography. The main areas where it is increasingly being used are where cryptography and strong encryption are outlawed (Bharvada, 2002, pp.268-269).

7. Conclusion

It is advocated that legal practitioners should turn their minds to overcoming the profession's perceived technophobia by embracing technology themselves. The bottom-line is this: Ignorance in cyberspace is not bliss and perhaps legal practitioners need to be advised to emerge from the prevailing ostrich politics and get their clients' rear ends out of harm.

As legal practitioners, one of the myriad ways in which we could do so is by distinguishing between different types of computer data as different legal collection regimes dictate the collection of each type of data. The applicability of an evidence collection mechanism (such as an interception and monitoring direction; a search and seizure, production or preservation order) to a particular type or form of data depends on the nature and form of the data that is to be collected. While the end result remains the acquisition of data, the preconditions for using, the accompanying safeguards and the scope of these coercive powers differ – the rationale behind this being foremost the protection of the right to privacy.

In addition, we have a collective duty to fast-track South Africa through the different stages of its legal response to technological developments (Lloyd, 2004, pp.xlv-xlvi):

> In respect of many technological developments the legal response can be divided into four stages. Step one could be taken from a Dickensian novel as elderly judges raise their eyes from the parchments littering the bench and, quill pen in quivering hand demand of counsel 'a **computer**, pray tell, what is that? Is it used by the Beatles?' Following denial comes a stage of grudging acceptance of the technology's existence but assertion that the application of general principles will suffice to resolve any disputes. … This stage may last for a number of years. … The attempt to

> remedy the situation brings us on to the third of our stages, where specific statutory provision is made for aspects of the new technology. … Most legal systems are currently hovering between the second and third stages described above. However, whilst computer specific statutes have a valuable role to play in filling *lacunae* in existing legal provisions, making exceptional provision for the regulation of technology whose application is becoming the norm is often an unsatisfactory approach. The final stage differs perhaps only in degree, but sees recognition of the implications of the technology at the very core of the law.

Despite the global digital divide, the African continent in general, and South Africa in particular, could take their places with pride among the nations of the Information Age. After all, Africa carries much less baggage from the Second Wave of industrialism than some other continents (Van Der Merwe, 2003, p.44).

References

Books and Periodicals

Bharvada, K (2002), 'Electronic Signatures, Biometrics and PKI in the UK', International Review of Law, Computers & Technology 265.

Carr and Williams (1994), Computers and Law (eds.) (New York: Intellect Books).

Casey, E (2002), Handbook of Computer Crime Investigation (ed.) (London: Academic Press).

Davis, C, Philipp A and Cowen D (2005), Hacking Exposed Computer Forensics Secrets & Solutions (California: McGraw-Hill/Osborne).

Earnshaw, C (2003), 'Search and Seize orders – The Role and Responsibility of the Forensic Computing Specialist', C & L Computer Forensics 11.

Farmer, D and Venema, W (2005), Forensic Discovery (Upper Saddle River: Pearson Education Inc).

FBI/CART (1997), Conducting Searches in a Computer Environment (Rev 2/21/97) (Washington: FBI/CART)

Gibson, W (1984), Neuromancer (Washington: Phantasia Press).

Grant, I (1995), 'Court and Spark', Intelligence Publication 40.

Hafner, K (1992), Cyberpunk (New York: Simon & Schuster).

Herold, R (2002), The Privacy Papers: Managing Technology, Consumer, Employee and Legislative Actions (ed.) (London: Auerbach Publications).

Joubert, CJ (1999), Applied Law for Police Officials First Edition (ed.) (Florida: Technikon SA Florida).

Kruse, II WG, and Heiser, JG (2002), Computer Forensics Incident Response Essentials (Mexico City: Addison-Wesley).

Lloyd, IJ (2004), Information Technology Law (USA: Oxford University Press).

Moore, RE (2003), Search and Seizure of Digital Evidence: An Examination of

Constitutional and Procedural Issues (University of Southern Mississippi: PhD Thesis).

Plowden, P and Stockdale, M (1998), 'A picture is worth a thousand words', 432.

Prosise, C and Mandia, K (2003), Incident Response & Computer Forensics (2 Ed.) (California: McGraw-Hill / Osborne).

Rittinghouse, JW and Hancock, WM (2003), Cybersecurity Operations Handbook (Burlington: Elsevier Digital Press).

Russell, R (2004), Stealing the Network How to Own a Continent (ed.) (Rockland: Syngress Publishing Inc)

Sammes, T and Jenkinson, B (2000), Forensic Computing A Practitioner's Guide (London: Springer).

Schwikkard, PJ and Van Der Merwe, S (2002), Principles of Evidence Second Edition (Lansdowne: Juta)

Sharpe, S (2000), Search and Surveillance: The Movement from Evidence to Information (Aldershot: Dartmouth Publishing Company Limited).

Shelly, GB, Cashman, TJ and Vermaat, ME (2002), Discovering Computers 2003 (Boston: Thomson Course Technology).

South African Law Reform Commission, (2001), Discussion Paper 99 on Computer-related Crime: Preliminary Proposals for Reform in respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects (Project 108) (Pretoria)

Steytler, N (2004), Constitutional Criminal Procedure A Commentary on the Constitution of the Republic of South Africa (Durban: Butterworths).

Vacca, JR (2005), Computer Forensics Computer Crime Scene Investigation Second Edition (Massachusetts: Charles River Media Inc)

Van der Merwe, DP (2003), 'Computer Crime', THRHR 30.

Van Der Merwe, D (2008), Information and Communications Technology Law (Durban: LexisNexis)

Volonino, L (2003), 'Electronic Evidence and Computer Forensics', Communications of the Association for Information Systems 1.

Whitcomb, CM (2002), 'A Historical Perspective of Digital Evidence: A Forensic Scientist's view', International Journal of Digital Evidence 1.

Zeffert, DT, Paizes, AP and Skeen, A St Q (2003), The South African Law of Evidence (Durban: LexisNexis Butterworths).

Case Law

Bernstein v. Bester NO 1996 (4) BCLR 449 (CC)
Narlis v. South African Bank of Athens 1976 (2) SA 573 (A)
Rudolph v. Commissioner for Inland Revenue 1996 (7) BCLR 889 (CC) 11
S v. Baleka (1) 1986 (4) SA 192 (T)
S v. Ndiki (2007) 2 All SA 185 (Ck)
S v. Mpumlo 1986 (3) SA 485 (E)
S v. Ramgobin 1986 (4) SA 117 (N)

Statutes and International Documents

Computer Evidence Act 57 of 1983

Constitution of the Republic of South Africa 108 of 1996

Electronic Communications Act of 2000

Electronic Communications and Transactions Act 25 of 2002

Interception and Monitoring Prohibition Act 127 of 1992

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICPCIA)

Telecommunications Act 103 of 1996

Internet

CCIPS (2001) 'Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001' <http://www.cybercrime.gov/searchmanual.htm>.

Council of Europe (1995) 'Explanatory Memorandum to Recommendation 1995(13) on Problems of Criminal Procedural Law connected with Information Technology' <http://cm.coe.int/stat/E/Public/1995/ExpRep(95)13.htm>.

Council of Europe (1995) 'Recommendation No R(95)13 of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law connected with Information Technology' <http://cm.coe.int/ta/rec/1995/95r13.htm>.

Council of Europe (2001) 'Cybercrime Convention Budapest 23.XI.2001' <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

Council of Europe (2001) 'Explanatory Report to the Convention on Cybercrime (ETS No 185) <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Feldman (2003) 'The essentials of Computer Discovery' <http://www.forensics.com/pdf/Essentials_of_Discovery.pdf>.

Google (2004) 'Definitions of Digital on the Web' <http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=define%3Adigital>.

<http://www.accessdata.com>

<http://www.asrdata.com/SMART>

<http://www.guidancesoftware.com>

<http://www.paraben-forensics.com>

<http://www.sleuthkit.org>

Mobrien.com (2006) 'Computer Crime' <http://www.mobrien.com/computer_crime4.htm> 1.

UNCITRAL 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 bis as adopted in 1998' <http://www.uncitral.org/pdf/english/text/electom/05-89450_Ebook.pdf>.

United States Department of Justice, the President's Working Group (2000) 'The Electronic

Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet' <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>.

USA CCIPS (2002) 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' <http://www.cybercrime.gov/s&smanual2002.htm>.

Whatis.com searchStorage.com Definitions (2001) 'Data' <http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci211894,00.html>.

Endnotes

[1] This article draws from research conducted by the author in fulfilment of the requirements for the degree of *Legum Doctor* at the North-West University, South Africa and for purposes of an article which appeared in the Association of Insolvency Practitioners of Southern Africa (AIPSA) News of November 2006. Readers are referred to these sources for the full acknowledgement of resources.

[2] A forensic duplicate is a file that contains every bit of information from the source, in a raw bitstream format. A 5 GB hard drive would result in a 5 GB forensic duplicate. Tools used to create a forensic duplicate are the Unix dd command and the open source Open Data Duplicator (Davis, Phillip and Cowen, 2005, p.153).

[3] A qualified forensic duplicate is a file that contains every bit of information from the source, but may be stored in an altered form, such as in in-band hashes and empty sector compression. Tools that create qualified forensic duplicate output files are SafeBack and EnCase (Davis, Phillip and Cowen, 2005, p.153).

[4] A mirror image is created from hardware that does a bit-for-bit copy from one hard drive to another. Hardware solutions are very fast. Mirror imaging introduces an extra step in the forensic process, requiring the examiner to create a working copy in a forensically sound manner. Mirror image backups replicate all the sectors on a given storage device exactly. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as 'evidence grade backups' and they differ substantially from standard file backups and network server backups. If it is possible to keep the original drive seized from the computer system that is being investigated, working copies can be easily made. If the original drive must be returned or may never be taken offsite, the analyst is still required to create a working copy of the mirror image for analysis. Examples of hardware duplicators are Logicube's Forensic SF-5000 and Intelligent Computer Solutions' Image MASSter Solo-2 Professional Plus ((Davis, Phillip and Cowen, 2005, p.154 and Vacca, 2005, p.808).

[5] Most computers use magnetic media for their permanent storage, the common denominator of which is that these media are all coated with a metallic oxide. This ferric (iron) oxide, which is the basic component of the coating of these magnetic media, and which is usually used in conjunction with cobalt or barium, is commonly called 'rust' (FBI/CART 'Conducting Searches in a Computer Environment', 1997, p.2).

[6] Entropy testing is a process by which the randomness of the distribution of data within a file can be tested. The specific randomness can then be compared against a table of known algorithm randomness to identify whether a known algorithm has been used. This works well for all publicly known and encryption algorithms, because the law enforcement officer can use them to document their randomness scale. However, if the suspect is using a new or non-public program, an entropy test is not able to identify the type of encryption used.