AN INVESTIGATION INTO THE UTILISATION OF SOCIAL MEDIA BY THE SAPS IN RESOLVING CRIME

By

LIZELLE TURCK

submitted in accordance with the requirements
for the degree of

MAGISTER TECHNOLOGIAE
in the subject

POLICING

at the

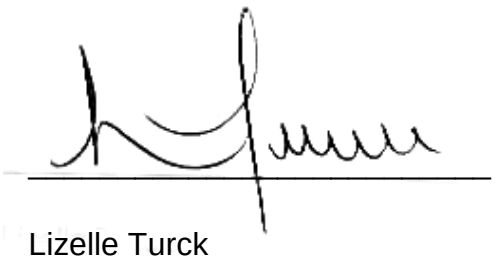
University of South Africa

SUPERVISOR: PROF M. MONTESH

2016

DECLARATION

I, Lizelle Turck, student number 36789941, hereby declare that this dissertation, entitled “An investigation into the utilisation of social media by the SAPS in resolving crime”, is my own work, and that all the consulted sources have been indicated and acknowledged by means of complete references. I further declare that ethical clearance to conduct the research was obtained from the South African Police Service (SAPS) and the University of South Africa (UNISA).



Lizelle Turck

2016-06-24

Date

ACKNOWLEDGEMENTS

It would not have been possible to complete this study without the assistance of: Warren, Chris, Cecilia, Kobus, Nelly, Jaco and my supervisor, Prof M. Montesh. It is also important for me to thank Dr N.J.C. Olivier, for his willingness to assist me in rectifying the recommendations by the examiners, and my mom for her prayers and support.

DEDICATION

This study is dedicated to all the police members who put their lives at risk daily to ensure a safer environment for all of us.

ABSTRACT

This study investigates the SAPS utilisation of social media in its fight against crime, and the extent to which the SAPS is already using it. The findings suggest that the SAPS is utilising social media in the fight against crime, mostly at a specialised level. Detectives at station level lack adequate knowledge and skills to use social media to their advantage. A lack of adequate resources and training is also identified.

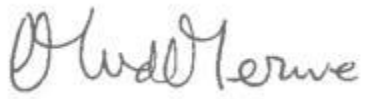
Social media is a communication platform for millions of people, and should therefore be used in the SAPS, to its advantage, to solve crime. Guidelines are in place for law enforcement officials who need to use it in their investigations.

Recommendations resulting from the study include benchmarking with international law enforcement agencies, and finalisation of relevant policies. Training material should be developed and presented to detectives and members at station level. Resources should be made available to members to use in their investigations.

Keywords: social media, investigation of crime, Internet, training, legislation, detectives, South African Police Service, Facebook, YouTube, Twitter.

CONFIRMATION OF LANGUAGE EDITING

I, Marlette van der Merwe, ID 4802060118085, hereby certify that the text and list of references of the master's dissertation, "An investigation into the utilisation of social media by the SAPS in resolving crime", By Lizelle Turck, have been edited by me, according to the Harvard reference method (2011 edition) as used by the School of Criminal Justice, Unisa.



Marlette van der Merwe

BA, HDipLib (UCT)

TABLE OF CONTENTS PAGE

LIST OF TABLES, IMAGES AND ILLUSTRATIONS

LIST OF TABLES

LIST OF IMAGES

LIST OF ILLUSTRATIONS

ACRONYMS AND ABBREVIATIONS

AU	-	African Union
BBM	-	BlackBerry Messenger
CAA	-	Copyright Amendment Act
CCMA	-	The Commission for Conciliation, Mediation and Arbitration
CCTV	-	Close Circuit Television
CPA	-	Criminal Procedure Act
DoS	-	Denial of Service Attacks
DPCI	-	Directorate of Priority Crime investigation
ECA	-	Electronic Communications Act
ECPA	-	Electronic Communications Privacy Act
ECTA	-	Electronic Communications and Transactions Act
ECU	-	Electronic Crimes Unit
ESI	-	Electronically Stored Information
GPS	-	Global Positioning System
IACP	-	The International Association of Chiefs of Police
ICASA	-	Independent Communications Authority of South Africa Act
ICCMA	-	International Cooperation in Criminal Matters Act
IM	-	Instant Messaging
IMEI	-	The International Mobile station Equipment Identity number
IMSI	-	International Mobile Subscriber Identity
iOS	-	Originally iPhone OS
IP	-	Internet Protocol
IPID	-	The Independent Police Investigative Directorate
ISP	-	Internet Service Provider
ISS	-	Institute for Security Studies
IT	-	Information Technology
IWF	-	Internet Watch Foundation
KINSA	-	Kids' Internet Safety Alliance
LEA	-	Law Enforcement Agency
MLAT	-	Mutual Legal Assistance Treaty
MMS	-	Multimedia Messaging Service

NCB	-	National Central Bureau
NDPP	-	National Director of Public Prosecutions
NFC	-	Near Field Communication
NYPD	-	New York Police Department
PAIA	-	Promotion of Access to Information Act
PDA	-	Personal Digital Assistant
PERF	-	Police Executive Research Forum
PPA	-	Privacy Protection Act
PPI	-	Protection of Personal Information Bill
P2P	-	Peer-to-peer
RFID	-	Radio-frequency Identification
RICA	-	Interception of Communications and Provision of Communication Related Information Act
RIPA	-	Regulations of Investigatory Powers Act 2000 (United Kingdom)
SADC	-	Southern African Development Community
SADEC	-	South African Development Economic Community
SAPS	-	South African Police Service
SARPCCO	-	Southern Africa Regional Police Chiefs Cooperation Organisation
SCA	-	Stored Communications Act (US Legislation)
SMILE	-	Social Media the Internet and Law Enforcement
SMS	-	Short Messages System
SNS	-	Social Network Service
SOCA	-	Serious Organised Crime Agency
SOP	-	Standard operating procedures
URL	-	Uniform Resource Locator
US	-	United States (of America)
US LEA	-	United States Law Enforcement Agency
WWW	-	World Wide Web

CHAPTER 1
GENERAL ORIENTATION

1.1. INTRODUCTION

Many people grew up without the Internet and the excitement of social media. Facebook, YouTube, Twitter, BlackBerry Messenger (BBM), WhatsApp, MixIt and others opened up a whole new world of communication for millions of people. Social media has its own advantages and disadvantages. It brings many people into contact with one another via networks, and enable them to search for old friends, but it also enables criminals to use it to their advantage, to commit crimes. People need to be informed about social media, and know where the dangerous potholes are on the cyber highway. Social media does not only have social users and users with criminal intent. Law enforcement can also use it to fight crime. The South African Police Service (SAPS) fights crime on a full-time basis, and should use all the available resources.

The SAPS has an official website on the Internet. In 2003, it was still a new concept, and Sonderling (2003:28) found that the SAPS website could be used as a tool to promote service delivery. Consultation and interaction between the SAPS and its clients are important pillars for successful service delivery, and utilising an SAPS web page is in line with international practice to involve the community in policing. This results in community and partnership policing. It is important for the SAPS website to adhere to specific requirements, in order to reach optimal service delivery. The development of a strategy pertaining to the development and maintenance of the website, was also a key factor for its success.

The same could be said for the usage of social media by the SAPS. Social media can be used to promote service delivery, in the sense that it could be utilised by the SAPS as a tool to solve crime. Currently, in 2015, it is still a new concept, and using it means following an international trend by implementing it in policing.

Melekian and Wexler (2013) state that police departments all over the world are developing new technology that could assist the police in rendering more effective and efficient services. They add that social media could be counted on as one of the new and important technologies.

The SAPS, or any police service for that matter, simply cannot operate optimally without the assistance of the public. This point is supported by Braga, Flynn, Kelling and Cole (2011:5), who state that many crimes are solved with the assistance of the public, when they identify suspects. Normally, detectives do not first obtain facts and then identify suspects – they first identify suspects and then find the facts leading to arrests, prosecution and conviction. However, the opposite is also true. According to Captain C. J. van der Berg (2015) – trainer at SAPS Academy, Paarl, and Captain C. E. van Dyk (2015) – trainer, and working at the Monitoring and Evaluation section at SAPS Academy, Paarl, detectives in the SAPS use the following identification categories in the investigation of crime – as prescribed by Van Heerden (1991):

- Situation identification
- Witness identification
- Victim identification
- Culprit identification
- Imprint identification
- Origin identification
- Action identification
- Cumulative identification

Many crimes are also solved with information provided by criminals. Millions of people, globally, participate on social media. Why not tap into that source of information? Why not use it to the police's advantage?

It is important for a police official to know and understand the Internet, and know and understand social media – and who is using it. Police officials cannot do their

work properly, without having proper training and knowledge. Training must not only focus on, but must include, applicable legislation and digital forensics. Digital forensics encompasses the identification, collection, preservation, documentation, examination, analysis and presentation of evidence from computers, computer networks, and other electronic devices. Computer/digital evidence is fragile, and the handling of this evidence differs from traditional tangible evidence. Special training and skills are required, as stated by Dempsey and Frost (2012:467-469). Chapters 4 and 5 of this dissertation deal with applicable legislation. Chapter 5, section 5.8, of this dissertation deals with digital/electronic evidence.

Future research in this field will be a good foundation from which to start a process to provide guidelines to people who can use social media as a tool to solve crime. The main focus of this study is to investigate the utilisation of social media in the investigation and solving of crime, by the SAPS.

1.2. BACKGROUND

Social media is becoming more popular by the day, and people are increasingly joining the different networks. Facebook had reached its 100 million mark in Africa by September 2014 (Fin24, 2014). Communication is taking place not only on paper and through fixed telephone lines, but also through electronic networks and with cell phone technology. People are sharing information from moment to moment.

The researcher decided on this specific topic because of the value it could add, should members of the SAPS use it as a tool to solve crime. Cohen (2010) states that Lauri Stevens, founder of LAwS Communications, said, at a Social Media in Law Enforcement Conference in April 2010, that social media was still in its "*very, very, early stages*". Many police departments have started using social media; however, keeping content updated remains a challenge. Limitations such as security of information, are still a concern.

The Police Executive Research Forum (PERF) (About PERF, 2014), founded in 1976, does research independently, and focuses on critical issues in policing. It strives to improve professionalism and service delivery in the police through the following actions:

- the exercise of strong national leadership;
- public debate on police and criminal justice issue; and
- research and policy development.

A report was issued by PERF (Wexler, 2014) about the role of local law enforcement agencies in preventing and investigating cybercrime. Principal Deputy Director Josh Ederheimer (Wexler, 2014) stated that the effectiveness of an agency depends on the trust that the community has in it. He said that trust is lost when a complainant only gets a blank stare from a police official after, for example, he explains that his stolen iPhone has an application on it to locate the device. Ederheimer further stated that specialised units have their place, but it starts with the patrol officer who attends to the first call. The police official 'on the ground' must be able to collect the correct information and ask the right questions.

According to Wexler (2014), San Diego (California) Acting Assistant Chief Lori Luhnow agreed that they had positive results when including patrol officers in the training of cybercrime and/or digital forensics. They were then equipped with the correct tools to start investigations. This statement was supported by Director William O'Toole, who stated that it was necessary for all officers to have a basic understanding of, and basic skills in, the investigation of cybercrime. They should be able to identify electronic evidence, and preserve it as far as possible for the specialist investigators to take over. He added that they needed patrol officers to use the same observation skills, awareness and proper documentation procedures also, when attending to cybercrime complaints (Wexler, 2014).

The researcher agrees with the abovementioned authors, and is of the opinion that training should start at ground level, and that it is not only members in specialised units who should be trained in detecting cybercrime.

The researcher is working at the Information Management Centre at the SAPS Academy in Paarl, Western Cape. There is no social media training material for detectives at station level, and no information on its usage as an aid in solving crime. Discussions with detectives at station level also made it clear that they had no official guidelines on how to access a suspect's profile on, for example, Facebook. However, the SAPS recognises the fact that the usage of social media is part of modern police work. Pictures of missing or wanted persons are circulated, and the public is requested to report crime, criminals and/or criminal activities, by calling Crime Stop 08600 1011 or sending an sms (Short Messages System) to Primedia Crime Line SA 32211, anonymously. Members of the public can post tips on www.crimeline.co.za and www.saps.gov.za.

According to Ebersöhn (2013), it was mentioned, at the 20th Anniversary SAPS Crime Stop and 5th Anniversary Crime Line, that there had been a steady increase in the number of calls and smsses to these centres. A Social Media desk, which will be operating from the Crime Stop contact centre, is also in the pipeline. The SAPS is contributing to the utilisation of social media as a medium, via a SAPS Twitter page that was developed on Twitter on the Internet. It serves as a tool for the SAPS to reach its audience (including the public) directly and immediately. It assists in the fight against crime, and followers are urged to identify suspects, find wanted criminals and share information. SAPS Twitter also shares information about the successes of the SAPS (Ebersöhn, 2013). The SAPS has an official Facebook page, and on 5 September 2015 it had 84,424 users (Facebook, 2015).

1.3. PROBLEM STATEMENT

Brynard and Hanekom (2013:16) state that a problem statement should inform the reader, in as few words as possible, of the planning of the research and the research itself. It must make it clear that the problem needs to be analysed. Social media can be used in the fight against crime; however, what must be analysed is whether and how the SAPS is, in fact, utilising it to investigate and solve crime.

1.4. RESEARCH AIM AND OBJECTIVES

Research objectives are specific information needed, in order to comply with the reason for conducting the research (*What are research objectives?*, 2014). De Vos, Strydom, Fouché and Delport (2011:94) state that the words 'goal', 'purpose', 'objective' and 'aim' are all synonyms for one another. The aim is the goal that one wants to reach, and the objectives are the steps how to reach the goal.

The researcher has conducted research on social media. The aim was to determine whether it could be used to investigate and solve crime, and to what extent the SAPS was already using it in its fight against crime. The researcher furthermore conducted a qualitative study, and collected data by using focus group discussions and short questionnaires for the target group (which consisted of detectives in the SAPS). Literature consulted included hard-copy sources, online publications and accredited journals. The information obtained was processed and analysed. This report, with findings and recommendations, was then compiled.

The research objectives were –

- to provide a general orientation (Chapter 1);
- to discuss the research methodology (Chapter 2);
- to explain the role of social media (Chapter 3);
- to discuss the legal mandate (Chapter 4);
- to discuss the legal mandate – international experiences (Chapter 5);
- to do data analysis and interpretation (Chapter 6); and
- to present findings, reach conclusions, and make recommendations (Chapter 7).

1.5. THE RESEARCH QUESTIONS

Welman, Kruger and Mitchell (2005:6) state that these problems/questions are the difficulties that a researcher experiences in certain situations for which solutions are required. The researcher must know both what the problem is, and the best way to find answers and solutions.

The research questions were as follows:

- Is the SAPS utilising social media in the investigation of crime?
- Does the SAPS access it to find missing persons?
- How far does a person's right to privacy protect them?
- What is social media?
- Who uses social media?
- Which legislation is applicable to the Internet and social media?
- Are there guidelines to using social media as a tool to solve crime?

1.6. VALUE OF THE RESEARCH

The value of this study will be that, should social media prove to be a valuable tool to solve crime, it would assist the SAPS in its fight against crime. It could provide a basis for the design of new programmes and curricula to train police officials to use the Internet and social media more efficiently. It could also be used to develop guidelines, policies and national instructions, with regard to the usage of social media in the investigation of crime. A Standing Operating Procedure (SOP) could be developed and implemented.

1.7. DEFINITIONS

Concepts and words are defined in this research report, because the reader needs to understand the meaning of these words and concepts. Collins (2005:171) defines 'definition' as: "*description interpretation, explanation, clarification, exposition, explication, elucidation, statement of meaning*". The *South African Concise Oxford Dictionary* (2002:305) defines 'definition' as "*a formal statement of the exact meaning of a word*." Berg (2004:29) defines 'definition' as a term "... *whatever you want it to mean throughout the research*".

1.7.1. Internet

According to Papadopoulos and Snail (2012:2), the Internet is an international network of computers – it is an "*interconnected system of networks that connect computers around the world*." Opperman (2013: preface) complicates the definition

by stating that the Internet is "*nothing more than an amorphous computer network with terminals and servers randomly scattered and haphazardly interconnected*".

Lesame, Mbatha and Sindane (2011) describe the Internet as "*new media technology*". The Internet is not human and cannot take sides; therefore, it could be used by anybody, and also for good and bad. The Internet could be used to gain knowledge through news articles, or it could be used to commit crime. The Internet is a medium to which millions of people, across the globe, have access. Millions of IT users are linked together and "*talk*" to one another.

Murray (2010:16) defines the Internet as a "*telecommunications system for computer networks*" – it connects computer networks, and allows digital data to be transferred across these networks.

1.7.2. Social media

Social media refers to the Internet-based tools that people use to interact with one another (Stevens, 2009). According to *Social media overview* (2015), "*[s]ocial media refers to the means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks*".

1.7.3. Social networking

Social media has more than one form – one of them is social networking. Social networking allows many persons to share information. Examples of social networking sites are Facebook, MySpace, YouTube and Twitter. When a person starts using Facebook, they must first open a profile, with personal information such as their name, hobbies, employment, and area where they stay. Pictures and videos are also information that could be posted and shared with friends – 'friends' is a Facebook term for users or groups to whom/which this person links. Online relationships are formed through sharing information on individuals. Home pages and users are able to control the visibility of their information through specific settings (Stuart, 2013).

According to Roos (2012), a widely accepted definition of Social Network Service (SNS) is that provided by Dana Boyd, a social media researcher. She defines SNSs as –

> web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.

1.8. SCOPE OF STUDY

The purpose of this research was to determine whether the SAPS is utilising social media to assist in solving crimes.

1.9. LAYOUT OF DISSERTATION

Chapter 1: General orientation: This chapter discusses the background to the study, and reasons why it was deemed necessary to conduct research on this topic.

Chapter 2: Research design and methodology: The questions on which method was used to achieve goals and objectives, are answered. This chapter deals with what was to be studied.

Chapter 3: Role of social media: This chapter discusses the role of social media. It provides information about its users, and possible advantages and disadvantages it holds for the SAPS.

Chapter 4: Legal mandate: an international experience: This chapter discusses some of the existing and developing legislation applicable to social media, and its execution in the Unites States (US) and the United Kingdom (UK). It also explains some processes in place, which are applicable to the usage of social media in an international policing environment.

Chapter 5: Legal mandate: This chapter gives insight into existing and developing legislation applicable to social media, and its execution in South Africa. It also explains some processes in place, which are applicable to the usage of social media in a policing environment.

Chapter 6: **Data analysis and interpretation**: This chapter deals with the analysis and interpretation of the information provided by the participants.

Chapter 7: Findings, recommendations and conclusions: This chapter deals with the findings, recommendations and conclusions of the research.

1.10. SUMMARY

More than a 100 million people are using Facebook, in Africa. Facebook is only one social network among many other social media networks. This means that more than 100 million people in Africa are using social media. It could therefore be a vast source of information for law enforcement. This chapter gave an overview of the background to the study, the problem statement, the research aim and objectives, the research questions, and the value and justification of the research, as well as definitions, and clarification, of some concepts. The scope of the study was explained, and a layout of the dissertation indicated. The next chapter focuses on the research design and methodology, with regard to the topic.

CHAPTER 2
RESEARCH DESIGN AND METHODOLOGY

2.1. INTRODUCTION

The study was conducted at the SAPS Academy, Paarl. This chapter outlines the history of the Academy, and gives a description and location of the study, the research design and methodology, and information on the literature review. Methods of data analyses, trustworthiness and ethics are also discussed.

2.2. RESEARCH DEMARCATION

2.2.1 History of Academy

On 2 January 1990, the South African Police officially opened the door of SAPS Academy, Paarl. It was then known as the SA Police College for Advanced Training. Training was presented to candidate officers and detectives. The name of the college changed on 22 July 1996 to "SAPS Training College, Paarl". Training then focused on functional skills training. The institution's name changed a number of times. Today it is known as "SAPS Academy, Paarl", and new programmes are developed and presented on a regular basis.

One of the highlights was the amalgamation between SAPS Academy, Paarl and SAPS Academy, Boland, Paarl, on 1 April 2011. Boland Academy became known as the Operational Centre. SAPS Academy, Paarl currently hosts a number of programmes for officers and detectives in the SAPS, as well for international counterparts such as the Southern Africa Regional Police Chiefs Cooperation Organisation (SARPCCO).

This study was conducted at SAPS Academy, Paarl. The reason for this is that it is close to the researcher, and the target group comprised learners from all over South Africa, who were undergoing training at the Academy. As the researcher is working at the Academy, the research on site was cost effective.

2.3 RESEARCH DESIGN AND METHODOLOGY

According to Welman *et al*. (2005:6), there are two research approaches, namely qualitative and quantitative. Welman *et al.* further define quantitative research as research where the feelings and opinions of the individual do not play a role. Information and results must be measured and observed objectively. For some scholars, in qualitative research, the researcher does not primarily observe behaviour, but rather focuses more on the understanding of behaviour. Welman *et al.* (2005:7) describe the difference between qualitative and quantitative research by using a metaphor of a fly looking at a bowl filled with liquid. This is quantitative research (the researcher is observing, and is not part of the process), whereas should the fly be in the bowl, it would experience the feeling of the liquid and the bowl, which then is qualitative research.

This study is qualitative and descriptive, as it entails the description of social media. It is also exploratory, because it investigated the utilisation of social media as a tool for the SAPS to solve/combat crime. The researcher used both primary and secondary data. The researcher consulted books, newspapers, the Internet, articles, and other recent relevant publications and documents, for the literature review. Group discussions with focus groups were carried out, and questionnaires distributed during the discussion sessions, in order to obtain primary data from the respondents. The target group was SAPS detectives undergoing training at SAPS Academy, Paarl.

The researcher used this information to investigate whether social media is used as a tool to investigate, solve and combat crime. The information was also obtained to determine whether detectives in the SAPS need training in the field.

2.3.1 Target population and sampling

The target group was detectives attending training programmes at the SAPS Academy, Paarl. Group discussions with focus groups were arranged, including the distribution of questionnaires to them for completion. Simple random sampling was used. Twenty-five percent (25%) of the detectives on the Detective

Commanders Learning Programme at the SAPS Academy, Paarl were requested to participate as the sample group. The learners represented all nine provinces of South Africa, and were selected for the programme on the grounds of their posts – they were detectives and commanders of their detective branches. The researcher selected them, because detectives in the SAPS are those members specifically tasked to investigate reported crime in South Africa. The researcher chose learners per class, and randomly, per person volunteering to participate. Group discussions were arranged, and short questionnaires were completed – and collected from the participants at the end of each discussion.

2.3.1.1. Purposive sampling

The researcher also made use of purposive sampling. Welman *et al*. (2005:56-57) differentiate between probability samples and non-probability samples. Probability samples are, for example, simple random samples, stratified random samples, systematic samples and cluster samples. Non-probability samples are, for example, accidental or incidental samples, quota samples, purposive samples, snowball samples, self-selection samples and convenience samples. In non-probability samples, one cannot determine the probability that any element or member of a population will be included. Non-probability sampling (thus including purposive sampling) can be used because it could be convenient and economical. According to Henning, Van Rensburg and Smit (2013:71), researchers have criteria which they use to find suitable samples. The criteria are formed by the knowledge of the researcher on the topic, and during the collection of information during the research process. The researcher looks for people who will fit this criteria – thus referring to purposive sampling.

According to Leedy and Ormrod (2014), purposive sampling comprises people or units that are chosen specifically for, and because of, a certain purpose; for example, the purposive sample in this research was Warrant Officer C Welgemoed – a trainer at SAPS Academy, Paarl. The researcher chose him because he presents mainframe systems to members of the SAPS, and is one

of the most knowledgeable persons in the field of computerised systems which are being used by the SAPS.

The researcher received permission from SAPS to do research. Letter for approval attached as per Appendix B.

2.3.2 Sampling procedure

The researcher chose learners per class, randomly, and they were requested to participate voluntarily. Group discussions were arranged, and questionnaires were completed – and collected from the respondents at the end of each discussion.

2.3.3 Methods of data collection

Qualitative: The researcher consulted a wide variety of sources, including books, policies, news articles, articles in police magazines, emails from people working and specialising in the field, personal interviews, photographs of billboards, and a variety of documentation (articles in academic journals, dissertations, papers and research reports) found on websites, with accredited material such as Google Scholar. Group discussions were done with focus groups, and a short questionnaire was completed by the respondents.

The researcher used focus groups. According to Welman *et al*. (2005:7), a focus group is a small group of individuals who give their opinions on specific questions. The group should consist of between six (6) and 12 members. The researcher compiled questions to use in the interviews, and used a random selection of detective commanders on training at SAPS Academy, Paarl. The target group was detectives, because they are specifically tasked to investigate crime. The participants met the criteria, because all of them had experience and knowledge in the investigation of crime. They represented the entire country. (It is to be noted that SAPS members attending courses are referred to as learners, and not students. This study adopts this convention.

According to Braga *et al*. (2011), a criminal investigator must be an expert in the following fields:

- Interviewing skills (be able to interview victims, witnesses and offenders)
- Be able to develop and manage informants
- Be able to conduct covert surveillance (and be able to use advanced surveillance technologies)
- Be able to identify and locate potential witnesses and sources of intelligence
- Be able to preserve and gather evidence
- Be able to prepare cases for prosecution, and liaise with prosecutors before and during trial
- Be able to protect, manage and prepare witnesses for trial
- Be able to sequence the investigative steps in an inquiry, in order to enhance chances of success.
- Must maintain knowledge of, and sometimes maintain relationships with, criminals and criminal groups.

The researcher explained the topic, the reason for the research, and the rules, to the participants. The respondents were requested to write their opinions and answers on a questionnaire provided by the researcher. They could participate anonymously, as this could contribute to openness regarding knowledge of the Internet and social media.

The following questions were asked at the focus group interviews:

- Have you ever had cases that you investigated where social media was used to solve a specific crime?
- If yes, which social network (e.g. Facebook/Twitter/You Tube/WhatsApp/MixIt/any other) played a role?
- Can you elaborate/explain how the social network contributed to your case?
- Do you have access to the Internet at your place of work?
- Do you know how to use Facebook/Twitter/YouTube/WhatsApp/MixIt or any other social networks, in the line of your investigations?

- Would you like to attend a programme that teaches you how to use social media as a tool to solve your cases, in your line of work?

2.4. LITERATURE REVIEW

This study was mainly a literature review of existing legislation and processes to be followed. A wide variety of sources was used, including books, policies, news articles, articles in police magazines, emails from people working and specialising in the field, personal interviews, photographs of billboards and a variety of documentation (articles in academic journals, dissertations, papers and research reports) found on websites with accredited material – such as Google Scholar. The research was based on social media on the Internet. One social media network, Facebook, was extensively used as an example, because it is the most popular social network site, with the most users (Ebizma, 2013).

2.5. METHODS OF DATA ANALYSIS

Data was captured, processed and analysed, in order to interpret the results retrieved. Data was interpreted using spreadsheets, a column chart and pie charts.

2.6. METHODS TO ENSURE TRUSTWORTHINESS AND RELIABILITY

Lehasa (2008:7) states that "*the quality of a research instrument is determined by its validity and reliability*." Welman and Kruger (2001:135) state that there are construct validity, criterion-related validity and content and face validity. In order to ensure construct validity, it is important that the instrument used must measure what it is designed for and what it is supposed to measure. A measurement cannot measure accurately if it is unreliable. In order to ensure validity, the researcher conducted a literature review – as done by Lehasa (2008:7), and designed a questionnaire for respondents to complete, as a measuring instrument. "*Reliability is the degree of consistency or dependability with which the instrument measures the attribute it is designed to measure*" (Lehasa, 2008:7). Welman and Kruger (2001:139) also state that reliability is when results could be generalised, even at different times of measuring, different measuring tests/forms and different administrators. The measurement is a questionnaire that must be completed by

participants to the best of their ability and honesty. Information should be reliable, if the participants complete it with the desired honesty and openness. Interview schedule attached as per Appendix “A”.

2.7. ETHICAL CONSIDERATIONS

According to the Unisa Policy on Research Ethics (Unisa, 2013), principles for research should be both moral and general. Moral principles include autonomy, beneficence, non-maleficence and justice. General ethics principles include the following: (i) are essentiality and relevance; (ii) include maximisation of public interest and social justice; (iii) consider competence, ability and commitment to research; (iv) respect and protect the rights and interests of participants and institutions; (v) require informed and non-coerced consent; and (vi) respect cultural differences, justice, fairness and objectivity, integrity, transparency and accountability, risk minimisation, and non-exploitation.

Babbie (2013:32) states that ethics is associated with morality – which then can be aligned to right and wrong. He further elaborates that the following ethical considerations should be adhered to:

- Voluntary participation
- No harm to participants (including informed consent)
- Anonymity (participant cannot be identified) and confidentiality (participant can be identified, but the researcher undertakes to keep their information confidential, and not share it with other people or readers)

Honesty and confidentiality are the two most important ethical requirements, according to Brynard and Hanekom (2013:6).

2.7.1. Informed consent

The researcher undertook to ensure voluntary participation, and that none of the participants were to be harmed. Information obtained from participants was treated as confidential. Their consent was obtained after open and clear explanations of what the research was about and the reason for the research.

2.7.2. South African Police Service ethics at SAPS Academy, Paarl

The SAPS Academy, Paarl has a value system, namely STICQ (SAPS, [s.a.]):

- S - Service orientation
- T - Teamwork
- I - Integrity
- C - Commitment
- Q - Quality

The researcher committed herself to these values, and applied them to the research. Integrity, honesty and ethical considerations were a priority throughout the research process.

2.8 LIMITATIONS OF STUDY

Responses from members from specialised units were limited, as they were not allowed to share confidential information. The experience of participants in the focus groups was limited, with regard to the use of social media during their investigations.

2.9. SUMMARY

This chapter set out the history of SAPS Academy, Paarl where the research was conducted. It gave a description and location of the study, the research design and methodology (including the target population, sampling and sampling procedure). Information was shared on the review, as well as on methods of data analysis, trustworthiness and ethics. Learners gave their informed consent, and the researcher's commitment and ethics were discussed. The limitations of the study and the demarcations applicable were indicated.

CHAPTER 3
ROLE OF SOCIAL MEDIA

3.1 INTRODUCTION

This chapter discusses the nature and role of social media. It then elaborates on possible advantages and disadvantages of social media for the SAPS.

With the rapid growth of the Internet and other computer networks, criminals have seized the opportunity for electronic crime. Crimes can be committed and facilitated online. Criminals can buy, sell and share information, and they can mask their identities and share information on victims (gathered and identified on the Internet) with other criminals. Investigators can use websites, electronic mail, chat rooms and other file-sharing networks as evidence in their investigations in crimes (Hagy, 2007:iii). In order to understand SAPS utilisation of social media in solving crime, it is important to first understand social media and its applications. The following are relevant aspects:

- The Internet
- Social media and social networking
- Users of social media
- Most popular social media networking sites
- Legislation applicable to the Internet and social media
- Legislation adapted to accommodate new communication media
- Guidelines for using social media as a tool to solve crime
- Crimes where social media were used/could be used to solve crimes
- International police agencies using social media in law enforcement
- Cybercrime
- SAPS readiness to utilise social media in the investigation of crime and finding missing persons
- Protection of right to privacy
- Advantages and disadvantages in the fight against crime

3.2 DEFINITIONS

3.2.1. Social

Collins Cobuild Essential English Dictionary (1989:758) defines 'social' as "*relating to society or to the way society is organized*". *Collins Thesaurus* (2005:662) defines 'social' as "*communal*", "*sociable, friendly*" and "*social gathering*". According to the *Oxford Advanced Learner's Dictionary* (1995:1127), 'social' is defined as "… *activities in which people meet each other for pleasure*". The *South African Concise Oxford Dictionary* (2002:1113) defines 'social' as: "… *an informal social gathering organized by the members of a particular club or group*".

3.2.2. Media

According to the *Oxford Advanced Learner's Dictionary* (1995:727), 'media' is defined as "*the main means of communicating with large numbers of people*". The *South African Concise Oxford Dictionary* (2002:722) defines 'media' as "... *plural form of medium….the means of mass communication (especially television, radio, and newspapers) regarded collectively*".

3.2.3. Twitter

Twitter Help Center (2014) states the following:

> Twitter is a real-time global information network that lets users create and share ideas and information instantly. People and organizations send 140-character messages through our website and mobile site, client applications (e.g., Twitter for Android; Twitter for Originally iPhone OS -iOS), SMS, or any variety of third-party applications.

3.3. ROLE OF SOCIAL MEDIA AS SOURCE OF COMMUNICATION

3.3.1. Social media and social networking

Social networks are divided into the following:

Table 3.1: Type, description and examples of social networks.

Social Network Type	Description	Example of Social Network
Personal Networks	These networks have emphasis on social relationships and users may create detailed online profiles and users connect with one another.	Facebook MySpace
Status Update Networks	These networks were designed for users to post short status updates. These updates ensure quick communication amongst users.	Twitter
Location Networks	The development of these networks was done on the same principle as global positioning systems (GPS) technology. They are designed to broadcast a user's real-time location. It can be posted as public script or as updated viewable by authorised contacts.	Google Latitude Foursquare Loopt
Content Sharing Networks	These networks were designed to enable users to share content that can be: verbal and text-based exchanges, music, photographs and videos.	YouTube Flickr
Shared Interest Networks	These networks were designed for users with a common interest and from a specific group of people	LinkedIn.

(**Source**: Matula, 2013).

According to Matula (2013), the examples of the social network services mentioned above are the most popular and widely used, and, according to SocialSafe Limited (2014), it is one more communication channel.

The term 'social media' is a description of different ways people communicate through digital communication. This includes social networks, blogs, mobile applications and others. The need for real conversations between individuals, organisations and government entities has increased (*Navy Command Leadership Social Media Handbook*, 2012:4). According to Boyd and Ellison (2007:2), social network sites have participants on their sites. These participants are not trying to meet new people, but are rather connecting and communicating with people whom

they already know and are part of their wide social network. These network sites are called social network sites. Types of social media are set out in the following table:

Table 3.2: Type, description and examples of social media.

Types of social media	**Examples**	**Description**
Social Networking	Facebook, Myspace, Bebo, Orkut, BlackPlanet, MiGente, AsianAve	Sites that provide forums for users to create online communities, including posting and viewing of content, interaction with other users, and variable privacy settings determining who may view content.
Blogging	Blogger, WordPress, TypePad, Xanga	An online form of journaling that allows for viewers to interact with the blogger or otherwise comment on the blog‘s content.
Microblogging	Twitter	Services that offer the ability for users to send messages using a limited number of characters and follow other users when they post messages.
Instant Messaging (IM) and Texting	Google Chat, Yahoo Messenger, Skype, texting using mobile phones/devices	IM and texting provide the ability to send and receive (typically brief) messages in real-time. Messaging services increasingly offer video messaging capabilities as well.
Photo Sharing	Flickr, Photobucket, Picasa, Snapfish	Services primarily offering a platform to post, view, and share photos (and, increasingly, videos) as well as post comments.
Video Sharing	YouTube	Services primarily offering a platform to post, view, and share videos as well as post comments.
Wikis	Wikipedia, Wikinews	Services that allow users to create and edit web pages that generally provide information on some topic.
Online Multiplayer Games/Virtual Worlds	World of Warcraft, Second Life	Online games that provide for the ability to play with individuals in various locations connected through the Internet.

(**Source**: Wolff, McDevitt & Stark, 2011:4).

Social media constitutes a collective platform where millions of users access different social media networks to communicate with one another – mostly socially, but also on a business level.

Google Playstore (2014) has many different social media sites available on android operating systems. Below is a series of screenshots of some of these sites, taken on a cell phone:

Image 3.1: Screenshots – Google Playstore - some social media sites available on android operating system cell phones.

(**Source**: Google Playstore: 4 September 2014).

Image 3.2: Screenshots – Google Playstore - some social media sites available on android operating system cell phones.

(**Source**: Google Playstore screenshot: 4 September 2014).

Roos (2012) shares a short history of the development of some of the social network services, as follows:

- The first SNS website was called Six Degrees and was launched in 1997.
- Social network service actually became popular with the launch of Friendster in 2002.
- Facebook was launched in 2003 by a Harvard student, Mark Zuckerberg.
- Other SNSs are Twitter and LinkedIn.
- Different SNSs cater for different interests, as shown in the following table:

Table 3.3: Different SNSs catering for different groups.

SNS	**Group**
LinkedIn Visible Path Xing	Professional sites which focus on business people.
Passion-centric Dogster	Help strangers connect on the basis of shared interests.

SNS	Group
Care2	Helps activists meet.
Couchsurfing	An informal travel network which allows people to book short-period informal home-stay accommodation with other members around the world.

(**Source**: Roos, 2012).

According to Roos (2012), Facebook obtains its income from advertisement – which means that considerable personal information is required. Roos (2012) lists the characteristics of an SNS as follows:

- *Characteristic 1*: A user can create a profile of himself/herself consisting of personal information. The following broad categories of information can be provided on Facebook (it is not compulsory, but for users to find one another, as much as possible information must be provided):
  - Basic information: Current city, home town, gender, birthday, interested in meeting men/women? Looking for friendship? Interest in dating, form a relationship or only network? A user can add his/her political and religious views and also add a biography and their favourite quotations.
  - An optional profile picture
  - A user's relationship status and family members
  - Taste in music, books, movies and television
  - Educational background and employment status
  - Contact information - email address, telephone numbers, physical address and websites where the user can be contacted.
- *Characteristic 2*: The user can add contacts to his profile. The user's contacts then have access to his/her profile information (as in Characteristic 1). The purpose of adding a specific contact depends on the type of SNS the user is using.

- *Characteristic 3*: The user is allowed to browse through other users' sites, and they can leave either a private or public message on these sites. For example, if a user posts a message on another user's "wall' on Facebook, then everybody can read the message linked to those users, and they can respond to it. Interaction also takes place through games. Photographs can be posted on Facebook, and persons can be "tagged" on it - their names will be added to the photographs. A user may "un-tag" himself/herself on a photograph.

Roos (2012) summarises the following characteristics:

- Users are allowed to create profiles consisting of personal information.
- They can add contacts to build their social network.
- They can visit other users' websites and interact with them.

3.3.2. Users of social media

According to a study conducted by Duggan and Brenner (2013:1), younger adults use social media more than older adults do. Their survey shows that females, African-Americans and Latinos show high interest in Twitter, Instagram and Pinterest. MWeb conducted research among 6 499 panellists in August 2009. Their findings are indicated in the following table:

Table 3.4: Users of social media (age and gender).

Age	16-24 years	30%
	25-34 years	28%
	35-44 years	19%
	45-64 years	20%
	Don't know/refused	4%
Gender	Male	58%
	Female	42%

(**Source**: *Friendship 2.0 - MWeb research report*, 2009).

It appears that young adults in South Africa are also more likely than older users, to be linked to social networks.

Gangs are also using social media. They use it for the recruitment of gang members, communication, selling of drugs and to publish their activities. It is all about numbers, for them. Their power grows with growing numbers of members/friends linked on their web pages. Social media is also used to mobilise and gather their members/friends quickly (Wolff, McDevitt & Stark, 2011:5).

According to Wexler (2014:38), cybercrimes are committed on computers, and police departments are also using computers and the Internet to investigate crime. Participants in the report by Wexler (2014) were using social media to gather intelligence, and they are using it in their investigations. Gang investigators in several agencies in Northern California use social media in their investigations, for signs of gang activity. According to Rogers (2014) (also referred to in Wexler's report (Wexler, 2014)), gang detectives in Richmond, U.S. also uses social media in their investigations. Rogers (2014) adds that the supervisor of the gang unit, Lance Daugherty, stated that in San Jose (California), social media provided evidence in more than 25% of gang felony cases. In the same article, it was also said by Tom Kensok, the assistant Contra Costa County district attorney, that social media provided evidence in more than 50% of cases. Evidence was collected from social media sites – Twitter, Facebook, Instagram and YouTube.

According to Dean, Bell and Newman (2012), terrorists and militant extremists are also using social media applications – specifically, Facebook, Twitter and YouTube. They use it to recruit and train members, and to communicate with one another. People can share their political opinions, and organise and instigate riots and revolutions because of the effectiveness of social media as a tool for mass communication. Groups are created on Facebook, which enables the introduction of, for example, jihadist material to members, not directly condoning or encouraging jihadist actions, and thereby not violating any policies. Terrorist organisations can recruit members internationally on Facebook. After recruitment

they train members, using video-sharing technology such as YouTube, and communicate through blogging technology such as Twitter.

According to Howard, Duffy, Freelon, Hussain, Mari and Mzaid (2011:2), social media (in this case Facebook, Twitter and YouTube) played a role in organising protests, criticising governments and the spreading of ideas about democracy in the Arab Spring, after Mohammed Bouazizi set himself on fire on 17 December 2010 in Tunisia in protest of the government. Civil war broke out in Libya, and protests took place in Algeria, Morocco, Syria, Yemen and elsewhere. Howard *et al*. (2011:2-3) found the following:

> First, social media played a central role in shaping political debates in the Arab Spring. Second, a spike in online revolutionary conversations often preceded major events on the ground. Third, social media helped spread democratic ideas across international borders.

According to a 2013 Survey Results (*2013 Survey Results, IACP Center for Social Media*, 2013), a fourth annual survey was conducted on law enforcement use of social media across the US. The International Association of Chiefs of Police (IACP) investigated the current state of usage of social media, to establish what the issues were that agencies were facing in using social media. The survey was done electronically, and 500 law enforcement executives in 48 states across the U.S. participated. Results were the following:

95.9% of the agencies are using social media.
86.1% use Social Media for criminal investigations
92.1% used Facebook, 64.8% used Twitter and 42.9% used YouTube
57.1% does not use social media, but consider usage thereof
69.4% have a social media policy
14.3% are in the process of developing a policy
80.4% reported that social media assisted to solve crimes
73.1% reported that social media improved relationships with the community.

It is clear that international police agencies are increasingly using social media in their daily investigations.

According to Ebersöhn (2013), the SAPS has a Twitter account with a follower count of more than 54 000, which is still growing, and, according to Warrant Officer C. Welgemoed (2015), a trainer at SAPS Academy Paarl, the SAPS is utilising social media in the investigation of crime. The Inkwazi system is being utilised, which includes the use of social media (among other sources) to compile a profile of a suspect. The researcher did not apply for permission to use information about the Inkwazi system, and therefore does not discuss it.

3.3.3. Most popular social media networking sites

The top 15 most popular social networking sites are indicated in the following table:

Table 3.5: The top 15 most popular social networking sites.

Number	Social Network	Number of estimated unique monthly visitors
1	Facebook	750,000,000
2	Twitter	250,000,000
3	LinkedIn	110,000,000
4	Pinterest	85,500,000
5	MySpace	70,500,000
6	Google Plus+	65,000,000
7	DeviantArt	25,500,000
8	LiveJournal	20,500,000
9	Tagged	19,500,000
10	Orkut	17,500,000
11	CafeMom	12,500,000
12	Ning	12,000,000

Number	Social Network	Number of estimated unique monthly visitors
13	Meetup	7,500,000
14	myLife	5,400,000
15	Multiply	4,000,000

(**Source**: Ebizma, 2013).

MWeb conducted research among 6 499 panellists in August 2009, to determine the most popular social networks (*Friendship 2.0 - MWeb research report*, 2009). The results are indicated in the following table:

Table 3.6: MWeb - most popular social networking sites.

Social Network	% - Participants using the social network
Facebook	82%
Youtube	32%
Mixit	29%
Twitter	28%
MySpace.com	18%
LinkedIn	14%
Blueworld	8%

(**Source**: *Friendship 2.0 - MWeb research report*, 2009).

In the report of Wexler (2012), one of the findings is that 83% of the police agencies participating, share information with the public via social media. They mostly use Facebook (74%), Twitter (57%), Nixle (34%), YouTube (34%) and MySpace (24%). Seventy percent (70%) of the participants receive crime tips or other information from the public, via social media.

Matula (2013) states that social networking activity is growing rapidly across the world and that Facebook is growing the fastest and most widely. Facebook

appears to be the most popular social network to be linked to, and because of this, the researcher focused on Facebook and its usage in the investigation of crime.

3.4. ADVANTAGES AND DISADVANTAGES OF USING SOCIAL MEDIA IN FIGHTING CRIME

According to Warrant Officer C. Welgemoed (2015), a trainer at SAPS Academy, Paarl (as referred to at the end of section 3.3.2), the SAPS is utilising social media in the investigation of crime. The Inkwazi system is being utilised – which includes the use of social media (among other sources) to compile a profile of a suspect. The usage of social media is to the advantage in the fight against crime. Warrant Officer Welgemoed (2015) is, however, of the opinion that the function to use social media in the investigation of crime, should stay at a specialised unit such as Crime Intelligence. He maintains that it would be too time consuming for a detective to concentrate on social media. He is also of the opinion that members of Crime Intelligence are trained to use the system optimally, and have better access to it – they also have access to more sensitive information, For example, Detective A is investigating suspect X. He does not know that Detective B is already investigating the same suspect in other cases, but the officer in Crime Intelligence should know.

Murray (2010:50) states that digital data is cheap to gather and cheap to store, but he adds that it also creates the impression that privacy can be disregarded by citizen journalists when they share and copy content.

Wexler (2012) refers to an incident where a police agency had a shooting at a bank which was broadcasted on television. The bank robbery suspect was shot and killed by the police after exiting the bank. Within five minutes after the incident, a video, taken by private parties, was already posted on the news and YouTube. The danger was that, at that time, the police had not eliminated the possibility of a bomb in the bank. The scene was still active when posted online. The police could not yet then discuss the situation with the press. That resulted in the press speculating on what they had seen on the footage posted in the media and on social media.

Families of persons on the scene were concerned, and people were second-guessing the police on their actions, while threats still existed and the scene was still active.

Another disadvantage of using the Internet – and for that matter, social media, in the fight against crime, could be when the law enforcement's computer systems are being hacked. Wexler (2014) reports on a number of hackings and the reasons for a good security system. He states that according to the FBI, a number of police departments' websites were hacked; for example, in February 2012, the websites of the Boston and Dallas police departments were hacked, and officer data stolen. It is imperative that networks be secured to prevent violation, as they contain data of communities and officers.

Wexler (2014) discusses the importance of network security. He refers to the San Diego county police department. The department is paperless, and all its information (victim and witness data, investigative notes, crime and arrest reports, personnel information and other sensitive data) is stored on networks. It could be very harmful should such data get lost – the threat of losing data is constant.

According to Wexler (2014), Tim Murphy, former FBI Deputy Director, says that communities lose faith in law enforcement when they are not protected against criminals, who are able to deface official websites, breach systems, and obtain data illegally.

Roane (2013) states that the SAPS website had been hacked, and that the personal details of almost 16 000 whistle-blowers were published. Lautier (2013), discussing the same incident, warned that South Africa was not immune to global cyber security threats.

A serious issue that an investigating officer must keep in mind is the issue of truthfulness of information circulated on social media. For example, video footage was circulated on social media about a xenophobic attack in Durban; later, it transpired to be an attack taking place in Rustenburg on 7 March 2015. The

footage turned out to be taken on a different date and at a different place than originally reported (Evans & Wicks, 2015).

3.5. SUMMARY

This chapter discussed the definitions and roles of social media. Advantages and disadvantages of social media, and the usage thereof for law enforcement, were discussed. The next chapter informs the reader about the legal mandate in South Africa.

CHAPTER 4
THE LEGAL MANDATE: INTERNATIONAL EXPERIENCE

4.1. INTRODUCTION

As stated by Melekian and Wexler (2013), many legal, civil rights related and privacy-related issues with regard to social media, must still be ruled on in court. This chapter deals with American and British legislation. It also deals with police processes regarding social media, and their utilisation in the U.S. and Canada. There are different types of software available, and more ways to use social media, to fight crime. Cases where social media played a role internationally in solving or reporting crimes, as well as international police agencies that use social media in law enforcement, are mentioned.

4.2. LEGISLATION APPLICABLE TO INTERNET AND SOCIAL MEDIA IN U.S.

Hagy (2007:75) states that it is important for investigators to familiarise themselves with federal requirements, state and local laws, policies and procedures, in order to avoid suppression challenges or civil suits. The following federal law in the U.S. impacts on state investigators:

- Fourth Amendment USA – The Fourth Amendment protects individuals from unlawful searches and seizures.
- Wiretap Act (Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510) – This Act allows the interception of information while it is in transit, and also the disclosure of this information.
- Pen Register and Trap and Trace Statute – This targets the transactional information of communications, and not the gathering of the content of the communications. It manages "*the real-time acquisition of dialling, routing, addressing, and signalling information relating to communications*".
- Electronic Communications Privacy Act [ECPA] (also known as the Stored Wire and Electronic Communications Section – Stored Wire and Electronic

Communications Section (18 U.S.C. 2701 et seq.) – This Act ensures that communications and files stored with a provider are protected on a higher level of privacy. Certain legal processes must be followed in order to force a provider to disclose specific information to law enforcers. (For example, a subpoena can be obtained for the identity of a customer/subscriber, his/her address, telephone records, length and type of service and so forth). The Act limits the voluntary disclosure of some types of information – even to the government. The ECPA is not applicable when an investigator needs information from an individual's computer. A subpoena can be obtained to get information about the identity of individuals.

- Privacy Protection Act [PPA] – (Privacy Protection Act, 42 U.S.C. § 2000aa et seq.) – This Act protects publishers (not only the traditional press, but also individuals who publish material on their web pages), against the handing over of information protected by the First Amendment. It will not, however, be applicable where a person is suspected of having illicit material. A subpoena must be obtained before information can be seized.

4.3. LEGISLATION APPLICABLE TO INTERNET AND SOCIAL MEDIA IN UK

Lloyd (2011:24-272) explains British legislation and procedures at length. Legislation and bodies discussed are the following:

- The Council of Europe – The Council of Europe itself focuses on data protection. Back in 1968, the Parliamentary Assembly of the Council of Europe started addressing the protection of individuals against "*abuse of modern technology*" (Lloyd, 2011:24).
- The Organisation for Economic Cooperation and Development (OECD) – Established in 1960, it focuses on the facilitation of cooperation between member states, aiming to promote economic development. They also published "*Guidelines for the Security of information Systems and networks*", including concepts of data protection and computer crime (Lloyd, 2011:26).

- The Data Protection Act 1998 – with 75 sections and 16 schedules (Lloyd, 2011:35).
- The Human Rights Act 1998
  (both these acts contain provisions to protect the individual, and make provision for the freedom of expression) (Lloyd, 2011:37).
- The Privacy and Electronic Communication Directive – This ensures the protection of fundamental rights and freedoms (specifically the right to privacy and confidentiality) (Lloyd, 2011:165).
- The Council of Europe Cybercrime Convention – The Council of Europe opened the Convention on Cybercrime for signature on 23 November 2011. This document took four years to complete, and one of its focus points is the retention and interception of communications data. So far, 45 countries have signed the Convention (including South Africa – which is a non-member state) (Lloyd, 2011:218). This Convention constitutes a criminal offence when (Lloyd, 2011: 223) the office is against –

    - the confidentiality, integrity and availability of computer data and systems;
    - computer-related offences;
    - content-related offences; and
    - offences related to infringement of copyright and related rights.

  The Convention also plays a significant role in the combatting of child pornography on the Internet (Lloyd, 2011:261). Murray (2010:406) also refers to the abovementioned offences, as well as to ancillary offences. According to him, the Convention strives to synchronise international cybercrime laws.
- The Regulation of Investigatory Powers Act 2000 – According to Lloyd (2011:263), this Act is the most important Act regulating the interception of communications data legitimately. It contains the basic structure to issue

warrants to authorise the interception of communications for the following reasons:

> (a) in the interest of national security,
> (b) for the purpose of preventing or detecting serious crime;
> (c) for the purpose of safeguarding the economic well-being of the United Kingdom; or
> (d) for giving effect to international mutual assistance agreements in connection with the prevention or detection of serious crime (Lloyd, 2011:264).

- The Police and Criminal Evidence Act 1984 (Lloyd, 2011:274)
- The Computer Misuse Act 1990 (Lloyd, 2011:267)
- The Criminal Evidence Act 1965 (Lloyd, 2011:272)

Murray (2010:408) states that British legislation is very well developed in terms of e-Crime of all varieties – such as computer misuse crime, content-related crimes and computer-enabled crimes. He refers to legislation and, additionally, refers to the following Acts:

- The Protection of Children Act 1978
- The Police and Justice Act 2006
- The Terrorism Act 2000 and 2006
- The Protection from Harassment Act 1997
- The Criminal Justice and Immigration Act 2008

Cybercrime has become a major threat, and the following investigative agencies in Britain have therefore been established:

- The National Hi-Tech Crime Unit – established in 2001. The unit investigates computer fraud, hacking, data theft, network attacks and supports the work of the Internet Watch Foundation (IWF) (particularly in cases of child abuse).

- The National Hi-Tech Crime Unit is part of the Serious Organised Crime Agency (SOCA), and is now known as the e-Crime unit in SOCA.
- The Child Exploitation and Online Protection Centre was created in 2006, and works closely with SOCA and Scotland Yard (Murray, 2010:408).

Murray (2010:408) is of the opinion that the UK leads the way in partnerships (also internationally) dealing with child abuse and pornography, as well as an international campaign against Nigerian e-fraud. Murray (2010:516) maintains that the police and law enforcement are able to do triangulation between cell towers, GPS tracking and observation of individuals through Close Circuit Television (CCTV). They are also able to do voice recordings via a person's cell phone. These powers of surveillance are very powerful, and are therefore regulated by the Regulations of Investigatory Powers Act 2000 (RIPA). The Act includes the prohibition of unlawful tracking of telephone calls, emails, Multimedia Messaging Service (MMS) and Instant Messaging (IM) messages. Law enforcement agencies may need warrants to intercept telephone calls, emails, Multimedia Messaging Service (MMS) and Instant Messaging (IM) messages.

According to Murray (2010:518), the retention of data is regulated by the Data Retention Directive (Directive 2006/24/EC). Member states can apply for telecommunication companies and Internet Service Providers (ISPs) to store data for a time frame of not less than six months, and not more than two years. Data could be information that enables the identity of the source of communication, the telephone number of a caller, the name and address of a subscriber, a registered user, a used ID and Internet Protocol (IP), telephone numbers dialled, calls forwarding data, data needed to identify the time, date and duration of a communication, logon and logoff details, type of communication – telephone or Internet service used, kind of equipment using International Mobile Subscriber Identity (IMSI), and the International Mobile Station Equipment Identity number - IMEI). Murray (2010:518) states that this data must be properly

stored, and made available to legal authorities, following a formal and official request. The providers are cell phone and Internet providers (telephone data as well as Internet data).

Gereda [s.a.]) refers to the following:

- The UK Electronic Communications Act, 2000 (UK Act) which has the main purpose of building confidence in electronic commerce. It also addresses electronic signatures and the usage of electronic communication and storage, replacing paper. This Act facilitates electronic communication and, thus, e-commerce.
- Electronic communications regulatory instruments, such as the Electronic Commerce (EC Directive) Regulations 2002, which aim to implement the main requirement of the EU Directive in UK law, and the Directive on Privacy and Electronic Communications, 2002 – which updates the existing EU Telecoms Data Protection Directive of 1999.

Lloyd (2011:271) explains the principle of hearsay evidence as evidence gathered from information created by a person on a computer. The person responsible for creating the original message must testify accordingly, in order for hearsay evidence not to be prohibited. Reliability becomes an issue when information is computer generated, that is, not created by a person on the computer – for example, breath analysers that work with microchips. The Criminal Evidence Act 1965 makes provision for documentary hearsay when (a) a document is created in the course of business, (b) the information is supplied by a person who has personal knowledge of the information, and (c) when a person who should have testified, is deceased, overseas, or, for some reasonable reason, could not remember the correct details/information.

Both national and international law seek to protect the individual against unlawful intrusion into their private space. Legislation enables law enforcers to obtain

unlawful information/publications/communications and make sure that perpetrators can be arrested and brought to justice.

4.4. CANADIAN POLICE: PROCESSES – USAGE OF SOCIAL MEDIA IN INVESTIGATIVE PROCESSES

Bulmer (2014) states:

- Detectives do not need a court order to look at someone's social media account.
- They are allowed to view it online, because it is the public domain of the Internet. They can access or see what is publicly available.
- If they see evidence or information pertinent to an investigation, they can take screen pictures, or download copies of what they see.
- The only complication to this process is that most social networks require you to have an account to be able to search for, and see, the profiles of other users of that network.
- Some police agencies do not allow their officers to have or use a social media account for on-duty work. Many officers create fake accounts using aliases, and do not identify themselves as police officers.
- This can be problematic if they don't have any training in undercover work.
- If they need further information from the social network company, they have to seek a court order to obtain those records.
- Their organisation authorises them to use both overt and covert accounts online, without the appropriate approvals and mandates. Officers must notify their supervisors of any Internet-related activity they undertake with either an overt or covert account.

4.5. AMERICAN POLICE: PROCESSES – USAGE OF SOCIAL MEDIA IN INVESTIGATIVE PROCESSES

As mentioned earlier, Melekian and Wexler (2013) state that if members use social media in investigations and intelligence gathering, they must do the following:

- Always be aware of legal issues when they use social media in investigations and in the gathering of information,
- Make sure that there is a distinction between information that is publicly available, and information obtained by a person using an alias. For example, the New York Police Department (NYPD) has a written policy that states that authorisation is not needed when information is in the public domain (when you do not need a password or other identifier to gain access to the information), but a supervisor's permission must be obtained when a police employee needs to create an alias to enable them to obtain information. The NYPD management is then enabled to keep track of aliases that were used in social media investigations and requests.

4.5.1. Forms and requests – Types of legal requests: Under ECPA – US

- According to the *Transparency Report ...* (2014), legal requests are done through different processes, but also include subpoenas, ECPA court orders, and search warrants. A short description of each document follows:

Subpoena

- The government can issue a subpoena without it first being reviewed by a judge or magistrate.
- A subpoena issued by a government agency can force Google to reveal only specific types of information (for example, Gmail – name of user, IP address, where account was created and signed in and out).
- A subpoena could be used in criminal and civil cases.

ECPA court order

- An ECPA court order must be judicially reviewed.
- The government agency needing the court order must present specific information to a judge or magistrate, and proof that the information is relevant and part of an ongoing criminal investigation.

- The same information can be obtained as with a subpoena, but more detailed. It could include IP addresses, parts of specific emails sent, from what account, or an IP from where a password account was changed; email headings (to, from, date) can also be included
- An ECPA court order can only be used for criminal cases.

Search warrant

- A government agency must request a judge or magistrate to issue the search warrant, and it must demonstrate "probable cause". It must prove why it believes certain information or contraband to be in a specific place that must be searched. The search warrant must contain the place to be searched, and what the agency is searching for.
- It could contain requests for the same information as per subpoena or court order, or be even more detailed. It could request a user's search query information and private information stored in Google accounts (for example, Gmail messages, documents, photos and YouTube videos).
- A search warrant can only be used for criminal cases.

Wiretap, Pen Register and Trap and Trace Orders: Under section 4.1.2 – international legislation, the following acts were mentioned:

- Wiretap Act (Omnibus Crime Control and Safe Streets Act of 1968,18 U.S.C. 2510); and
- Pen Register and Trap and Trace Statute.

➢ According to the *Transparency Report ...* (2014), search warrants and subpoenas are used to gain information created in the past, and, in contrast, information in real time can be obtained by using processes that fall in two categories, namely (1) wiretaps and (2) pen register and trap and trace orders. A short description of these processes is as follows:

Wiretap

- A company may be ordered with a wiretap order to reveal information about communications in real time.
- Wiretaps orders are the hardest to obtain.
- The government agency must prove that –
  - a crime is being committed listed in the Wiretap Ace.
  - information about the crime will be collected with the wiretap.
  - the telephone number or account is part of the crime being committed.
  - 'normal' ways of investigating the crime have failed/will fail/or are too dangerous.
  - there is a time frame of the wiretap – limited.
  - users were notified of having been tapped.

Pen Register, and Trap and Trace

- Information must be revealed about a user's communication (not content) in real time.
- Information such as 'dialling, routing, addressing and signalling information' can be obtained.
- It could include numbers dialled from the user's phone, or IP addresses issued by an ISP to a subscriber.
- It is easier to obtain a pen register or trap and trace order, than a wiretap order or a search warrant.
- The agency must certify that information will likely be obtained, and will be relevant to an ongoing criminal investigation.

4.5.2. Data provided by Google through proper legal processes

- According to the *Transparency Report ...* (2014), Google mostly receives information requests from government agencies in the U.S. for Gmail, YouTube, Google Voice and Blogger. Information it may be forced to provide, according to the ECPA legal process, is the following:

Gmail

Subpoena:

Subscriber registration information (e.g., name, account creation information, associated email addresses, phone number)

Sign-in IP addresses and associated time stamps

Court Order:

Non-content information (such as non-content email header information)

Information obtainable with a subpoena

Search Warrant:

Email content

Information obtainable with a subpoena or court order

YouTube

Subpoena:

Subscriber registration information

Sign-in IP addresses and associated time stamps

Court order:

Video upload IP address and associated time stamp

Information obtainable with a subpoena

Search warrant:

Copy of private video and associated video information

Private message content

Information obtainable with a subpoena or court order

Google voice

Subpoena:

Subscriber registration information

Sign-up IP address and associated time stamp

Telephone connection records

Billing information

Court Order:

Forwarding number

Information obtainable with a subpoena

Search Warrant:

Stored text message content

Stored voicemail content

Information obtainable with a subpoena or court order

Blogger

Subpoena:

Blog registration page

Blog owner subscriber information

Court order:

IP address and associated time stamp related to a specified blog post

IP address and associated time stamp related to a specified post comment

Information obtainable with a subpoena

Search warrant:

Private blog post and comment content

Information obtainable with a subpoena or court order

4.5.3. iCloud, Find My Iphone and extracting Data From Pass Code Locked iOs Devices

According to the *Legal Process Guidelines* (2014), Apple has the following guidelines:

iCloud

iCloud is a cloud service from Apple that enables users to have access to their music, photos, documents etc. from all their devices. Users can back up their devices to the iCloud, and they can set an iCloud.com email account. iCloud email domains can be @icloud.com, @me.com3 and @mac.com. Data is encrypted, and

Apple does not give keys to third-party vendors. The encryption keys are kept at Apple's U.S. data centre. The following information may be available from iCloud:

- Subscriber Information – basic subscriber information – name, physical address, email address, and telephone number may be provided to Apple. Additionally, also iCloud feature connections. iCloud subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process.
- Mail Logs – it is retained for about a period of 60 days. Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs may be obtained with a court order under 18 U.S.C. § 2703(d) or a court order with an equivalent legal standard or a search warrant.
- Email Content – iCloud only stores a subscriber elected email account while it is active. Apple cannot provide deleted content.
- Other iCloud Content: Photo Stream, Docs, Contacts, Calendars, Bookmarks, iOS
- Device Backups – iCloud only stores subscriber content elected while the account is active. Deleted content cannot be retrieved. Content may be stored photos, documents, contacts, calendars, bookmarks and iOS device backups, as well as videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. iCloud content may be provided in response to a search warrant issued upon a showing of probable cause.

Find My iPhone

This application enables the user to locate a lost iPhone, iPad, iPod touch or Mac, and it enable options such as locking or wiping the device. Apple does not have records of maps or email alerts from the service. Find My iPhone connection logs may be available and can be obtained with a subpoena or greater legal process. Find My iPhone transactional activity for requests to remotely lock or erase a

device may be available with an order under 18 U.S.C. § 2703(d) or a court order with the equivalent legal standard or a search warrant. Apple cannot activate this feature on users' devices upon a request from law enforcement. The Find My iPhone feature has to have been previously enabled by the user for that specific device. Apple does not have GPS information for a specific device or user.

Extracting Data from Pass Code Locked iOS Devices

Apple does not have the encryption keys for devices running iOS 8.0 and later versions - they will therefore not be able to do iOS data extractions. Requests for certain categories of active data can be provided with older versions (accompanied by a valid search warrant) from passcode locked iOS devices.

Certain information can then be provided to law enforcement on their own external media. Extraction processes can be done on iOS4 to iOS7. Information that can then be provided is the following: SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history.

Apple cannot provide email, calendar entries, or any third-party app data. The data extraction process can only be performed at Apple's Cupertino, California headquarters for devices that are in good working order. For Apple to assist in this process, the language outlined below must be included in a search warrant, and the search warrant must include the serial or IMEI number of the device. Apple requests that law enforcement attend the data extraction; if not, special arrangements must be made.

A law enforcement officer must provide a FireWire hard drive with enough storage capacity. Apple does not keep copies other than the one that has been applied for – therefore the preservation of the evidence will be the responsibility of the law enforcement agency (LEA).

Apple can intercept a user's communications (ordered by a Wiretap Order); it can also intercept email communications, but cannot intercept users' iMessage or

FaceTime communications because they are end-to-end encrypted. Mail header data may be provided in response to a valid Pen Register Order that includes a showing issued upon 18 U.S.C. § 2703(d).

4.6. DIFFERENT SOFTWARE USED BY POLICE DEPARTMENTS IN FIGHT AGAINST CRIME

According to Wexler (2012), a Chicago (Illinois) commander, Steven Caluris, states that earlier years it was a tiresome process to get a mugshot of somebody printed in colour. Now, they use a data system called Caboodle - the program merges statistics and intelligence analysis. The system is available at any department computer and officers log into it with their own user ID and password. They can run searches to find a variety of information displayed in different ways.

TX Deputy Chief Lauretta Hill, from Arlington (Washington, U.S.) states that they were faced with many unique opportunities during the hosting of big sport events (Wexler, 2012). They had to overcome technological challenges, because many different operating systems were brought by several organisations. They must have operable communications and information sharing. Their biggest asset is that they can communicate in real time. All the commanders were issued with iPads, and they use Digital Sandbox (risk management software that enables the users to input, store and access critical infrastructure and key resource information). Virtual Commander enables users to share and keep track of information of what is going on across the region. Everyday event management software is a useful tool with which to send out direct email or text messages to all the officers or specific groups (Wexler, 2012).

Wexler (2014) states that the following speakers shared the following, with regard to their usage of different software:

Toronto (Canada) Deputy Chief Mike Federico states that the investment in human resources and technology equals cyber-preparedness, and it is important to be aware of the latest technological innovations. He also states that there is open-

source freeware that they can use where activities may appear private, but are, in fact, public – for example, Facebook and Twitter. He also talks about geofencing. Geofencing assists with searches in the virtual world. He states that the police can search for online posts (for example, on Facebook or Twitter) that occurred, for example, shortly after a crime was committed, by people near a crime scene when posting their comments.

In Wexler (2014), the use of geofencing is also supported by Toronto (Canada) Deputy Chief Peter Sloly, who states that geofencing is a very important tool for them as well. He states that the software can be used to search for open source social media content, information within a defined geographical area, and in a specified time frame. Geofences could be used anywhere. He uses an example where they had a stabbing incident during a festival. They used geofencing narrowing it down to surrounding streets. They found thousands of Twitter and Facebook postings about the incident, with the advantage of having many witnesses available.

Photographs were also posted at the time of the incident, which provided more evidence in the investigation. Deputy Chief Sloly, according to Wexler (2014), continued that they were able to use social media to indicate that gang associations led to the stabbing. They use other software tools as well; one, specifically, can "*catalogue all of a person's associations from a single tweet or Twitter account*". The advantage of the technology is that it saves time and manpower. Ongoing monitoring of social media also makes it possible to prevent revenge crimes, and to know the hotspots. Deputy Chief Sloly agrees that using the technology does not prevent or solve every crime, but the police can use the technology with all core operations, and it also provides a great deal of information and dates that can always prove useful (Wexler, 2014).

TX Deputy Chief Lauretta Hill, from Arlington (Washington, U.S.), states that Snap Trends is also software that includes geofencing. Snap Trends can link social media tracking, which enables the monitoring of social media feeds at a specific

area. They were, for example, able to track a person after making a bomb threat in Louisiana: "*Using this tool gives us more information about what's occurring*" (Wexler, 2014).

4.7. MORE WAYS TO USE SOCIAL MEDIA TO FIGHT CRIME

According to Cohen (2010), social media is used by law enforcement agencies – not only to investigate Internet-related crime, but also to solve crimes that are happening on the streets and in the community. The author lists six ways in which law enforcement could use social media and real-time searching, in order to improve their strategies, circulate information to the public, and fight crime:

- Police Blotter Blogs
- The Digital "Wanted Poster"
- Anonymous E-Tipsters
- Social Media Stakeout
- Thwarting Thugs in the Social Space
- Tracking and Informing with Twitter

They are described briefly as follows:

- *Police Blotter Blogs*: A police blotter is, according to Cohen (2010), all the events happening at a police station. Earlier, it was recorded in a register; now, it is done on Twitter feeds, blogs, YouTube, and Facebook fan pages. An example of a blotter can be found on the web page of the Boca Raton Police Department in Boca Raton, Florida (Boca Raton Police Department, 2014b). Their blotter link is on their homepage, and their blotter page specifically contains information about their daily bulletin with arrests made.

Image 4.1: Screenshot – Police Blotter Blog.

(**Source**: Boca Raton Police Department, 2014a).

The digital "Wanted poster": Cohen (2010) states that text, photos and video can be posted on networks such as Twitter, Facebook, and YouTube. Millions of people are using it, and it is a very good way of getting information out about wanted persons. These updates can happen in real time, providing that it is being updated "*up-to-the-minute*".

An example of a police department using this method is the Boynton Beach Police Department in Florida (Boynton Beach Police Department, 2014), where they posted a video on their Facebook page about a wanted suspect. The heading of the post was as follows: "*Do you recognize this brazen gun thief*?"

Image 4.2: Screenshot – A digital “Wanted poster”.

(**Source**: Boynton Beach Police Department, 2014).

- *Anonymous e-tipsters*: According to Cohen (2010), the CitizenObserver Corporation developed a tip411 program, where members of the public can send tips/information anonymously via text, web chat and secure social media publishing, to the police. This information can then be filtered, and then used on other web programmes. For example, they can then send it to Google Maps to enable them to see in which areas crime is concentrated.
- *Social Media Stakeout*: Cohen (2010) states that the Boston Police Department is using Twitter search to monitor postings with specific key words and phrases. It can be used either to react on emergencies (for example, people suddenly tweeting about smoke in a specific area) or it could be used to detect specific patterns in the fight against crime. Cohen (2010) states: "*Use of social media monitoring has a strategic, tactical and operational application for law enforcement*".
- *Thwarting Thugs in the Social Space*: According to Cohen (2010), the NYPD is using the Internet to monitor gang activities. Myspace, Facebook and Twitter are some of the sites used by gang members, and the police use it to their advantage. Gangs have been infiltrated by the police where they were posing as gang members online. They made connections and

intercepted communications of a criminal nature. Photos, videos and links with friends on these pages help the police to understand gangs better – specifically, when they are investigating gangster activities.

- *Tracking and Informing with Twitter*: Cohen (2010) states that many law enforcement agencies are using Twitter to communicate with the public. For example, he states that Sergeant Tim Burrows, from the Toronto Police Service, shares information for the traffic service unit. Twitter is a quick way to share information with the public and local media, and is seen as a valuable service to the public. Cohen (2010) also states that the Broward County Sheriff's Office used Twitter as an example, and created CyberVisor, which is used to broadcast information in real time – for example, about crimes in progress, or information about a bank robbery. The public cannot respond to CyberVisor, but they get the information from the police. It was also used to report a child missing from a local elementary school, with necessary information including descriptions of the child, clothing, and where the child was last seen.

Murray (2010:514) refers to Radio-Frequency Identification (RFID) tags, and Near Field Communication (NFC), that can be added to any device (mostly found on cell phones) – they merge data. Global positioning systems (GPS) and cameras and, for example, iPhones, can expand the real-world environment. An application such as Google Latitude enables a user to track friends by using Google maps. Grindr can be used to find a date by tracking and displaying details of other users of Grindr near the user, and then they can chat via Instant Messaging (IM). Cell triangulation tracking (the cell signal is triangulated between cell towers) is accurate, and, according to Murray (2010:515), in future could be linked to live camera feeds.

Murray (2010:515) states that nobody may track another person without that person's consent. He refers to passive location technology (as used by Google Latitude, Trace a mobile, Mobile Locate and Child Locate), which is regulated by industry code practice. He also states, however, that when a person has given

consent, there is no rule to enforce that a person must be informed every time their location is requested (UK legislation). He further states that the police and law enforcement have for some time been able to do the triangulation between cell towers, GPS tracking and observing individuals through CCTV. They can also record a person via his cell phone microphone, by remotely switching it on.

4.8. EXAMPLES OF CASES REPORTED BY SOCIAL MEDIA

It was reported on 24 April 2013, that in Fulton, more than 45 years ago, a 4-year-old girl, Carolee Sadie Ashby, was killed in a hit-and-run accident. In 2012, a retired detective from the Fulton police, Lieutenant Russ Johnson, added information on the case on a local history Facebook page. An unnamed person came forward with information, and a male, Douglas Parkhurst, 62, was identified as the driver who killed the girl. The statute of limitation had expired, and Parkhurst was therefore not charged (*Facebook helps solve 45-year-old case*, 2013).

According to News24, a U.S. man was jailed for an Obama threat tweet (*U.S. man jailed for Obama threat tweet*, 2013). An American male, Jarvis M. Britton, was sentenced to a year in prison in Huntsville, Alabama. He tweeted a message in which he said that the American president, Barack Obama, should be killed. The 26-year old man pleaded guilty, and he is now on three-years probation, after finishing his time in prison.

It is clear that crimes committed are not only being reported on social media sites, but that the sites also contribute to solving crime. According to *Man kills wife, posts photo on Facebook* (2013), a U.S. man in Miami, Derek Median, 31, was questioned by detectives. He turned himself in after the death of his wife, Jennifer Alfonso. He apparently posted a photograph of his wife's blood-soaked body on Facebook before giving himself up.

In Memphis, Tennessee, a man was arrested for charges including rape, kidnapping and attempted murder, after he allegedly violently attacked a woman.

The woman escaped, and later received a call from an unknown number. She used an application called “Hello”, which connects numbers and Facebook pages. The image of her attacker then popped up. The victim identified the attacker to the police (Brown, 2015).

4.9. INTERNATIONAL POLICE AGENCIES USING SOCIAL MEDIA IN LAW ENFORCEMENT

International police agencies, such as in Canada and the U.S., are using social media in law enforcement. There are more. For example, in Lincolnshire, UK, the police have embraced social media by developing a police policy document which became effective in August 2010. The principles and scope of their policy outlines the use of social networking and video-sharing websites such as Facebook, Twitter, Yammer, Bebo, YouTube and blogs. Social networking and video-sharing websites could be used to publish news and, among others, information of wanted persons, missing persons, and job vacancies in the Force. It could link viewers to police videos. It could contain feedback from residents about policing, and messages on crime prevention (*Social networking and video sharing websites policy PD 174*, 2010).

The 8th SMILE conference (Social Media the Internet and Law Enforcement) took place on 24-26 September 2013, in Omaha, Nebraska. The focus of the event was sharing knowledge on social media strategy, reputation management, policy, and other issues regarding community outreach. There was an international mix of speakers and leading thinkers in these areas. The subject matter experts concentrated on social media, Internet education, investigative techniques and case studies. Papers included research on officer safety, social media policy and strategy, legal issues, and recruitment and retention (*SMILE Conference Omaha*, 2013):

> The SMILE Conference has pioneered the adoption of social media by law enforcement agencies across the world for public outreach, crime prevention, and forensics (*SMILE Conference Omaha*, 2013).

The researcher is of the opinion that the fact that the SMILE organisers have hosted their eighth conference already, shows that social media, the Internet and law enforcement are linked. Social media in law enforcement is growing at a fast rate, and many police services and forces have started to embrace it.

4.10. SUMMARY

In this chapter, information was given on American and British legislation. The chapter covers information on police processes regarding social media and its use in the U.S. and Canada. Various types of software are available to assist in the fight against crime. International cases reported, where social media played a role in the solving or reporting of crimes, were discussed, as was the use of social media by international police agencies. The next chapter deals with the data analysis and its interpretation.

CHAPTER 5
LEGAL MANDATE

5.1. INTRODUCTION

According to Melekian and Wexler (2013), many legal, civil rights and privacy-related issues with regard to social media, must still be ruled on in court. State departments have been using social media (for example, Facebook and Twitter) to circulate information to the public about crime issues, and crime prevention programmes and activities. Toronto Police Service has one of the most advanced procedures in place (Melekian & Wexler, 2013). Social media, can, however, be used to prevent and investigate crime, and the police can then use social media platforms to gather and distribute information.

This chapter relates to the legal mandate in South Africa. Matters discussed are the following: legislation applicable to the Internet and social media, adaptation of the law to accommodate this new medium of communication, guidelines available for law enforcement, police processes in South Africa, examples of where social media play a role in crimes and crime investigation, challenges experienced, digital evidence and cybercrime. Matters regarding the use of social media by the SAPS in the fight against crime, privacy matters, hearsay, entrapment and clandestine and covert operations, are also covered.

5.2. LEGISLATION APPLICABLE TO INTERNET AND SOCIAL MEDIA IN SOUTH AFRICA

5.2.1. South African Law

According to Cyberlaw@SA - Legal library (Opperman, 2013), legislation applicable in South Africa to cybercrime, includes the following:

- Broadcasting Act 4 of 1999
- Copyright Act 98 of 1987
- Films and Publications Act 65 of 1996
- Films and Publications Amendment Act 34 of 1999

- Interception and Monitoring Prohibition Act 127 of 1992
- National Gambling Act 33 of 1996
- Open Democracy Bill 67 of 1998
- South African Constitution 108 of 1996
- Telecommunications Act 103 of 1996
- Trademarks Act 194 of 1993

According to the South African Law Reform Commission (2010:xiv), the following legislation is applicable to electronic evidence in criminal and civil proceedings:

- Civil Proceedings Evidence Act 25 of 1965
- Computer Evidence Act 57 of 1983
- Criminal Procedure Act 51 of 1977
- Electronic Communications Act 36 of 2005
- Electronic Communications and Transactions Act 25 of 2002
- Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Papadopoulos and Snail (2012:4-6) list the following most significant legislation applicable to crime on and through the Internet:

- The Constitution [specifically section 14 – The right to privacy, section 16 – The right to freedom of expression, section 32 – The right to access to information]
- Promotion of Access to Information Act 2 of 2000 (PAIA)
- Electronic Communications and Transactions Act 25 of 2002 (ECTA)
- Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA)
- Electronic Communications Act 36 of 2005 (ECA)
- Independent Communications Authority of South Africa Act 13 of 2000 (ICASA)
- Protection of Personal Information Bill B9 of 2009 (PPI)
- Copyright Amendment Act 125 of 1992 (CAA)

Papadopoulos and Snail (2012:343) state that cybercrime is legislated by the Electronic Communications and Transactions Act 25 of 2002 (ECT Act or ECTA). Pieterse (2015) agrees that this act is the most significant Act in combating cybercrime, and notes the objectives of this Act as being to –

- provide for the facilitation and regulation of electronic communications and transactions;
- provide for the development of a national e-strategy;
- promote universal access to electronic communications and transactions;
- prevent abuse of information systems, and
- encourage the use of e-government services.

Currently, online media falls under the Films and Publications Act 65 of 1996 (South Africa, 1996c). An Internet and Cell Phone Pornography Bill is in the process of becoming a new regulation. This will also make it illegal, in South Africa, for ISPs not to prevent content carrying pornography. According to *Freedom on the Net, South Africa* (2012), a revised draft of the proposed Bill, dealing with Internet pornography, was presented to the Minister of Home Affairs, but was not yet approved in early 2012.

Section 14 of the Constitution (South Africa, 1996a) states: "Everyone has the right to privacy", which includes the right not to have "(d) the privacy of their communications infringed", but it is also important to keep the other aspect in mind, where Cronjé (2013) states that the Promotion of Access to Information Act, (PAIA) 2 of 2000 is in line with the constitutional right of access to information which the state, or any other person, has, when it is required to exercise or protect the rights of anybody.

Section 32 (1) (b) of The Constitution states: "Everybody has the right of access to ..... (b) any information that is held by another person and that is required for the exercise or protection of any rights" (South Africa, 1996a).

Cronjé (2013) continues:

- the State must respect, protect, promote and fulfil, at least, all the rights in the Bill of Rights which is the cornerstone of democracy in South Africa;
- The right of access to any information held by a public or private body may be limited to the extent that the limitations are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom as contemplated in section 36 of the Constitution.

According to Shaikh (2013), the right to and protection of privacy is addressed in the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) Act 70 of 2002 which protects against interception of communication. Shaikh (2013) however is of the opinion that the law in terms of privacy is underdeveloped.

According to the SAPS Cybercrime Unit (SAPS, 2013), the members in this unit, which falls under Technical Support Service, specialise in the gathering of digital evidence in a forensic manner, from computers, cell phones, memory devices, networks, intranets, wide area network and the Internet. They use and develop technology techniques, in order to assist investigators in high-technology crimes. Their work is bound by the following legislation:

- The Constitution of the Republic of South Africa Act 108 of 1996
- Common Law
- Criminal Procedure Act 51 of 1977
- South African Police Service Act 68 of 1995
- Films and Publications Act 65 of 1996
- Electronic Communications and Transactions Act 25 of 2002

Papadopoulos and Snail (2012:338-339) explain that laws governing the investigation of crime evolved in three phases:

Phase 1: There was no legal regulation of the Internet, because it was created as technology – and, specifically the U.S. (which commercialised the Internet in the 1990s), did not see any need to become involved in legislation. For South Africa, the years between 1993 and 2002 (when the legislation was implemented) were uncertain about the legal aspects. Internet crimes could not be investigated, because this conduct was not against any Act.

Phase 2: Governments started to implement legislation. In South Africa the ECTA was implemented. Traditional investigation methods were used, which made the investigation of Internet crime very difficult. ISP's had to be a third-party part of the investigation process. The reactive approach was also not successful because in many cases it was too late to find evidence identifying a suspect as the information no longer existed. An investigatory tool needed to be developed to give investigators access to information on the Internet.

Phase 3: Surveillance, interception or censorship became means of information-gathering on the Internet. There is a difference between censorship (state censorship is an extreme form of control) and surveillance (monitoring, interception, decryption and data retention/preservation). Surveillance technology in South Africa is governed by the RICA. State surveillance was controversial and it met with resistance from the human rights proponents.

Papadopoulos and Snail (2012:340) refute this. They explain that state surveillance as an investigatory tool has the following elements:

- It is not censorship
- It is done to address law enforcement and national security on the Internet
- It is limited to the investigation of serious crime
- It must be governed by legislation to prevent countries becoming a police state
- It is a broad term that embraces different methods and procedures to do surveillance

- Investigators must collect different types of information when they are investigating a crime on the Internet (e.g. content data, traffic data, surveillance method: monitoring, interception , traffic data retention or traffic data preservation and decryption)
- The type of information needed will determine the method of surveillance
- Legislation about data retention and data preservation is new in most countries and ISP's can be obliged to retain traffic data of all its uses for a specific time
- Data can be collected either by the ISP or the investigating agency
- Surveillance methods must be distinguished in the gathering of information, for example in search and seizure.

Osterburg and Ward (2010:204-205) define electronic or technical surveillance as: "the use of any form of technological or computer equipment to monitor the movement or actions of a suspect". It can be done with wiretaps, pen registers (eavesdropping devices), beepers (electronic tracking devices) and a range of optical devices.

According to Papadopoulos and Snail (2012:342), the Council of Europe Convention on Cybercrime (Cybercrime Convention) introduced a treaty in 2001. It was signed by all the Council of Europe countries and is the only international treaty on cybercrime. The focus of the treaty was on law enforcement and not national security. The Cybercrime Convention is seen as outdated because the types of crime on the Internet committed have evolved. Papadopoulos and Snail (2012:342) still recognise the treaty as important because it unites countries in the fight against cybercrime and it forms the basis of law such as the South African ECTA.

Pieterse (2015) confirms that the existing international cooperation with regards to the Council of Europe's Cybercrime Convention on Cybercrime enhances cooperation between law enforcement across borders which is necessary to combat cybercrime.

The authors above mention a number of laws applicable to the Internet and social media in the South African Law. Some of them overlap with their referrals to legislation. A list of legislation referred to above is given in the table below:

Table 5.1: List of legislation.

YEAR	NUMBER	ACT
1965	Act 25 of 1965	Civil Proceedings Evidence
1977	Act 51 of 1977	The Criminal Procedure
1983	Act 57 of 1983	Computer Evidence
1987	Act 98 of 1987	Copyright
1992	Act 125 of 1992	Copyright Amendment
1992	Act 127 of 1992	Interception and Monitoring Prohibition
1993	Act 194 of 1993	Trademarks
1995	Act 68 of 1995	South African Police Services
1996	Act 33 of 1996	National Gambling
1996	Act 65 of 1996	Films and Publications
1996	Act 103 of 1996	Telecommunications
1996	Act 108 of 1996	The Constitution of the Republic of South Africa
1998	Act 67 of 1998	Open Democracy Bill
1999	Act 4 of 1999	Broadcasting
1999	Act 34 of 1999	Films and Publications Amendment
2000	Act 2 of 2000	The Promotion of Access to Information (PAIA)
2000	Act 13 of 2000	The Independent Communications Authority of South Africa (ICASA)
2002	Act 25 of 2002	The Electronic Communications and Transactions (ECTA)
2002	Act 70 of 2002	The regulation of Interception of Communications and Provision of Communication-Related Information (RICA)

YEAR	NUMBER	ACT
2005	Act 36 of 2005	The Electronic Communications (ECA)
2009		The protection of Personal Information Bill (PPI)
		Common Law

(**Source**: Opperman, 2013; South African Law Reform Commission, 2010; Papadopoulos & Snail, 2012:4-6; *Freedom on the Net, South Africa,* 2012; SAPS, 2013).

5.2.2. Impact of legislation on new communication media

- According to the *Transparency Report ...* (2014), government agencies in the U.S. are regulated by a federal statute called the ECPA. It regulates the legal process of how to force companies (for example, Google) to reveal information about their users. According to the report, this Act was passed in 1986, before the Web existed. The report further states that the Act did not keep up with development and the usage of the Internet. Google is therefore working with advocacy groups, companies and other entities such as the Digital Due Process Coalition, to have the law updated and to guarantee the level of privacy that their users should enjoy.

  According to Latib and Thuynsma (2013), social media has been growing so fast, that the courts and legislatures across the world have not had sufficient opportunity to develop social media law: "*it is a very unique and an interactive field*".

  Strutin (2011:288) also agrees that legislation must be updated and include definitions of criminal laws with regard to electronic media. Courts must be able to adapt and be up to date with the latest technological developments. It is a virtual environment, and the interpretation of legal and ethical rules by attorney conduct, can be influenced by it.

  Orenstein (2012) is also of the opinion that case law has not kept pace with technological advances. Some cases involve MySpace, but fewer involving

Facebook (currently the social media leader) and, according to Orenstein (2012), even less cases involving Twitter – although Twitter is the "*real next big thing*".

According to Shaikh (2013), there is no social media law in South Africa. Pieterse (2015) states that procedural law, criminal investigations and prosecutions in South Africa are done by using the Criminal Procedure Act (CPA) Act 51 of 1977, and is of the opinion that this law "*needs to be amended to fully accommodate implications of Information Technology*". Pieterse further states that South Africa has common-law and statutory offences that could be used to prosecute cybercrime criminals. Pieterse (2015) maintains that there is a definite need for legislation to be addressed in line with international legislation. He also refers to the Electronic Communications and Transactions (ECT) Act 25 of 2002, and is of the opinion that this Act fails to recognise the seriousness of cyber offences. He suggests that a working group between the U.S. and South Africa be established. This group must identify areas of mutual interest, strengthen cooperation, and focus on technical assistance, capacity building, training and sharing of best practices. It must include the private sector and civil society stakeholders in future meetings.

Murray (2010:386) states that communities and lawmakers will be challenged, specifically in the next ten to twenty years, particularly with regard to crime against children, on the Internet.

Papadopoulos and Snail (2012:338-339) explain three phases of how laws governing the investigation of crime have evolved, but the process of development is clearly not enough and definitely not fast enough.

5.3. GUIDELINES FOR USING SOCIAL MEDIA TO SOLVE CRIME

It is important to have certain aids in place before a detective or other police official starts using social media as a tool in the investigation of crime. SAPS members must have specific and clear guidelines available to them. They must know what they can and cannot do. This is important, because it will provide them with the

relevant knowledge, and if they act accordingly, they will be protected against civil claims and unlawful actions. It is therefore important to have a proper policy document and proper training in place.

5.3.1. Social media policy and strategy

Melekian and Wexler (2013) state that the use of social media is new, and that many police departments are still in the process of experimenting with social media. Some of the departments use it more extensively than others, and in many cases formal policy was not developed before practical implementation. SocialSafe Limited (2014:6) also refers to the importance of having clear policies in place.

According to Wexler (2012:3), 58% of agencies have an existing policy with regard to employees who post on social media sites, and 12% of agencies are busy working on policies.

Director Daphne Levenson, a director at Gulf States Regional Centre for Public Safety in the U.S. (Wexler, 2014:38) states that the department is proactive, and has good results when there are social media strategies in place. Levenson further states that crime can be solved in a much shorter time when social media is used, because communities are more involved, and provide information to the police – this did not happen before. Social media could be used two ways: firstly, the community could provide information to the police, and secondly, police could warn the community of crimes – for example, scams that are running. Another advantage of using social media in this way is that law enforcement members could concentrate on other issues, funds are better spent, and there is more community involvement.

According to Ebersöhn (2014), the Corporate Communication Component at SAPS Head Office is responsible for monitoring all media (including social media platforms such as Twitter, Facebook and YouTube). They receive reports of fake SAPS accounts on social media, SAPS employees posting negative comments, and inappropriate photographs taken or obtained while on duty. Police members

are urged to be cautious with what they post on their social media network pages (Ebersöhn, 2014).

Emma Sadleir, an associate at Webber Wentzel (M-Net, 2013) states that comments on social media – Facebook and Twitter – could have serious consequences in that it could lead to social media lawsuits. Writing or redistributing comments on social media equals publicising, and therefore the same legislation would apply to the traditional media. It means that when information is posted, it is publicised. Bongani Bingwa, presenter at Carte Blanche, warned:

> What is becoming clear is, every responsible employer should have a social media policy in place. But even if they don't, employees need to know that ... whatever they are writing, Big Brother will be watching (M-Net, 2013).

Some of the recommendations and findings in the report by Melekian and Wexler (2013) are important to mention:

(a) Developing a Social Media Strategy for disseminating information to the public:

- Appoint the right members to manage the social media.
- Keep the privacy of other people in mind - be careful and exact with what you say on social media, because it can stay there forever.
- Know what the implications of social media are for the whole police department.

(b) Use of social media in investigations and intelligence-gathering:

- Always be aware of legal issues when you use social media in investigation and in the gathering of information.
- Make sure that there is a distinction between information that is publicly available and information that was obtained from a person using an alias. For example, NYPD has a written policy that states that authorisation is not needed when information is in the public domain (when you do not need a

password or other identifier to gain access to the information), but a supervisor's permission must be obtained when a police employee needs to create an alias to enable him/her to get information. The NYPD management is then able to keep track of aliases that were used in social media investigations and requests.

Pieterse (2015) is of the opinion that an SOP in a form of a uniform South African version of a Digital Practice Field Guide should be developed, and that it must have clear guidelines on the following:

- search
- seize
- secure (acquisition) and protect the evidential integrity of digital evidence (data storage devices)

Pieterse (2015) states that there should be a clear distinction between "*true computer crime*" and "*computer connected crime*". Separate categories of crime will assist law enforcement in addressing specific identified threats.

Technology, crime and methodology are interlinked. A wide and generic approach to the investigation of crime relating to information and communication technology, should be adopted. Before police members can start using social media as a tool to investigate crime, they must first have a policy document available, to assist them with proper guidelines. It will protect the employees and the SAPS against lawsuits.

5.3.2. Training

Samuel DeMaio, a director at Newark Police (New Jersey), states that they have a police officer who is monitoring social media, to find out where a crime is being planned. This information then enables him and his personnel to act accordingly, to prevent the crime (Wexler, 2014:39).

Melekian and Wexler (2013) state that the Toronto Police Service has two training programmes which are essential for members working with social media:

- A three-day programme to teach members how to use social media to communicate with the public; and
- A five-day programme to teach members how to use social media in the different computer-facilitated crimes, investigative strategies, and how to use social media in the investigation of crime. This programme is presented by an experienced cybercrime detective, to division-level detectives (it is not for persons involved in covert or undercover assignments). The course topics include:

- Internet investigations, including IP addresses and tracing websites
- Social media searches and source intelligence
- Facebook account management, privacy settings, and data searches
- Cellular telephones and devices, Internet service providers, and cell tower data
- Search and seizure of computers, cell phones, and related devices
- Forensic analysis of computers, cell phones, and related devices
- Cross-border investigations, multi-agency cooperation, and other law enforcement resources
- E-Learning tools and resources for continuing education

Von Solms (2015) is of the opinion that training is important. He did a presentation on 24 January 2015 at a seminar hosted by the Institute for Security Studies. He highlights crucial cyber security issues in South Africa and identified priorities of which one is that "*SA must urgently create more cyber expertise*".

According to Kempen (2015a:19-20), the head of Electronic Crimes Unit (ECU), Brigadier Pieterse, is of the opinion that detectives at station level could also be trained to investigate cybercrime. He was a keynote speaker at a seminar hosted by the Institute for Security Studies (ISS) on 26 January 2015.

The researcher could not find any evidence of training given to police officers at station level, on the usage of social media as a tool in the investigation of crime. Training is, however, available for specialised units. For example, the ECU (which falls within the Directorate of Priority Crime investigation [DPCI], also known as the Hawks) is responsible for combatting cybercrime (Kempen, 2015a:21), and the international body – Kids' Internet Safety Alliance (KINSA) – has presented courses on child pornography on the Internet, in South Africa (KINSA, 2015).

The importance of both a proper policy document and proper training, should not be underestimated. There is a gap between the training of detectives at station level and the training of specialised members in specialised units, specifically with regard to crimes relating to the information technology (IT) environment, which should be addressed.

5.4. GUIDELINES FOR LAW ENFORCEMENT

According to Bulmer (2014), social media companies each have their own law enforcement guidelines which they publish either on their websites, in publications or on brochures. Four examples, as discussed, are Facebook, Twitter, Google and Apple. They are all working according to United States Law Enforcement Agency policies (US LEA), because they are American companies.

5.4.1. Guidelines for law enforcement – Facebook

According to *Information for Law Enforcement Authorities | Facebook* (2013), Facebook, one of the social media networking sites, has specific guidelines that must be followed by law enforcement authorities. (There are other guidelines for civil litigants and criminal defendants). Records will only be disclosed in line with the terms and applicable laws – which include the federal Stored Communications Act (SCA), 18 U.S.C. Sections 2701 – 2712. Recent login/logout IP address(es) will be disclosed only when a valid subpoena is issued in an official criminal investigation. A court order under the same Act, section 2703(d), will allow the investigator to get the same record as above, and also specific records or information, but no contents of communications (including message headers and

IP addresses). Stored contents in an account will only be disclosed when a valid search warrant has been issued.

International legal process requirements are that Facebook will only disclose information in terms of its applicable laws. They demand a mutual legal assistance treaty request or letter, before being forced to disclose any information. In case of an emergency, Facebook has a law enforcement online request system, where law enforcement officials can apply for immediate information – specifically where there is "*imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay*" (*Information for Law Enforcement Authorities* | *Facebook*, 2013).

Seventy-four (74) governments (about half of the orders from the United States) requested information from Facebook on about 38,000 Facebook users. The information was requested within the first six months of 2013 (*Governments demanded 38K FB users data*, 2013).

- Evidence of the process and legislation that South Africa uses to request information from social media administrators, could not be found. It still needs to be further investigated. However, there are processes in place, because the South African government has also requested user information from Facebook and Google (*Govt requests Facebook, Google user info*, 2013). A total of fourteen (14) requests were submitted to Facebook and three to Google, during 2013. None of the requests were granted by Facebook, but Google granted one request because of a court order in a case involving defamation. The requests were made by the police, the Hawks and the Department of State Security. According to the *Transparency Report ...* (2014), from January to June 2014, seven requests were submitted from South Africa.

5.4.2. Guidelines for law enforcement – Twitter

Twitter Help Center (2014) provides the following information and guidelines:

The information of Twitter users is held by Twitter, Inc. Most of the information can be seen by anyone because most of the account information is public. A user profile consists of a profile photo, header photo, background image, and status updates (called Tweets). Users can decide if they want to use the location setting and/or the "bio" section to be displayed on their public profile. Users can post photos and videos (via Vine - a Twitter, Inc.-owned standalone mobile service) on their Twitter accounts. It is important for investigating officers to keep in mind that Twitter stores different types of information for different periods of time, and that accuracy cannot be guaranteed by Twitter. Users may create fake or anonymous profiles, because they are not forced by Twitter to provide real names, email verification or identity authentication. Twitter may be able to access a user's account information for a very brief period, if the account has been deactivated; however, deleted content is generally not available (Twitter Help Center, 2014).

Twitter Help Center (2014) states that Twitter will only provide non-public information to law enforcement agencies if they provide a subpoena, court order, or other legal valid documentation. Emergency requests are evaluated on a case-by-case basis, in line with relevant U.S. law – depending on the emergency involving danger of death or serious physical injury, to a person. There are specific guidelines available (Twitter Help Center on https://support.twitter.com/entries/41949-guidelines-for-law-enforcement#.
Search warrants are required for requests of contents of communications which could be Tweets, Direct Messages and photos. Information requested from Twitter will be provided in electronic format, unless it was otherwise agreed upon. The integrity of Twitter information is ensured, because of the fact that its records are self-authenticating and electronically signed. Declarations must be requested specifically (Twitter Help Center, 2014).

Requests from outside the U.S will be treated according to an existing Mutual Legal Assistance Treaty (MLAT), and Twitter will then respond to requests in accordance with this treaty (Twitter Help Center, 2014).

5.4.3. Guidelines for Law Enforcement – Google and YouTube

- According to the *Transparency report ...* (2014), Google has a team that reviews law enforcement requests, to ensure that they satisfy its legal requirements. Requests must be in writing, signed by authorised officials, and according to the appropriate legislation. Documentation needed is subpoenas, court orders or search warrants. They could make exceptions in the case of emergencies, but could not be forced by government if legal processes were not followed. Emergency cases are when a person's life is in danger or a person could be seriously physically harmed. There is, however, legislation in place that allows them to make information available in cases where there are bomb threats of kidnappings involved.

5.4.3.1. Requests from outside the US

- Information will be provided if correspondence goes through the U.S. Justice Department (using MLATs and/or other diplomatic and cooperative arrangements). The U.S. Federal Trade Commission may also provide assistance. When U.S. legislation is applicable, the matter can be investigated by a U.S. agency that then can provide information to non-U.S. investigators. Information provided will be in line with the diplomatic processes in the MLATs, but will be the same as if locally requested, if a U.S.-issued ECPA subpoena, court order or search warrant was obtained (*Transparency report ...*, 2014).
- The MLAT in not the only way for other countries to obtain information from Google. It could also be done with joint investigations between the U.S., local law enforcement and emergency disclosure requests (*Transparency report ...*, 2014).

5.4.3.2. MLAT process between South Africa and the U.S.

- According to the *Transparency report ...* (2014), an MLAT is an agreement between the U.S. and another country. This agreement stipulates how each country will help one another in legal matters – including criminal investigations. Companies (Google included) can be requested via the American government to submit information – on condition that the request was approved by the government first. According to the *INCSR treaties and agreements report* (2012),

treaties are defined as agreements allowing "*evidence and information in criminal and related matters*" to be shared.

South Africa is one of the countries with whom the U.S. has an MLAT agreement (*INCSR treaties and agreements report*, 2012). Other countries are Antigua & Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, the Czech Republic, Dominica, Egypt, Estonia, France, Germany, Greece, Grenada, Hong Kong, Hungary, India, Ireland, Israel, Italy, Jamaica, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Mexico, Morocco, the Kingdom of the Netherlands (including Aruba, Bonaire, Curacao, Saba, St. Eustatius and St. Maarten), Nigeria, Panama, Philippines, Poland, Romania, Russia, St. Lucia, St. Kitts & Nevis, St. Vincent & the Grenadines, South Korea, Spain, Sweden, Switzerland, Thailand, Trinidad & Tobago, Turkey, the Ukraine, the United Kingdom (including the Isle of Man, the Cayman Islands, Anguilla, the British Virgin Islands, Montserrat and Turks and Caicos), Uruguay, and Venezuela. Negotiations with other countries to include them are ongoing.

- The MLAT process is set out in the *Transparency report ...* (2014). The following example below illustrates the process:
  1. A case of identity theft is being investigated in London.
  2. There is evidence that the perpetrator has a Gmail account.
  3. The officer must now find out who this person is.
  4. There is a MLAT between the UK and the U.S.
  5. The officer then sends an application to the UK home office to request the information from the Office of International Affairs in the U.S. Department of Justice.
  6. From there the request is sent to the appropriate U.S. attorney's office (who must now follow the U.S. legal process) and serve the user data request to Google.
  7. Google will then (if proper procedure was followed, and the law and Google policy have been met) provide the information to the U.S. attorney's office,

which will then send it through the correct channels to the officer in London who originally requested it.

5.4.4. Guidelines for law enforcement – Apple

Apple has legal process guidelines in place (*Legal Process Guidelines*, 2014). These guidelines are for use by law enforcement in the U.S. International agencies must contact Apple via subpoenas@apple.com. Apple will only respond to requests posted from a valid government email address.

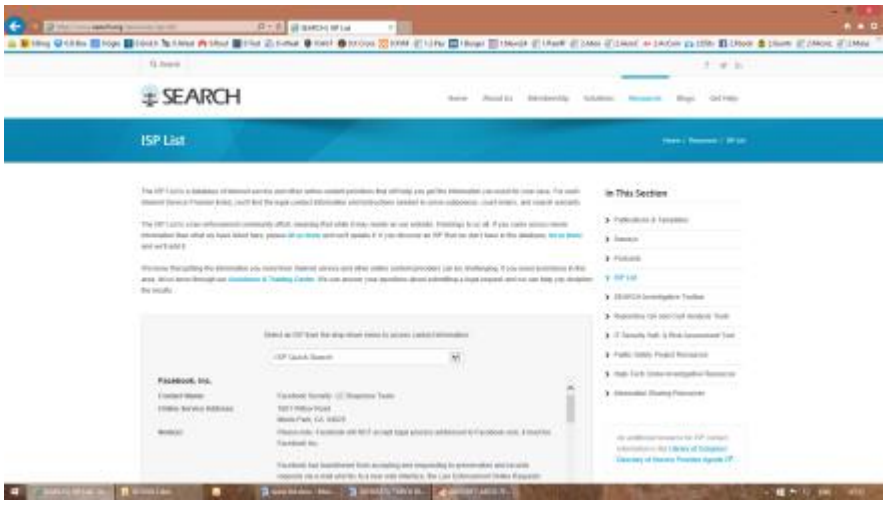
Apple responds to subpoenas, search warrants and court orders, and will, in terms of the preservation requests and U.S. law, preserve information for a specific period of time. They will, under U.S. law, voluntarily disclose information to law enforcement in case of emergencies involving danger of death or serious physical injuries to a person (*Legal Process Guidelines*, 2014).

5.4.5. Guidelines for law enforcement – ISP lists

According to Bulmer (2014), the following website provides an alphabetical list of LEA contact for many Internet Service Providers: http://www.search.org/resources/isp-list/

An example of what the search page on the Internet looks like:

Image 5.1: Screenshot of a search page on the Internet.



(**Source**: Search/ISP List [s.a.]).

5.5. POSITION IN SOUTH AFRICA

5.5.1. SAPS processes - usage of social media in investigative processes

The researcher established that specialised units in the SAPS are working on crimes committed on the Internet or using the Internet. One of these sections is the Electronic Crimes Unit (ECU). Its processes of investigation are confidential, and could therefore not be shared with the researcher. Another international body specialising on the investigation of crimes on the Internet, is KINSA. Its motto is as follows: "*Because the Internet has no borders, this type of crime cannot be addressed from within the confines of one country*" (KINSA*,* 2015)*.*

5.5.1.1. Role of Electronic Crimes Unit

According to Kempen (2015b), the ECU was founded in 2011, and is a national SAPS unit. It resorts under Commercial Crime in the Directorate of Priority Crime Investigation (DPCI). Its members support the SAPS. Its responsibilities are to do the following:

- Conduct research in cybercrime and electronic crime, and develop strategies to address these crimes;
- Develop policies and procedures to police cybercrime;
- Develop cyber security strategies;
- Develop stakeholder partnerships (in the anti-cybercrime community);
- Provide training in cybercrime and electronic crime prevention and investigation;
- Create cyber security awareness; and
- Provide support and coordination in investigations.

5.5.1.2. Role of KINSA

According to the website (http://kinsa.net/), KINSA is a not-for-profit organisation. KINSA strives to rescue children globally from harm and specialises in training police worldwide to find and investigate crimes against children on the Internet. The organisation presents training on two levels, namely general level and

advanced level. KINSA is skilled in peer-to-peer investigations, and teaches members how to build a National Image Library Database. KINSA concentrates on training members in the prosecution of offenders, and works closely with the Royal Canadian Mounted Police, the Virtual Global Taskforce, Interpol, and other global leaders (KINSA, 2015).

5.5.1.3. Role of Interpol

According to the Interpol website (Interpol, 2015c), Interpol is the largest international police organisation in the world.

It helps police organisations around the world to work together. It has a high-tech infrastructure (technical and operational support) to assist in the fight against crime. Its Head Office (The General Secretariat) is in Lyon, France, and it operates on a 24-hour basis the whole year round. It has seven regional offices in the world, with representative offices at the United Nations in New York and at the European Union in Brussels. Interpol has 190 member countries (including South Africa, since 1 January 1948).

According to the page Frequently Asked Questions on the Interpol page, (Interpol, 2015a), police officers must forward requests for international assistance in investigations to its National Central Bureau (NCB) – every member country has a NCB.

The Interpol NCB for South Africa is located in Pretoria, and is part of the SAPS Corporate Communications Department (falling under the National Commissioner). It has permanent members based in Pretoria, and more than twenty (20) liaison officers in other countries. Interpol Pretoria assists the SAPS in its fight against crime, on an international level – it ensures cooperation and exchange of information between police in different countries. It is also working together with SARPCCO – the South African Development Economic Community (SADEC) and the African Union (AU). According to the website of Interpol, Pretoria –

processes extradition requests, stolen vehicle enquiries and drug and fraud offences, and provides assistance to SAPS and Interpol member countries in cases relating to missing persons, child abuse and illegal immigration (Interpol, 2015b).

It is structured as follows:

- Commercial Crime
- Development and Training
- Distribution and Operational Technical Support
- Drugs and Organised Crime
- Economic Crime
- Extraditions
- Fraud
- General Crime
- Intelligence
- Marketing
- Operations
- SARPCCO, Southern African Development Community (SADC) & AU
- Vehicle Crime (Interpol, 2015c).

5.6. EXAMPLES OF CASES REPORTED ON SOCIAL MEDIA

Ajam (2013) reports that Judge Nigel Willis ruled in a case in February 2013 in the South Gauteng High Court, that an interdict which a Johannesburg applicant brought against his ex-girlfriend, was approved. Names were not publicised. She had slandered him on Facebook. The man applied for an interdict for the arrest of the woman, should she post any more defamatory remarks. The woman had to pay his costs. She was ordered to remove the remarks/posts from her Facebook page. This goes to show that persons may be sued for damages, should they make defamatory remarks on Facebook.

Bezuidenhout (2013) reports on a video clip of shots fired between alleged gang members, which was posted on YouTube. Solomons (2013) reports on various videos posted on YouTube, displaying footage from CCTV and private security firms. The videos showed different crimes, such as break-ins, hijackings, assault and murders. Solomons (2013) refers to the following two incidents:

- Ryan Sutherland and a friend were attacked, in Durban, by two men armed with a panga and a knife. They had been hiding in the bushes at Sutherland's home. A third man joined in the attack, and is seen on the footage stabbing Sutherland twice.
- Four men broke in into the premises of a Cape Town company. They stole two laptops and two computer towers, and flew the scene.

Stolley (2015) reports on an incident at a Vereeniging school, where a video was taken of one teenager assaulting another. The filmed incident was posted on Facebook and YouTube.

According to News24 (*Man targeted young girls on BBM, WhatsApp*, 2014), a Rustenburg man appeared in court. He had alledgedly befriended young girls on BBM and WhatsApp, and persuaded them to send him naked pictures of themselves.

A man known as the "Facebook rapist" was arrested near Johannesburg. He was suspected of having committed a number of crimes, and was sought for crimes committed in Cape Town, Durban and Gauteng. According to Dolley (2011), law enforcement tried to track the man through social media, laptops and cell phones that he had used.

5.7. CHALLENGES SINCE INTRODUCTION OF INTERNET

According to Osterburg and Ward (2010:562), the potential of the usage of computers as an aid in investigation of crime has not yet been fully recognised. Reasons for this could be that there is a lack of funding, computer usage is limited because of concerns about a person's right to privacy, there are not enough

trained technicians, and resistance from officers who do not understand what a computer can do for law enforcement.

Osterburg and Ward (2010:5) define the responsibilities of an investigator of crime, as follows:

- He must first find out if a crime was committed.
- He must know if the crime was committed in his jurisdiction, or not.
- He must find out all the facts related to the complaint (find and follow up clues, search for and preserve physical evidence – and remember to answer the following: when? where? who? what? how? and why?).
- He must recover stolen property.
- He must eliminate suspects and identify perpetrators.
- He must find and arrest the perpetrator/s.
- He must assist in the prosecution of the perpetrator – provide admissible evidence to the court.
- He must testify in court – be an effective witness.

From the above, the responsibilities of an investigator seem relatively straightforward, but reality proves to be the opposite. According to Captain C. J. van der Berg (2016), a trainer at SAPS Academy, Paarl, an investigator has the abovementioned responsibilities, but he also agrees that those responsibilities are not straightforward. Investigators must have skills and knowledge – such as knowledge of the law, proper training, experience, administrative skills, interrogation skills, statement-taking skills, know how to protect a crime scene and collect exhibits, have the ability to sort through information and know what is important and what to discard, and be computer literate and be able to communicate effectively with people. They must have informers to enable them to obtain information. Investigators should also be able to handle inquests. They must be able to handle firearms, in order to protect life, and must know how conduct searches and house penetrations. As stated in Chapter 2, section 2.3.3,

Braga *et al*. (2011) state that a criminal investigator must be in expert in certain fields:

- They must have interviewing skills (be able to interview victims, witnesses and offenders).
- They must be able to develop and manage informants.
- They must be able to conduct covert surveillance (and be able to use advance surveillance technologies).
- They must be able to identify and locate potential witnesses and sources of intelligence.
- They must be able to preserve and gather evidence.
- They must be able to prepare cases for prosecution, and liaise with prosecutors before and during trials.
- They must be able to protect, manage and prepare witnesses for trial.
- They must be able to sequence the investigative steps in an inquiry, in order to enhance chances of success.
- They must maintain knowledge of, and sometimes maintain relationships with, criminals and criminal groups.

Papadopoulos and Snail (2012:334) differentiate between the investigation of a crime in a "*physical medium and an electronic medium*" – for example, the Internet, because of "*traditional laws*" that do not always address crime committed on/with the Internet or electronic media. Criminal investigations are guided by laws that were developed for a physical medium, and are characterised as follows:

- "*The object of the crime is mostly tangible in nature*".
- The perpetrator is present at the crime, when committing the crime.
- The crime is mostly committed within the country, and therefore within the jurisdiction of the investigation of the crime.
- The investigation is done by law enforcement agencies, and they also ensure the enforcement of the law.

- An investigation starts after the crime has been reported – investigations are mostly reactive.

Several challenges have emerged since the introduction of the Internet and the World Wide Web (WWW). According to Papadopoulos and Snail (2012:334-335), these challenges are as follows:

- A new electronic medium co-existing with the physical medium.
- This communication system is "*global, borderless, 24-hour and 7-days-a-week*" available.
- Traditional crimes (child pornography, fraud [identity theft], espionage and extortion) have moved to a faster level since being committed on the Internet, with more serious consequences in some cases.
- Denial of Service attacks (DoS) and hacking are new types of criminal behaviour.
- A person can commit cybercrime without being physically present at the time and place of the execution of the crime.
- Perpetrators can communicate online without meeting face to face.
- Cybercrime can be committed (more so than not) against multiple victims at once.
- Intangible information is created, exchanged, received and stored on computing technology and the Internet; therefore, when a crime is committed in respect of information, a criminal investigation is done by collecting information that can be used as evidence of the crime.
- When a crime is committed in one country, and the effect of the crime is felt in another country, then both the countries' domestic laws will apply during the investigation of the crime.
- The information on the Internet or within the electronic medium can lead to the identification of the perpetrator; therefore, the crime can then be linked to a person in the real world.

- Sharing of information, international assistance and cooperation in the gathering of information between investigators, is important when a crime is committed outside the borders of a country.

Pieterse (2015) was a keynote speaker at a seminar hosted by the ISS on 26 January 2015. He is the Section Head of the ECU, Commercial Crime, Directorate for Priority Crime Investigation, in the SAPS. He pointed out some challenges in law enforcement. They include the following:

- Traditional methods of investigating crime are not working in cybercrime investigation.
- There is an increase in cybercrime in the financial environment, and it poses a threat to the democracy and economy of South Africa.
- Strategies must be developed to get rid of cybercrime in South Arica.
- Encryption and access protection are increasingly being used, making it more difficult for investigators to extract evidence from computers.
- Victims do not report these cases – "*many victims are unaware that their computers had been compromised*").
- Strategies/measures against cybercrime have to follow a criminal justice rationale, linked to broader crime prevention and criminal justice policies, and aimed at contributing to the rule of law and the promotion of human rights.

There are unique operational challenges experienced by law enforcement (Pieterse, 2015). They are as follows:

- Digital evidence will, in the future, be part of most of the crime scenes, and law enforcement officials still lack the knowledge on how to gather digital evidence. They do not know the SOPs.
- Cybercrime investigators must address cyber-related investigations, and they must be exposed to testify about it in court (criminal cases).
- There is a critical shortage of trained experts who can analyse and testify about digital evidence.

- Digital evidence can be very volatile, and can easily be compromised by poor handling. These actions may have an influence on the outcome of criminal cases. Law enforcement agencies depend heavily on the availability of *prima facie* evidence.

Some of the lessons learnt, according to Pieterse (2015), are:

- It is difficult to destroy computer-generated information – which means that a forensic footprint could exist. More criminals are using computers in their crimes and therefore more digital evidence is available to be used for the apprehension and prosecution of criminals.
- Many of these crimes are transnational by nature.
- It is difficult and time-consuming to find and secure the evidence and even more so to successfully identity and prosecute these criminals. They use sophisticated techniques and will always find a way to counter security measures. Corruption of corporate and state employees plays a role.
- It is difficult to comprehend cybercrime, because it is a faceless problem.
- Many investigations fail because of mistakes made early in the cases, when important digital evidence is ignored, destroyed, compromised and/or inappropriately handled.

5.8. DIGITAL/ELECTRONIC EVIDENCE

As stated in Chapter 1, section 1.1, digital forensics encompasses the identification, collection, preservation, documentation, examination, analysis and presentation of evidence from computers, computer networks, and other electronic devices. Computer/digital evidence is fragile, and the handling of this evidence differs from that of traditional, tangible evidence (Dempsey & Frost, 2012:467-469). Ngomane (2010:67) defines ‘electronic evidence’ as –

> any probative information stored or transmitted in electronic form that may be legally presented at trial. As with any other type of evidence it is

important for electronic evidence to have a direct bearing on the crime committed.

5.8.1. Search and seizure of electronic evidence in criminal cases

Papadopoulos and Snail (2012:328) state that according to section 82(4) of section 15(3) of the ECTA, “premises" and "article” include information systems and data messages; therefore, the traditional way of search and seizure, according to the CPA sections 20, 21 and 22, may apply. Papadopoulos and Snail further refer to section 81(2) of the ECTA, whereby a cyber-inspector could be of assistance in the matter, but as yet there have been no appointments of cyber-inspectors.

Section 82 (4) of the ECTA reads as follows: "*For the purposes of this Act, any reference in the Criminal Procedure Act, 1977, to "premises" and "article" includes an information system as well as data messages*" (South Africa, 2002a). Section 83 of the ECTA deals with obtaining warrants by cyber inspectors, and reads as follows:

> "83. (1) Any magistrate or judge may, upon a request from a cyber-inspector but subject to the provisions of section 25 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), issue a warrant required by a cyber-inspector in terms of this Chapter. (2) For the purposes of subsection (1), a magistrate or judge may issue a warrant where— (a) an offence has been committed within the Republic; (b) the subject of an investigation is— (i) a South African citizen or ordinarily resident in the Republic; or (ii) present in the Republic at the time when the warrant is applied for; or (c) information pertinent to the investigation is accessible from within the area of jurisdiction of the court. (3) A warrant to enter, search and seize may be issued at any time and must— (a) identify the premises or information system that may be entered and searched; and (b) specify which acts may be performed thereunder by the cyber inspector to whom it is issued. (4) A warrant to enter and search is valid until— (a) the warrant has been executed; (b) the warrant is cancelled by the person

> who issued it or in that person's absence, by a person with similar authority; (c) the purpose for issuing it has lapsed; or (d) the expiry of one month from the date on which it was issued. (5) A warrant to enter and search premises may be executed only during the day, unless the judge or magistrate who issued it, authorises that it may be executed at any other time" (South Africa, 2002a).

A search warrant is, according to Joubert (2001:283-284),

> a written notice issued by a judicial officer such as a magistrate or judge on information on oath received from a police official that an item under section 20 of the CPA is in the possession or under the control of any person or upon or at any premises within the area of jurisdiction of the person that is approached with the application. It must appear to the judicial officer that reasonable grounds exist.

According to Bekker, Geldenhuys, Joubert, Swanepoel, Terblanche and Van der Merwe (2003:223), a subpoena is a document and procedure used by the prosecutor, accused and/or the court, to secure a witness's attendance in court. Failure to comply might lead to the witness's arrest, in order to bring them to court. Different sections in the CPA are applicable (**see** sections 179, 186, 188, 184 and 185.

Milo and Stein (2013:112-113) define a Section 205 subpoena, in terms of the CPA, as a document, used by the National Director of Public Prosecutions (NDPP), instructing a person who refused to give a statement to the police, to provide (under oath) information about a crime, or produce documentary evidence to assist in the prosecution of a crime. The NDPP applies to a judge or magistrate to authorise and sign the Section 205 subpoena. The Section 205 refers to section 205 of the CPA.

One of the members on the focus group (2015-06-04) explained the Section 205 process as follows, to the researcher:

- The investigating officer submits a statement to the State Prosecutor with the details, including the reason why they want a specific person or company summoned to court, and the alleged offence. The investigating officer must be specific about what information he needs from that person or company. He must motivate why he needs the subpoena, and the application must be signed and certified by the investigating officer.
- The prosecutor then completes and signs an application for summons, in term of Section 205 of the CPA.
- The magistrate will then peruse all the documentation, and, upon approval, sign a summons in terms of Section 205 (subpoena).

The researcher was also informed, by one of the members of the focus group (2015-06-04), that a detective who needs information from, for example, Facebook, will also follow the Section 205 process, and then forward it to Interpol Pretoria. Interpol then deals with it through the correct channels. (This process could not be confirmed by the researcher via other resources).

According to Fadilpašić (2015), Facebook opened an office in Johannesburg (South Africa) in September 2015. There are more than a billion people living in Africa, of which 120 million are connected to Facebook.

Legal processes to obtain information from Facebook should then be simplified. Interpol does not have to be contacted – a detective should be able to follow the Section 205 process. (As mentioned, Section 205 refers to Section 205 of the CPA (Milo & Stein, 2013:112-113), the same as obtaining information from a local service provider. The matter should, however, be further researched and investigated.

Lambrechts (2015:67-69) refers to procedures to be followed when South Africa receives a letter of request for evidence. Authorities from Belgium needed information in a criminal case. The request was approved in terms of Section 7(4)

of the International Cooperation in Criminal Matters (ICCMA) Act 75 of 1996 (also referred to as the Cooperation Act). Lambrechts makes a comparison between Section 205 of the CPA and the Cooperation Act sections 7 and 8. The main differences are as follows:

- Cooperation Act – Proceedings conducted by a magistrate, as opposed to the CPA, where a South African Director of Public Prosecutions (DPP) or a Public Prosecutor, play a role in the proceedings.
- Cooperation Act – Refers to evidence, whereas the CPA refers to information.
- Cooperation Act – the Minister's approval must be forwarded to "the magistrate within whose area of jurisdiction the witness resides", but in the CPA no mention is made in this regard. According to Lambrechts (2015), "*such a subpoena can be issued by a magistrate irrespective of where the person, who is to be examined, finds himself/herself*".

5.8.2. Electronic evidence and authentication

According to the South African Law Reform Commission (2010), Casey defines electronic evidence as evidence specifically relating to crime:

> any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi.

Casey defines a computer as any device that stores and manipulates data (South African Law Reform Commission, 2010).

According to the *South African Law Reform Commission* (2010), 'data' and 'data message' in terms of Section 1 of the ECTA, means electronic representations of information in any form, and 'data' message' means data generated, sent, received or stored by electronic means and includes —
(a) "*a voice, where the voice is used in an automated transaction; and*
(b) a stored record".

Chapter 1 of the ECTA states that according to Section 37, "*advanced electronic signature*" means an electronic signature resulting from a process accredited by the Authority.

Zeffert, Paizes and Skeen (2003:699) also support the notion that the ECTA makes provision for the submission of data/information from "*an electronic communications transaction*" to be admissible in court. According to Papadopoulos and Snail (2012:315), there is no formal definition for 'electronic evidence' and describes it as any evidence in digital form. Mason (2014) defines digital evidence by stating that –

> what we mean by 'digital' is anything that has been created or stored on a computer or a computer-like device; this includes data from satellites, for instance. At present, there is no agreed term relating to the form of evidence that comes from our use of technology: specifically, software. For the sake of shorthand, the words "electronic" and "digital" are used interchangeably.

According to Papadopoulos and Snail (2012:317), there are three categories of traditional evidence:

- Oral – testimony of witnesses
- Real or physical evidence – tangible evidence (for example, tape recordings, computer printouts, photographs): "*therefore, where electronic or technologically derived evidence is introduced as proof in itself rather than proof of the facts asserted in the evidence, it would be relevant and admissible as real evidence*"
- Documentary evidence – letters, contracts, affidavits, deeds, notes, printings, pictures, sketches or recordings.

Ngomane (2010) states that the courts classify electronic evidence as real evidence (a computer printout is automatically generated by the computer without human interference) or documentary evidence (a printout of content printed by a

person) – depending on the type of evidence submitted. There is also a difference between electronic and paper evidence, which may be treated differently in court. It is easier to destroy paper evidence, because it can be shredded or burnt, but electronic evidence can still be found on a computer's hard drive, even if deleted; it would only appear to be deleted. It is difficult to destroy electronic evidence.

Papadopoulos and Snail (2012:316) state that electronic evidence can be found on the following: computer internal and external hard drives, email servers, email repositories, single-message files, distinguishing email repositories, file servers, process servers, log files, back-up tapes, removable media and portable devices (for example memory sticks, CDs, DVDs and electronic and voicemail messages on phones).

Mason (2014) lists the following sources of electronic evidence:
Physical devices: computers, mobile telephones, smartphones, Personal Digital Assistants (PDAs) and tablets.

Components: hardware, the processor, storage, software (system software, application software), the clock, time stamps, storage media and memory and data formats.

Networks: the Internet; corporate intranets, wireless networking, cellular networks and dial-up; and, applications, including email, instant messaging, computer to computer (P2P, meaning peer-to-peer), and social networking.

Osterburg and Ward (2010:552) state that locations where evidence could be found are, for example, a person’s home, a person’s workplace, portable devices and/or personal computers, social networking sites (for example Facebook, MySpace, LinkedIn), Internet Service Providers (ISPs), chatrooms, websites and/or external storage devices.

The researcher is of the opinion that detectives do not need a desktop computer with Internet access in order to find a suspect’s social media pages – they can use

a number of devices such as a cell phone, tablet, laptop and any other device that has access to the Internet, but – the question of downloadability of the evidence arises.

The Head of the SAPS electronic crime unit, Piet Pieterse, maintains that technology, crime and methodology are interlinked (Mashiloane, 2014). According to Mashiloane (2014), Pieterse also said that –

> [d]igital evidence is often highly volatile and easily compromised by poor handling. The chances of success in litigation or successful criminal prosecution by law enforcement agencies depend heavily on the availability of prima facie evidence.

Pieterse also states that there is "an urgent need for more trained experts to analyse and to testify about digital evidence." It was also noted that investigations failed where computers were involved, because of mistakes made early in the investigations. Digital evidence is “ignored, destroyed, compromised or inappropriately handled.

With regard to the admissibility of electronic evidence in court, the South African Law Reform Commission (2010) states that The Computer Evidence Act 57 of 1983 (now repealed by Section 92 of ECTA), provided that an “authenticated computer-print-out (was) admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible”. ‘Authenticated’ required the printout be accompanied by an authenticated affidavit and other supplementary affidavits necessary to establish the reliability of the information contained in the printout.

The admissibility of data messages as evidence in court, is now regulated by Section 15 of ECTA which states: “15 (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence—

(a) on the mere grounds that it is constituted by a data message; or
(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
(2) Information in the form of a data message must be given due evidential weight.
(3) In assessing the evidential weight of a data message, regard must be had to-
(a) the reliability of the manner in which the data message was generated, stored or communicated;
(b) the reliability of the manner in which the integrity of the data message was maintained;
(c) the manner in which its originator was identified; and
(d) any other relevant factor.
(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract" (South Africa, 2002a).

The South African Law Reform Commission (2010) discusses the admissibility and evidential weight of data. Section 15 of the ECTA deals with the admissibility and evidential weight of data messages. The scope and meaning of its provisions are still uncertain. The purpose of the section is to establish whether data messages are admissible in legal proceedings, as evidence. Issues are addressed in Section 15(3) of the ECTA.

Papadopoulos and Snail (2012:327) also refer to Section 15(3) of the ECTA, and state that a role will increasingly be played in court by the following:

- the assessment of the weight of electronic evidence;
- testimonies of computer experts; and
- testimonies of computer forensic investigators.

According to Papadopoulos and Snail (2012:322), the ECTA is the only Act that regulates electronic evidence in South Africa. They state that Section 15 of the Act is about the admissibility and evidential weight of data messages. They continue to state that a copy of a data message will be admissible in court, if it could be stated that it was the best evidence that could be found. Section 15 (1) does not make all data messages automatically admissible in court. In the end, data messages are the same as documents, and must therefore abide by the same rules of admissible evidence. Papadopoulos and Snail (2012:322) state that for private electronic documents to be admissible in court the following must be proved:

- Production - the document must first be produced in court – See section 17 and section 28 of ECTA – this means that the document should be handed in during the court proceeding provided that it adheres to certain criteria). According to Schwikkard, Skeen and Van der Merwe (1997:260), the contents of the document must be relevant to the facts in issue, the authenticity of the document must be proved, and the original document must usually be submitted.
- Presentation in original form – the data message must be presented and retained in its original form (integrity must be preserved by means of a proper chain of custody) (Papadopoulos & Snail, 2012:322).
- Authenticity – proof that the document is what it is, by using techniques to prevent date manipulation, alteration and falsification – deliberately or inadvertently. People who can testify to prove authenticity are the writer of a document, an attesting witness, or a person in whose lawful custody the document resides. Authentication will, in the end, depend on the type of document (Papadopoulos & Snail, 2012:323).

Orenstein (2012:222) suggests that attorneys who want to authenticate Facebook pages or other SNS pages, must ensure that –

- a foundation is laid for the origin of the printout of the SNS page.

- the witness gives evidence of where and how the Internet page was located and downloaded.
- the Uniform Resource Locator (URL) of the page is visible on the printout.
- the witness gives evidence of the accuracy of the printout and what they saw on the webpage.
- there is evidence of who has access to the page.
- there is evidence of the identity of the owner of the page. This can be done by either the testimony of a person with knowledge, preferably the owner, or a statement from the service provider. There must be enough information available on the printout (for example name, birth date, geographic location, photo, and other identifying characteristics of the page owner). Processes to obtain information from service providers and computer experts are expensive. It is, however, still possible to obtain information from service providers and computer experts, by means of subpoenas.
- there is proof that the page owner wrote the post. Circumstantial evidence (content of the post) can prove who wrote the post, should the owner deny the fact that they wrote it.

Mason (2014) states that one all uses technology, and that electronic signatures and evidence form a central part of one's lives. The approach to seize, investigate and capture digital evidence must be considered and planned carefully, because flaws in the initial process can render evidence as inadmissible. It is imperative to keep challenges with regard to authenticity, in mind. Authenticity can be hugely affected by the characteristics of digital evidence.

Patzakis (2014) states that the evidence gained from social media is relevant in many legal disputes, and that the challenges in this evidence lie in its authentication. Patzakis (2014) is also of the opinion that evidence relevant to litigation disputes and investigation matters, can be found on many websites. He

states that social media evidence is "*widely discoverable*" and in general it is not restricted by privacy when it is relevant to a case held by a party to litigation or by a key witness. Problems are, however, experienced in court with regard to the authentication of social media data.

The question arises whether a printout of digital evidence will be admissible in court. Section 15 (4) of the ECTA reads as follows:

> (4) a data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract (South Africa, 2002a).

Patzakis (2014), however, states that in many court cases, mere screen printouts of evidence are not enough. It could be sufficient circumstantial evidence if the metadata and file level hash values associated with electronically stored information (ESI) are tested, and their authenticity established. Social media data is of a cloud-based nature, and therefore it cannot be preserved according to traditional computer forensics tools and processes. A major concern is the collection of this data in time – it can be deleted and destroyed very easily.

According to Patzakis (2014), there was a court case where a Facebook printout was submitted as evidence. The court did not find it as authenticated evidence, and did not accept it. However, in another case, MySpace evidence was accepted, because key circumstantial evidence was presented. Evidence included relevant metadata fields, the person’s username, his email addresses registered to the

account, user ID number, stated location, communications with other suspects, and posted photos of the person with associated date and time stamps.

Patzakis (2014) continues that the Texas appellate court found that –

> this is ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them.

In short, the court accepted the evidence, because it was accompanied by the victim's testimony, as well as evidence in the form of metadata, including date stamps and user account names.

Patzakis (2014) states that in order to ensure authentication and preservation of all available evidence, it is important to do proper collection, preservation, searching and production of social media data evidence. It is much easier to establish authenticity if a proper chain of custody is followed.

Patzakis (2014) lists the following key metadata fields, of which any combination of these items could be used to authenticate social media items as key circumstantial data:

Table 5.2: List of key metadata fields to authenticate social media items.

Metadata Field	**Description**
Uri	Unified resource identifier of the subject item
fb_item_type	Identifies item as Wall item, News item, Photo, etc.
parent_itemnum	Parent item number-sub item are tracked to parent
thread_id	Unique identifier of a message thread
recipients	All recipients of a message listed by name
recipients_id	All recipients of a message listed by user id
album_id	Unique id number of a photo or video item
post_id	Unique id number of a wall post

application	Application used to post to Facebook (i.e, from an iPhone or social media client)
user_img	URL where user profile image is located
user_id	Unique id of the poster/author of a Facebook item
account_id	Unique id of a user's account
user_name	Display name of poster/author of a Facebook item
created_time	When a post or message was created
updated_time	When a post or message was revised/updated
To	Name of user whom a wall post is directed to
to_id	Unique id of user whom a wall post is directed to
Link	URL of any included links
comments_num	Number of comments to a post
picture_url	URL where picture is located

(**Source**: Patzakis, 2014).

The following is a list with metadata fields for individual Twitter items:

Table 5.3: List of key metadata fields for individual Twitter items.

Metadata Field	**Description**
created_at	UTC timestamp for tweet creation
user_id	The ID of the poster of a tweet
handle	User's screen name (different from user name)
retweet_id	The post ID of a retweet
retweet_user	The username of the user who retweeted
Reply	Indicates if this tweet is a reply
direct_message	Indicates if this tweet is a direct message
Hashtags	List of all hashtags in the tweet
Description	Up to 160 characters describing the tweet
geo_enabled	If the user has enabled geo-location (optional)
Place	Geo-location from where user tweeted from
Coordinates	Geo-location coordinates where tweet sent

in_reply_to_user_id	unique id for the user that replied
profile_image_url	location to a user's avatar file
recipient_id	unique id of direct message recipient
recipient_screen_name	display name of direct message sender
screen_name	display name for a user
sender_id	unique id of direct message sender
Source	application used to Tweet or direct message(i.e., from an iPhone or specific Twitter app)
time_zone	a user's time zone
utc_offset	time between user's time zone and UTC time
follow_request_sent	Indicates request to follow the user
Truncated	If the post is truncated due to excessive length

(**Source**: Patzakis & Murphy, 2011).

Patzakis (2014) also states that not only metadata must be collected, but also the MD5 hash values of each social media item. MD5 hash values are unique information generated to support the proper chain of custody.

According to Patzakis (2014), X1 Social Discovery is technology that, through several functions, establishes an accepted chain of custody, and, at the end of technical processes, enables quick searches, reviews and the exportation of information.

e-Discovery is another process for finding (identifying, collecting and producing) ESI for lawsuits and investigations. It is also referred to as as e-discovery, ediscovery or eDiscovery (The Basics, [s.a.]).

ESI refers to information such as emails, documents, presentations, databases, voicemail, audio and video files, social media and websites. Retrieval processes are complex, because of the large volume of data that must be analysed. Data is dynamic, and can contain metadata (information such as time-date stamps, author and recipient information, and file properties). It is imperative to keep the original

content and metadata of evidence, because claims can be made, should the evidence be spoiled or tampered with. Relevant electronic material (also including hard copies) is placed under legal hold where it cannot be modified, deleted, erased or otherwise destroyed. It is then sorted, analysed, coded and kept in a secure environment; document reviews can now be done by paralegals and attorneys. The information can be converted to file formats such as TIFF or PDF. "*The ultimate goal of eDiscovery is to produce a core volume of evidence for litigation in a defensible manner*" (The Basics, [s.a.]).

Electronic evidence in criminal and civil proceedings is problematic, as stated by the South African Law Reform Commission (2010), on the grounds of the legitimacy of its accuracy and authenticity. Criminals also use technology in their activities – which means that there are valuable sources of evidence available. Courts are increasingly presented with electronic evidence which comes from a variety of sources. Different crimes, where computers are involved, require different types of evidence that must be submitted.

The South African Law Reform Commission (2010) states that electronic evidence has special characteristics, due to its intangibility and temporality – specifically in a network area. Evidence can easily be created, stored, copied and transmitted. It can also easily be tampered with and modified. Users can hide, disguise or obscure their files quite easily, and in a number of ways. Computer data is also unique, because it contains metadata that can reveal information such as the title of a document, the date of its creation, the author, when the document was last modified, and its location, including details of when it was last transmitted.

Casey (2002) states that networks provide an opportunity for a number of errors, with regard to evidence on networks, specifically with regard to the origin, time of events, errors in logging applications, system limitations, data loss, individuals who conceal or fabricate evidence, mistakes in data presentation and analysis. An advantage, however, is that a single action leaves traces on more than one system. It is possible to trace actions from different systems, and therefore it is also difficult

for criminals to destroy all evidence. Forensic examiners must ensure that they compare data from multiple and independent sources.

Digital evidence must be retained according to legislation. Section 16 of ECTA states that:

> 16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, 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.
> (2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received (South Africa, 2002a).

Gereda [s.a.] states that this provision in the ECTA makes it easier for institutions who must keep records, whether they must keep it according to their own policies or according to legislation – for example, in terms of PAIA. The information must be represented accurately; therefore, it must be stored in the same format as originally generated, sent or received.

The South African Law Reform Commission (2010) discusses the storing of digital evidence, and states that the possibility that the continuous development of hardware and software applications may result in incompatibility, where documents and other media will not be readable, understood or used any more. It is imperative to develop strategies for preservation – not only for the short term, but also for the long term – and safeguarding of storage media, content and documentation, as well as computer software and hardware.

Ngomane (2010:51) states that South Africa does not have a developed or tested (in court) standard process in place to collect, preserve and analyse electronic evidence. Investigators rely on international standards which might not always meet the needs in South Africa. It is, however, important for investigators to maintain the chain of custody, and therefore they must ensure proper collection, preservation and analysis of evidence – or else it would not be admissible in court. If an investigator does not feel qualified enough, they may make use of the services of skilled computer forensics experts. Canada has, according to Wexler (2012), a proper system in place. According to Wexler (2012), Roger Chaffin, a Calgary (Alberta, Canada) Deputy Chief, states that according to their policy, they must hold all digital evidence (including in-car video and digital photographs) for one year. Information that falls under the U.S. Freedom of Information Act must be stored for seven years, before they can destroy it (Wexler, 2012).

Ngomane (2010:72-73) remarks:

> Technology is evolving all the time and becomes more and more complex, therefore a high level of expertise is needed to collect, preserve, analyse and present electronic evidence. Investigators must be properly trained in this field to ensure that evidence is admissible at a trial.

Clear guidelines and training programmes should be developed for all investigators. Training must not only focus on the technical details of cases; investigators must also learn how to use analysis software tools (Ngomane, 2010:72-73).

5.9. CYBERCRIME

As established earlier, in Chapter 3, section 3.3.2, gangs also use social media. They use it to recruit members, for communication, to sell drugs, and to publish their activities. It is all about numbers to them. Their power grows with the increase in members/friends linked to their web pages. Social media are also used to

mobilise and gather their members/friends quickly (Wolff *et al*., 2011:5). Ebersöhn (2013) states that SAPS Twitter has a follower count of more than 54 000, which is still growing. SAPS Facebook on 5 September 2015 had 84 424 users (Facebook, 2015).

As established in Chapter 3, section 3.3.2, terrorists are also using social media for recruitment, training and communication, on a large scale. The researcher is of the opinion that cyber terrorism is too wide to cover in this report, but it is necessary to mention it and to note that according to Dean *et al*. (2012), cyber terrorism is a real threat that must be confronted by police and security agencies.

According to Dean *et al*. (2012), there are specific requirements needed to encounter terrorism of social media - such as proper counter-terrorism policies and methodologies. These policies and methodologies must include a technical infrastructure, human resources (with emphasis on skilled and trained experts in their field) and knowledge and intellectual capital (be at the forefront of new trends and developments).

Wexler (2014) defines cybercrime as "*crimes facilitated by the use of computers or the Internet*". According to Papadopoulos and Snail (2012:337), cybercrime is crime committed on the Internet, and also when a crime is committed by using computing technology. "*Cybercrime is one of the largest illegal industries in the world. Symantec is deeply committed to stopping cybercrime..... online*" (*Symantec Cybercrime*, 2013). It is a significant crime, and therefore needs to be mentioned specifically, because, according to *Symantec Cybercrime* (2013), eighteen (18) adults become victims of cybercrime every second - this equals more than 1.5 million cybercrime victims per second all over the world.

Lesame *et al*. (2011:275-285) list the following different, most common and most dangerous types of cybercrime:

- Phishing and spoofing
- Hacking

- Cyber bullying
- Cyber stalking
- Pornography
- Computer viruses and malware
- Sexual predators
- Identity theft

Papadopoulos and Snail (2012:347-350) list the following as crimes on the Internet:

- Online gambling (the National Gambling Act 7 of 2004 regulates gambling, but online gambling is prohibited).
- Cyberstalking (which could be abusive/threatening/obscene emails, sending many junk emails, "*sending computer viruses*", sending abusive emails under another person's name, and giving a person's name to a sex newsgroup – so that other persons can call or visit the victim). According to Papadopoulos and Snail (2012:348), it was found in a study by the Law Reform Commission, that stalking is not fully covered by criminal law, and it is not addressed as an independent crime. For example, depending on circumstances, it must be addressed as assault, *crimen injuria*, murder, and so forth. However, harassment and stalking is addressed in the Domestic Violence Act 118 of 1996, where a domestic relationship exists. The Protection from Harassment Bill 1 of 2010 may address these issues outside a domestic relationship, but, for now, legislation against cyberstalking has not been implemented.
- Phishing, which could also be called identity theft (a person suspected of phishing could be charged with fraud or that they contravened the Consumer Protection Act 68 of 2008, Section 42(7), or the ECTA, Section 87).
- Creation, distribution and possession of child pornography (The Constitution of South Africa, Section 28, protects children, and the Films and

Publications Act 65 of 1996 makes it illegal for persons to create, distribute and/or be in possession of child pornography. The criminalisation of child pornography is also regulated by the Convention on Cybercrime).

Papadopoulos and Snail (2012:335-336) state that the investigation and prosecution of cybercrime can be difficult – especially when crimes are committed in other countries. They identify the following problems with regard to the investigation of cybercrime:

- Criminal and procedural laws are needed against certain behaviour on the Internet (for example, hacking and DoS). There must be methods available to investigate these crimes and to gather information on the Internet.
- It could happen that a country has legislation in place, but which is not adequate to address the crime.
- An electronic trail can go cold, and therefore the investigators must be able to act quickly when a crime is committed or detected.
- Foreign cooperation and assistance between countries is not always sufficient.
- Laws should address the admissibility and reliability of evidence.
- Cybercrime cannot be addressed by the traditional procedural reactive approach to criminal investigation, because it is not successful.
- In order for the investigation of a crime to be effective, the ISP must assist.
- The use of technology by perpetrators can hamper the investigation of a crime in an electronic medium – for example, peer-to-peer file-sharing, steganography and anonymous remailers – they can ‘hide’ crimes.
- Investigators should keep up with new technology and developments, as information and communication technology is always evolving. They must have the technical ability and skills to investigate these crimes, and know how to gather information.
- The laws created to govern cybercrime must be written in such a way that they accommodate technical development and the effect of globalisation.

Papadopoulos and Snail (2012:346) state that according to the RICA, the ISP should be able to intercept and store traffic data, and they must assist law enforcement and intelligence agencies. According to Papadopoulos and Snail (2012:346), evidence can be obtained with a search and seizure process when the crime is committed on a computer, but when a crime is committed on/through the Internet, surveillance can be used to gather evidence.

In section 5.2.1 Papadopoulos and Snail (2012:338-339) state that surveillance technology in South Africa is governed by the RICA. According to this Act, a law enforcement agency can obtain information by means of a direction (interception direction/real-time communication-related direction/archived communication-related direction/decryption direction). The direction must be issued by a designated judge (a judge from the High Court or a judge designated by the Minister – section 1 of RICA). The information can be gathered by the ISP or the law enforcement agency. The ISP must store traffic data for three years – information can thus be obtained after a crime has been committed. The RICA makes provision for information relevant to serious crimes that have been/are being or will be committed (some of these crimes could be high treason/terrorism/loss of a person's life/organised crime), to be collected.

Papadopoulos and Snail (2012:346) make it clear that none of the Acts must be isolated; there are various rights that must be taken in consideration – for example, the right to privacy and the right to be presumed innocent until proven guilty. The gathering of information must be seen as a serious matter, which is evident in the fact that only a designated judge may give permission, and that it may only be obtained in serious crimes.

5.10. SAPS UTILISATION OF SOCIAL MEDIA IN INVESTIGATING CRIME

According to Wexler (2012), 70% of international agencies make use of social media, where they receive information and tips on crime from the public, and 89% of agencies monitor social media, in an attempt to find investigative leads. For example, a known or suspected gang member may brag about a crime that they

committed, or post comments that could be incriminating information. They could also provide leads that could be used by the police in their investigation of crime.

The SAPS uses social media to find suspects. Below is a screenshot of a post on Facebook, by an investigating officer. See Screenshot - dated 5 August 2014, detective using Facebook Page - Wanted Suspects Western Cape, where he posted that he is searching for a person.

Image 5.2: Screenshot – Post on Facebook by an investigating officer.

(**Source**: Facebook screenshot (5 August 2014)).

According to Warrant Officer C. Welgemoed (2015), a trainer at SAPS Academy, Paarl, the Inkwazi system is a profile compilation programme used by the specialised unit Crime Intelligence. The procedure is that a detective should contact a crime intelligence officer who will then build a profile for them about a specific suspect. The intelligence officer then uses sources such as social media, informers and newspapers, and subsequently does a system search on mainframe systems, such as ICDMS Systems, Firearms System, CAS, and Circulation System. Inkwazi combines all the information, to create a proper profile of the suspect and his friends.

Internationally, social media is being used to find missing persons. For example, Cohen (2010) states that the Broward County Sheriff's Office used Twitter, and created CyberVisor. It was used to report a child missing from a local elementary school, giving the necessary information about descriptions of the child, clothing and where the child was last seen.

Below, is a photo of a billboard at the SAPS Academy, Paarl, taken on 15 September 2014. The billboard displays printouts of the Pink Ladies who send out missing person alerts:

Image 5.3: Billboard at SAPS Academy, Paarl.

(**Source**: Billboard at SAPS Academy, Paarl (15 September 2014)).

5.11. PRIVACY

Roos (2012) explains that –

> South African courts accept Neethling's definition of privacy. Neethling defines privacy as 'an individual condition of life characterised by seclusion from the public and publicity. This

> condition embraces all those personal facts which the person concerned has himself [or herself] determined to be excluded from the knowledge of outsiders and in respect of which he [or she] has the will that they be kept private'. From this definition it is evident that a person determines the destiny of his or her private facts him- or herself. The scope of his or her interest in privacy is therefore also determined by the person him- or herself.

Privacy is protected by Section 14 of The Constitution (South Africa, 1996a).

5.11.1. The right to privacy

Emma Sadleir, an Associate at Webber Wentzel (M-Net, 2013) states:

> Social media law is the law that regulates any conversation that takes place over the Internet, called 'user generated content'. And a decade ago user generated content just didn't exist. If you wanted something published, you had to write a letter to the newspaper, the editor would check it. These days anyone with an Internet connection is a publisher and subject to the same laws that have traditionally regulated the old school media.

Papadopoulos and Snail (2012:252) discuss defamation, and ask the question: When do publication and defamation occur on the Internet? They state that 'publication' is "…. *that it has been made known to at least one person other than the defamed individual*". It can be done in printed or voice media, and therefore includes information posted on social media as well. This means that when a person writes something on the Internet (including social media pages) they have published content. It is available for others to see. The question then arises: Does that person still have the right of his privacy being protected, or not?

According to Milo and Stein (2013:51), every person has a right to privacy, dignity and reputation. For purposes of this research, only the right to privacy will be discussed. The right to privacy is protected by common law, the Constitution of

South Africa (specifically Section 14) and legislation (which also includes the ECTA). There are two ways to invade a person's privacy, according to Milo and Stein (2013:53): "*through an unreasonable intrusion into or interference with a person's private sphere*", or "*through unauthorised disclosure of private facts. Invasion of privacy could lead to civil prosecutions as well as to criminal prosecutions*".

Milo and Stein (2013:53) note the following means of invasion of privacy:

- Intercepting, monitoring and recording communications
- Surveillance, stalking or harassment of a person
- Entering a private home
- Eavesdropping
- Searching a person
- Interrogating a person
- Hacking or gaining unauthorised entry to a person's computer

5.11.2. Privacy of individual

"*.....Facebook is fraught with dangers especially in the field of privacy*" (words of Judge J Willis in *H v W* (12/10142) [2013] par 36). Latib and Thuynsma (2013) discuss the case, and state that on 27 February 2012 the respondent posted on Facebook that the applicant did not provide financially for his family. The applicant was also portrayed as a person with problems with drugs and alcohol, and that he was more interested in that than in his family. The applicant argued that his right to privacy had been infringed, and requested that the posts be removed from Facebook, by the respondent. The respondent refused, on the grounds that the aim of it was for the applicant to take note of his problems.

According to Latib and Thuynsma (2013), the applicant then applied for a court order to force the respondent to remove the post, and to not post further information about him. Judge Willis referred to a number of court cases, and said that users of Facebook should ensure that they change their privacy settings regularly, because of Facebook changing its privacy policy on a frequent basis.

Users themselves should make sure that their privacy settings are set to protect them.

Judge Willis also said (Latib & Thuynsma, 2013), that the test is whether a reasonable person would understand the words and the meaning of the post. It was defamatory, and that in this case the applicant did not protect his privacy. Judge Willis stated that although the comments may have been true, the law still protected a person's right to dignity and reputation. Posts must be to the benefit of the public or in the interest of the public, before they may be published – there must be a clear distinction between "*what is interesting to the public*" and "*what is in the public interest to make known*". In the end, the respondent was ordered to remove the posting from Facebook.

Latib and Thuynsma (2013) further state that Judge Willis found that the respondent could not be ordered not to make further postings, because it would depend on the justification of the publication. A person should remove a post when requested by an offended party. The "*so what*" clause has not been tested in South African courts often, and people should be cautious when posting on social media.

Shaikh (2013) also discusses a case (*Smith v Partners in Sexual Health (non-profit)* (2011) 32 ILJ 1470 (The Commission for Conciliation, Mediation and Arbitration - CCMA), where an employer read an employee's private email account. It was found that email content is not the same as on an Internet blog (accessed not restricted) or social network sites (for example, Facebook) whereby privacy is not secured. Social media sites allow users to view posts by other users (interception) when they are not part of those discussions/communications.

5.11.3. Privacy of public or well-known figures

Latib and Thuynsma (2013) state that the abovementioned case was about an individual's post about a private person, but that Judge Willis also commented on the importance of the difference in standards when a public or well-known figure is involved. There is public interest which is legitimate in the affairs of public figures,

but it is also true that it is not in the interests of the public that every single bit of information and gossip be made public. Just as with the general public, public figures also have the same human rights. It is important to take note of the distinction between what is interesting to the public, and what it is in the public interest to make known.

5.11.4. Privacy of companies

> In the circumstances, a balance needs to be struck between freedom of expression and the limits thereof need to be considered while taking into account whether the defamatory statements, given the context and publication thereof, are true and in the public's interest (Latib & Thuynsma, 2013).

Rheeder (2011) states that what people post can come down to misconduct, as in the cases *Sedick & another v Krisray (Pty) Ltd* [1](2011) 20 CCMA 8.7.1 *and* [2011] 8 BALR 879 (CCMA). The employees (applicants) were dismissed because of "bringing the employer's name into disrepute in the public domain". Derogatory comments were made on Facebook by three employees about their employer (owner and members of his family employed at the company) and the company itself.

One question that arose was whether the employer obtained the evidence legally or whether there was a breach of the employee's privacy? According to Rheeder (2011), the RICA, as amended, applied in this case. In short, it was found that the employer had a right to the information and could intercept it. It was also stated that the Internet is public domain and therefore Facebook is also public domain, but, with unrestricted access only up to a certain level.

The employees failed to make use of the privacy settings and did not restrict access to their postings on their Facebook walls. One of the managers had her own Facebook page and because of the public domain a non-restriction on the employees wall, had free access to the information posted. Therefore, as stated

by Rheeder (2011), it was said that the manager could read, download and print the posts. For all purposes, the employees' posts were open for all - same as if it had been published in newspapers. According to Rheeder (2011), the commissioner therefore found that the employees waived their rights to privacy in the RICA.

A summary of some of the Commissioner's findings in *Sedick & another / Krisray (Pty) Ltd* [2011] 8 BALR 879 (CCMA) by Everett (2011) also made it clear that 1) "interception" is defined in the RICA 2) Facebook pages are in the public domain but it is not any more in the public domain if a user have privacy settings in place 3) The right to privacy is abandoned when users do not use the privacy settings as in this case,

Everett (2011) continues that the right to privacy is also constituted under section 14 of the Constitution, where there is a two-stage process to establish a claim, namely: there must be a "legitimate expectation" of privacy, and should there be an infringement of privacy, then it must not be justifiable in terms of section 36 of the Constitution, which is also supported by Shaikh (2013).

Roos (2012) agrees that the Constitution, specifically Section 14, recognises the right to privacy. It is seen as a basic human right. The section not only protects a person's privacy, but also provides protection against searches, seizures and the infringement of privacy of communications. Roos (2012) refers to two parts of privacy, namely substantive privacy rights and informational privacy rights. Substantive privacy rights means that a person can make decisions about their family relationships, home life and sexual orientation. Informational privacy rights mean that a person cannot gain, publish, disclose or use information about others, without their permission.

According to Roos (2012), to prove the invasion of privacy, the following must be applicable:

- Impairment of the applicants' privacy

- Wrongfulness
- Intention (*animus iniuriandi*)

Everett (2011) refers to the following Australian case: Damien O'Keefe v Williams Muir's Pty Ltd T/A Troy Williams The Good Guys [2011] FWA 5311, Fair Work Australia where an employee was dismissed because of crude and threatening posts concerning a manager on Facebook. Remarks were as follows: (a) it does not matter if the "attacked" person is named or not, and in this case (b) even if the user blocked the post and the employer could not read it, other employees could still read it, and (c) the act of blocking some people from a post could be evidence that the user knew that what he was doing was wrong.

According to Roos (2012), the right to privacy as a legal concept originated in the U.S. in the late 19th century with the growth of newspapers. The introduction of computers in the 1950s also had a huge influence on the development of people's right to privacy. Personal information could be misused, and people were not only concerned about that, but also because of computers disseminating this information at a very fast speed.

Roos (2012) continues that the PPI Bill 9 of 2009 is proposed legislation that has the protection of data in mind:

> The object of all data protection laws is to regulate the processing of personal information or data. These laws aim to give legal protection to a person with regard to the processing of data concerning himself or herself by another person or institution.

Section 14 of The Constitution protects privacy. Section 16 provides for the freedom of expression, and Section 32 provides rights to specific information. However, Section 36 is about the limitation of rights – an individual's rights are partially protected (South Africa, 1996a). The right to privacy means, in practice, that the SAPS and the public must be careful what they say and do, so that it does

not infringe on the right of others. A person must always be aware of what is said, written and publicised, and to whom, when and where.

5.11.5. Threats to privacy

According to Roos (2012), privacy comes under threat when –

- a user adds personal information on his webpage.
- the SNS or third party receives this information and processes it.
- a third party gains access to a user's personal information.
- "Facebook Places" was launched in August 2011.

According to Roos (2012), it is important for users to look at their personal settings on their SNSs and make sure that their privacy settings are set according to their needs. Facebook is also indexed by Google. This enables a person to search for another by only typing in the name of the person on Google. You will then find links to the person's Facebook page, for example. Even if the user has a privacy setting in place, the person on Google will still be able to see the user's username and profile picture.

5.12. PERSONAL INFORMATION STORED IN FACEBOOK

According to Roos (2012), Facebook receives and stores the following personal information:

- Personal information that the user gives out when signing up for Facebook;
- Any content posted by a user (for example, status updates, links shared to a site or other users, messages sent to other users);
- Transaction or payment details made on Facebook;
- ‘Friend’ information provided by a user when searching for friends;
- Activities by the user on the site – for example, sending gifts or adding connections;
- Information about the computer/cell phone/laptop that the user uses to gain access to Facebook (browser type, location and IP address and pages that the user visits);
- Information contained in cookies;

- Information about users from third parties – for example, games that are not part of Facebook, but are linked to the page;
- Information provided from advertising partners, which enables the evaluation of the effectiveness of the advertisements shown to the user; and
- Personal information on users from other users – for example, users tagging one another in photographs.

Roos (2012) states that third-party access to personal information is another threat to take into consideration. This type of threat to privacy is when third parties gain access to personal information by the following:

- Security breaches – no sites are 100% secure.
- Commercial data mining – no real protection is provided (Facebook has it in its terms of service that third parties are prohibited from using the site for data mining, but this is not enough protection).
- Database reverse engineering. (Facebook has an 'advanced search' option which allows a user to search for information on another user's page – even if the security setting allows friends only).
- Passwords can be intercepted – they are not sent in encrypted format.
- The name of the user can be used to search for photographs of them.
- It is easier to gain access to photographs than a user profile.
- Personal information is disclosed to advertisers.
- Users tag other persons in photographs.

5.13. PRIVACY – "PLACES" AND GEO LOCATION IN FACEBOOK

Roos (2012) describes that tracking the location of users could also post threats to privacy. For example, on Facebook there are 'Facebook Places', which is a geo-location service. A user can link to different 'Places' with different devices (computers, laptops, smartphones, iPhone or Blackberry). Users inform their 'friends' on Facebook where they are. Privacy settings can be set to allow only

some friends to see the location. A ‘Here Now ‘application can also be used to display a list of users who check in at a certain ‘Place’.

Roos (2012) states that the Internet is a very public place, and that subscribing to an SNS and submitting personal profile information would be the same as having it up in a public place. Facebook is not different. According to Roos (2012), the privacy settings chosen by a user must be taken in account when the question arises of what information the user wanted to be public or not. If the users chose the ‘only friends’ setting, then ‘only friends’ have access to the information and not any other people. Should one of these ‘friends’ then make any information public, then that person would be liable for breach of privacy. Roos (2012) also states that it is important to keep in mind that grounds of justification can negate wrongful infringement of privacy.

5.14. GROUNDS OF JUSTIFICATION

Consent – Roos (2012) states that when users post private information on their web page, then they consent to the publication of the information (provided that certain criteria have been met – for example, the user must know and understand the nature and extent of repercussions).

Roos (2012) adds that it is wrongful for a third party to gain access to a user’s information on an SNS when the privacy setting is ‘friends only’. In this author's opinion, it should also be wrong to conduct an extensive search on the Internet and SNS for a person. She states that "...*such conduct could, in my view, be considered analogous to the ‘shadowing’ of a person in real life, and could therefore be wrongful*". But is it? The Internet is public domain - why would it be wrong?

5.15. HEARSAY AND ADMISSIBILITY OF EVIDENCE

Zeffert *et al*. (2003:393) ask whether data messages and data could be defined as hearsay, as in the ECTA, and according to Section 3 of the Law of Evidence

Amendment Act 45 of 1988. They also ask "*to what extent do the provisions of both the Act and ECTA liberate such evidence from the exclusionary rule?*"

They answer that a computer is not a person, and therefore the evidence does not depend on another person's credibility – other than the one presenting the evidence. This means that the police official presenting the evidence must ensure that the evidence has its probative value, is credible, and that the information on the printout was accurately registered and processed. Zeffert *et al*. (2003:393) state that it would be hearsay "*whenever it is tendered in evidence in circumstances where the probative value of the evidence depends, in this sense on the credibility of such a person*".

Zeffert *et al.* (2003) are of the opinion that Section 15 of the ECTA has the purpose of including as much computer-generated evidence to be admissible, and to not let it fall into the "*hearsay trap*". Zeffert *et al.* (2003:395) state that there are statutory provisions where the submission of affidavits and certificates as *prima facie* proof of the content will be admissible. The CPA makes provision for it.

Papadopoulos and Snail (2012:324) state that where the truth of a data message is contested in court, the author of the message must testify and be cross-examined about it. If not, then it would be seen as hearsay evidence.

According to Orentstein (2012:194), posts or statements on social media sites are seen, by definition, as being out-of-court, and would raise concerns that such posts or statements were hearsay. This could raise issues in criminal cases, should the government wish to use these statements against an accused if there is not supportive testimony. Orentstein (2012:195) could not find any examples using social media.

Hearsay evidence is regulated in South Africa by the Law of Evidence Amendment Act 45 of 1988. According to Section 3 (1), hearsay evidence shall not be admissible in court unless both parties agree that it could be submitted as evidence and if the person

> "(1)(b) ... upon whose credibility the probative value of such evidence depends, himself testifies at such proceedings"," or where the court takes into account the nature of the evidence, the purpose of the evidence, the reason why the person " upon whose credibility the probative value of such evidence depends, or any prejudice and any other factor that must be taken in account by the court" (South Africa, 1988).

According to *Memorandum* (2008), evidence in hearsay is mostly inadmissible. Although it could be relevant, it is not trustworthy because the person who wrote or spoke the statement is not the one testifying about it.

Everett (2011) asks the following questions with regard to privacy and hearsay, when evidence is submitted:

- What if the remarks were reported to the employer by a 'friend'?
- Is the information provided hearsay or real evidence?
- If the answer is 'yes' and the information provided is hearsay, there could be, according to Everett (2011), a possibility that it could be admissible - if (a) the witness testified that it is what he saw that was posted, and (b) that he printed the page.

Zeffert *et al.* (2003:395) state that computer-generated evidence may be admissible as hearsay evidence in exceptional circumstances, and, according to Section 221 of the CPA, in specific situations.

5.16. ENTRAPMENT

When an investigative officer opens a social media account – for example, a Facebook page, under a false identity, and befriends a suspect, the question of entrapment could arise.

The researcher has added this paragraph, because it should be made clear that opening a false page and befriending a person does not entice that person to commit a crime. It is clearly seen in the definition of 'entrapment', where

Osterburg and Ward (2010:197) define entrapment as when a police officer entices a person to commit a crime.

For the purposes of this research, the crime has already been committed. The investigating officer is merely using social media as one of the tools in his investigation of the crime, and therefore he will not persuade a person to commit a crime. Entrapment is thus not applicable in this kind of investigation.

5.17. CLANDESTINE OR COVERT OPERATIONS

Osterburg and Ward (2010:554) state that 'sting operations' have become common practice in the US whereby investigators communicate online with suspected paedophiles.

The following statement was made in Melekian and Wexler (2013:12):

> Location of suspects: I was looking for a suspect related to drug charges for over a month. When I looked him up on Facebook and requested him as a friend from a fictitious profile, he accepted. He kept 'checking in' everywhere he went, so I was able to track him down very easily.

Section 252A of the CPA reads as follows:

> Authority to make use of traps and undercover operations and admissibility of evidence so obtained:
> (1) Any law enforcement officer, official of the State or any other person authorised thereto for such purpose (hereinafter referred to in this section as an official or his or her agent) may make use of a trap or engage in an undercover operation in order to detect, investigate or uncover the commission of an offence, or to prevent the commission of any offence, and the evidence so obtained shall be admissible if that conduct does not go beyond providing an opportunity to commit an offence: Provided that where the conduct

> goes beyond providing an opportunity to commit an offence a court may admit evidence so obtained subject to subsection (3)
>
> (2) In considering the question whether the conduct goes beyond providing an opportunity to commit an offence, the court shall have regard to the following factors:
>
> *(a)* Whether, prior to the setting of a trap or the use of an undercover operation, approval, if it was required, was obtained from the attorney-general to engage such investigation methods and the extent to which the instructions or guidelines issued by the attorney-general were adhered to (South Africa, 1977).

Pieterse (2015) states that law enforcement uses undercover agents searching for, and attempting to record, in real time, acts of criminals who are already committing computer crimes. An advantage of the proactive approach is that it "*bypasses some of the investigatory hurdles of anonymity, lack of record and under-reporting inherent in computer cases*". It also has the potential to stop criminals before "*damage is done*".

5.18. SUMMARY

This chapter related to the legal mandate in South Africa. It deals with legislation applicable to the Internet and social media, the adaptation of the law to accommodate this new medium of communication, guidelines available for law enforcement, police processes in South Africa, examples where social media played a role in crimes and the investigation thereof, challenges experienced, and digital evidence and cybercrime. It elaborated on how the SAPS is using social media in their fight against crime. Information is shared on privacy matters, hearsay, entrapment, and clandestine and covert operations. The next chapter gives some insight on the utilisation of social media in the fight against crime on an international level.

CHAPTER 6
DATA ANALYSIS AND INTERPRETATION

6.1 INTRODUCTION

This research investigated the utilisation of social media by the SAPS in resolving crime. The main objective of the study was to find out how it could be used to investigate and solve crime, and to what extent the SAPS is already using it in its fight against crime. The researcher conducted a qualitative study, and collected data, using focus group discussions and short questionnaires for the target group, namely detectives in the SAPS. Literature consulted was in the form of printed material, online publications and accredited journals. The information obtained was processed and analysed. Twenty-nine (29) learners participated in the research project. They were from Namibia and South Africa (the Independent Police Investigative Directorate - IPID, Mpumalanga, Gauteng, the Free State, Kwazulu Natal, Western Cape, Eastern Cape, Head Office, North West and Limpopo). Results from the study are discussed in this chapter.

6.2. DATA OBTAINED FROM TARGET GROUPS

The research was qualitative, and the study descriptive, as it entailed the description of social media. It was explorative, because it investigated the use of social media as a tool to assist the SAPS in solving crime. The researcher used primary as well as secondary data. The researcher consulted books, newspapers, the Internet, articles, and other recent relevant publications and documents, for the literature review. Group discussions were conducted, and questionnaires distributed, to obtain primary data from the persons participating in the research.

The researcher used the information to investigate whether social media is used as a tool to investigate and solve crime. Focus groups were arranged. The target group was detectives on training at SAPS Academy, Paarl. They were selected because they were specifically tasked to investigate crime. The sample was randomly chosen, and consisted of detective commanders attending training

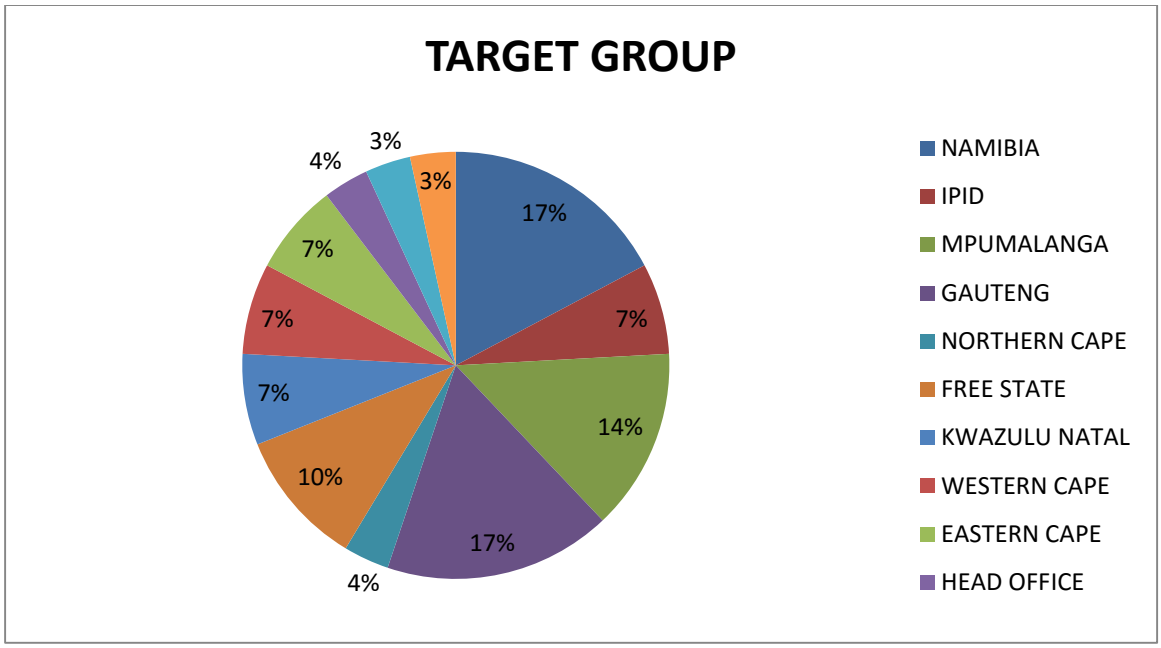
programmes at the time. They fulfilled the criteria, because all of them had experience in the investigation of crime. They were representatives from all over the country, and not only from one area.

The researcher explained the topic, the reason for the research, and also the rules, to the learners. They were requested to write their opinions and answers on a questionnaire provided by the researcher. They could participate anonymously, as this was conducive to openness regarding their knowledge of the Internet and social media.

The researcher had four focus group interviews with four groups of learners, between November 2014 and June 2015:
Session 1 – 2 December 2014: 12 learners at the session, of whom only six completed the questionnaire.
Session 2 – 10 February 2015: Six learners – one participant for IPID and five detectives.
Session 3 – 10 February 2015: – Six learners – six detectives.
Session 4 – 4 June 2015: 11 learners - five from Namibia, one learner from IPID and six detectives from all over South Africa.

The following 29 members participated in the research project. They were : Namibia – 5 (17%), IPID – 2 (7%) , Mpumalanga – 4 (14%), Gauteng – 5 (17%), Northern Cape – 1 (3.5%), the Free State – 3 (10%), Kwazulu-Natal – 2 (7%), the Western Cape – 2 (7%), the Eastern Cape – 2 (7%), Head Office – 1 (3.5%), North West – 1 (3.5%) and Limpopo – 1 (3.5%).

Illustration 6.1: Target group: participants as per province.



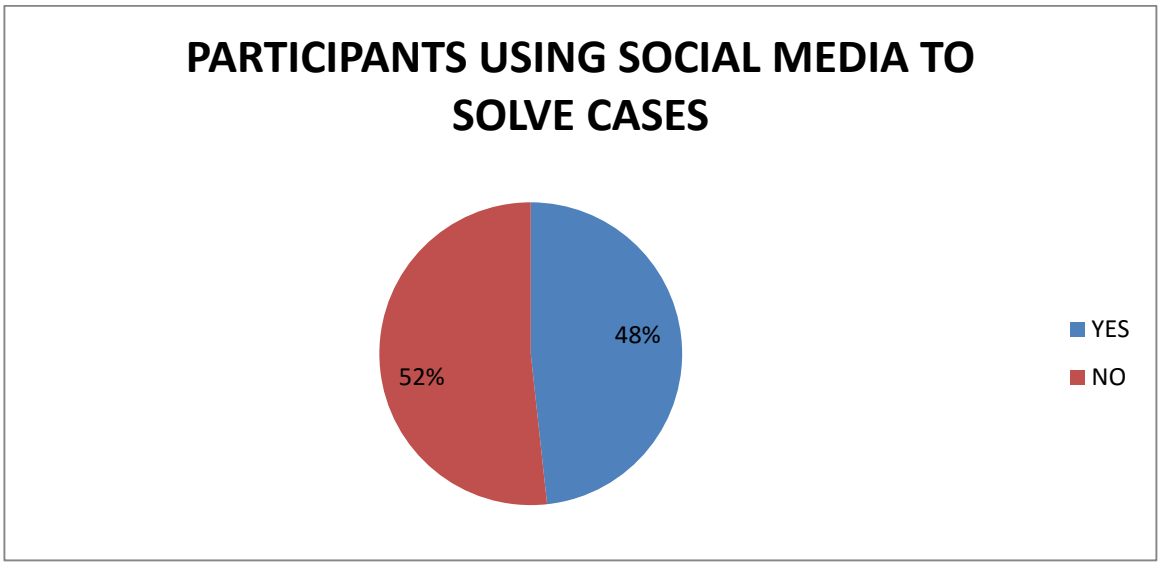
The five members from Namibia were included, to give some perspective of another country.

The researcher found that the topic was quite new for most of the learners. Most of the participants were familiar with WhatsApp, and had used the Section 205 process in their investigations, where they tracked and traced cell phones between towers and with the cell numbers, or obtained data from service providers to use in their cases. One participant indicated that he used the Internet on a daily basis during his investigations. None of the learners had dealt with retrieving evidence from, for example, Facebook, and could therefore not explain how this process, and the legal aspect, worked. One learner in the discussion group informed the group that Interpol must be contacted for information from international service providers. He had not dealt with the process, and could not give specific step-by-step information. Learners from Namibia indicated that they are not using such a process themselves – their specialised units investigate technology-related crimes.

Results from the questionnaires were as follows:

1. Have you ever had cases that you investigated where social media was used to solve a specific crime? Yes – 14 (48%), No – 15 (52%).

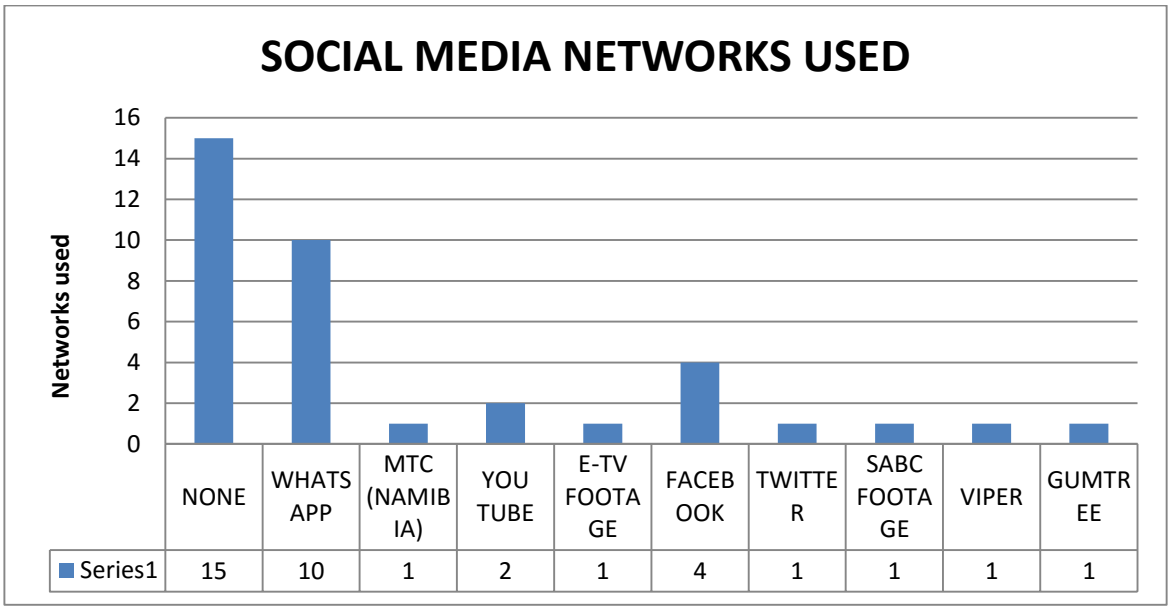
Illustration 6.2: Participants using social media to solve cases.



2. If yes, which social network (e.g. Facebook/Twitter/You Tube/WhatsApp/MixIt/any other) played a role?
   WhatsApp – 10 (34,48%) / MTC (Namibia) – 1 (3,45%) / YouTube – 2 (6,9%) / E-TV Footage – 1 (3,45%) / Facebook – 4 (13,79%) / Twitter – 1 (3,45%) / SABC footage – 1 (3,45%) / Viper – 1 (3,45%) / Gumtree – 1 (3,45%).
   WhatsApp was used the most.

   It can be noted that some learners indicated more than one social media network being used. The conclusion can also be formed that the figures for WhatsApp and Facebook separately, are not significant, but when they are combined, equal 48% – which makes it more significant.

Illustration 6.3: Social media networks used.

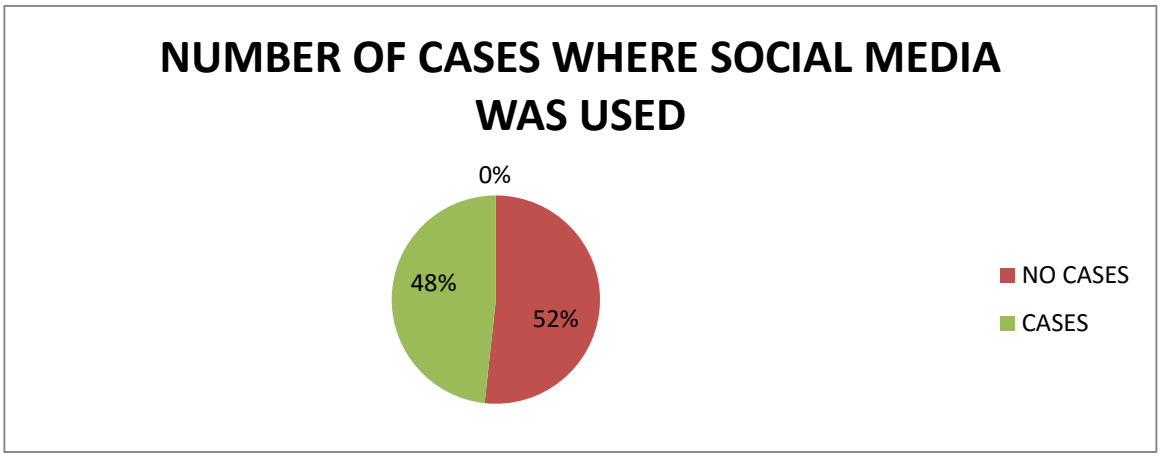


3. Can you elaborate/explain how the social media networks contributed to your case investigation?

   Fifteen (15) (52%) participants never investigated any cases using social media.

   Fourteen (14) (48%) learners elaborated on their cases in broad terms: 13 learners stated that they used evidence from cell phones in their investigations, and one (1) participant indicated that Gumtree (Internet) and Facebook (Internet) were used during investigations. One participant explained that in a case he had where evidence was downloaded on YouTube, he and his team tracked down a person who had taken the original footage, and presented the cell phone used, to court.

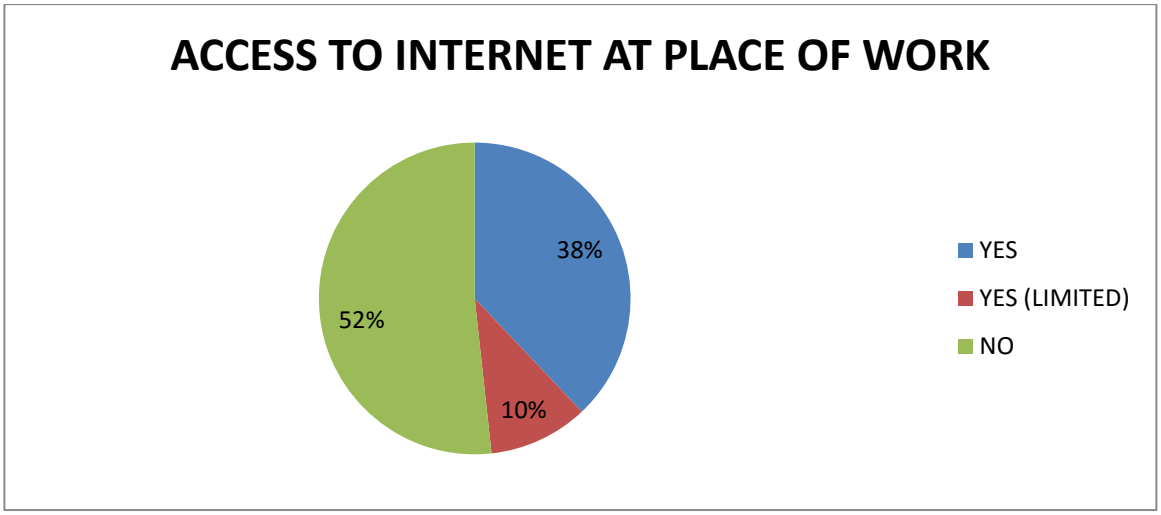
Illustration 6.4: Number of cases where social media was used.



4. Do you have access to the Internet at your place of work?

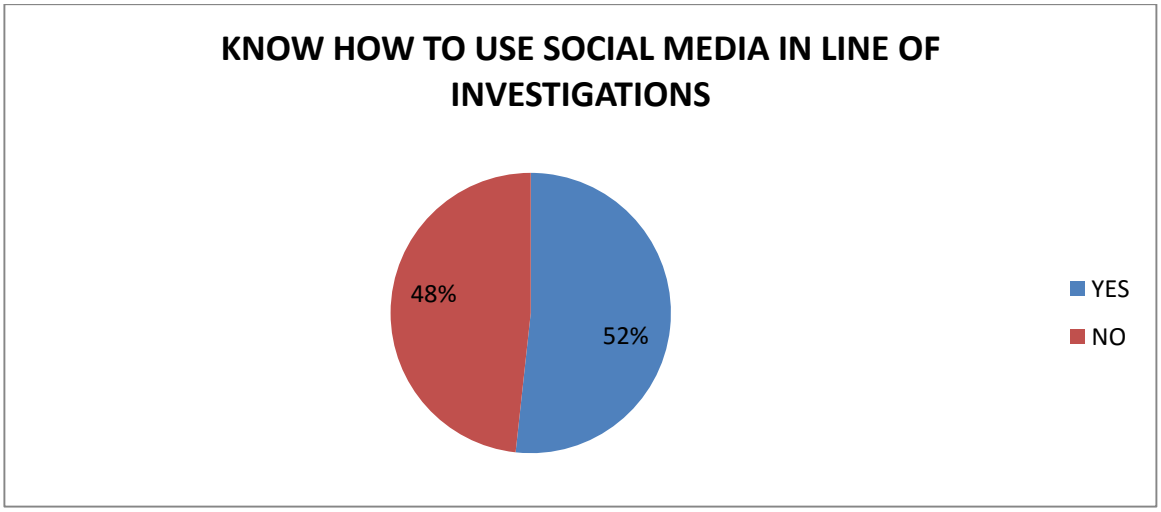
   Yes – 11 (38%), Yes, limited access – 3 (10%), No – 15 (52%).

Illustration 6.5: Number of participants having access to the Internet at their place of work.



5. Do you know how to use Facebook/Twitter/YouTube/WhatsApp/MixIt or any other social media networks, in the line of your investigations?
   Yes – 15 (52%), No – 14 (48%).

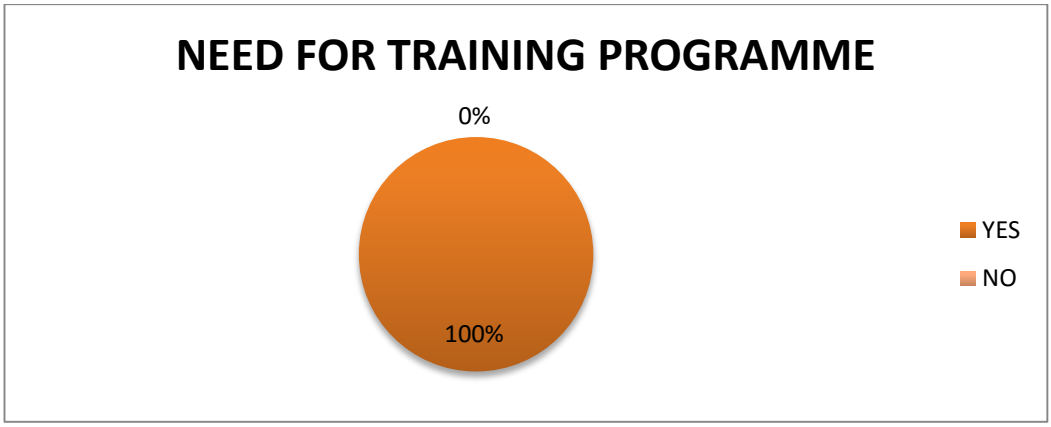
Illustration 6.6: Number of participants indicating that they know how to use social media in the line of their investigations.



Most learners indicated that they knew how to use social media in their investigations. This is probably because they knew how to use WhatsApp and the official investigative processes with regard to cell phones, but were not necessarily familiar with social media networks – for example, Facebook. Nobody could explain the process with regard to networks such as Facebook, and how to obtain evidence from it.

6. Would you like to attend a programme that teaches you how to use social media as a tool to solve cases in your line of work?
   Yes – 29 (100%), No – 0 (0%).

Illustration 6.7: Number of participants indicating that they have a need for a training programme.



6.3 SUMMARY

The main objective of this study was to find out how social media could be used to investigate and solve crime, and to what extent the SAPS is already using it in its fight against crime.

In the study conducted, the researcher found that the detectives interviewed could not share the exact process of obtaining information from social media administrators. Although learners indicated that they knew how to use social media in their investigations, the researcher could not substantiate it with feedback during the discussion groups. Some indicated that they had experience with it in their cases, but not to the extent to prove that it was being used by detectives.

The study further revealed that specialised units were using the Internet and resources, but not the average detective at station level. Some members have no (or limited) access to the Internet at their offices. WhatsApp is a popular network utilised by the SAPS to obtain information in cases.

In Chapter 2, the researcher suggested that detectives in the SAPS needed training in the field. All the participants in the focus groups indicated that they would want to attend available training in technology.

CHAPTER 7
FINDINGS, RECOMMENDATIONS AND CONCLUSION

7.1. INTRODUCTION

The researcher conducted research on social media. The aim was to determine whether it could be used to investigate and solve crime, and to what extent the SAPS was already using it in its fight against crime. The researcher furthermore conducted a qualitative study, and collected data using focus group discussions and short questionnaires for the target group, namely detectives in the SAPS. Literature consulted included hard-copy sources, online publications and accredited journals. The information obtained was processed and analysed. This report, with findings and recommendations, was then compiled.

In Chapter 1, section 1.4, the research objectives were stated as follows:

- to provide a general orientation, as done in Chapter 1, where the background to the study, and the reasons why it was deemed necessary to conduct research on this topic, were discussed.
- to discuss the research methodology, as done in Chapter 2, where the questions of which method was used to achieve goals, aims and objectives, were answered. This chapter dealt with what was to be studied.
- to explain the role of social media, as done in Chapter 3, where the role of social media was discussed. The chapter provided information about its users, and possible advantages and disadvantages for the SAPS.
- to discuss the legal mandate – international experiences, as done in Chapter 4, which elaborated on some of the existing and developing legislation applicable to social media and its execution in the United States (U.S.) and the United Kingdom (UK). It also explains some processes in place, which are applicable to the use of social media in an international policing environment.
- to discuss the local legal mandate, as done in Chapter 5, which gave insight about existing and developing legislation applicable to social media and its

execution, in South Africa. It also explained some processes in place that are applicable to the use of social media in a policing environment.

- to do data analysis and interpretation, as done in Chapter 6, in which the data provided by participants was analysed and interpreted.
- to present findings, make recommendations, and reach conclusions, as done in this chapter.

In Chapter 1, section 1.5, the following research questions were asked:

- Is the SAPS utilising social media in the investigation of crime?
- Does the SAPS access it to find missing persons?
- How far does a person's right to privacy protect him/her?
- What is social media?
- Who uses social media?
- Which legislation is applicable to the Internet and social media?
- Are there guidelines to use social media as a tool to solve crime?

7.2. SPECIFIC FINDINGS

Findings to these questions are as follows:

- Is the SAPS utilising social media in the investigation of crime?

Specialised units, such as the ECU at the Division Crime Intelligence, are using social media in their investigations. The Inkwazi System, the so-called Section 205 process, and proactive investigations by specialised units, indicate that the SAPS is utilising social media in the investigation of crime. The SAPS is also using social media to find suspects and missing persons. (See Chapter 5, sections 5.3.1, 5.5.1, 5.8.1, 5.10 and 5.17 of this report).

- Does SAPS access social media to find missing persons?

Yes, as indicated above. (Chapter 5, section 5.10 of this report)

- How far does a person's right to privacy protect him/her?

Section 14 of the Constitution protects privacy, and Section 16 provides for the Freedom of Expression. Section 32 provides for rights to specific information.

Section 36 is about the Limitation of Rights (South Africa, 1996a) – an individual's rights are protected but with limitations. Individual must always be aware of what they says/write/publicise, and to whom, when and where. There is proper legislation in place to protect the individual, a public person and companies. When a person posts information on the Internet (including social media pages) it is deemed as published content. There is a difference between email content, an Internet blog (accessed not restricted) and social network sites (for example, Facebook) whereby privacy is not secured. Users are allowed to read posts by other users even when they are not taking part in the discussions (Chapter 5, section 5.11).

- What is social media?

Social media is the platform where millions of people communicate through a digital medium. Communication takes place through social networks, blogs, mobile applications and other. They interact socially and on a business level. Some types of social media are the following: social networking (for example, Facebook, Myspace, Bebo, Orkut, BlackPlanet, MiGente, AsianAve); blogging (for example, Blogger, WordPress, TypePad, Xanga); microblogging (for example, Twitter); IM and Texting (for example, Google Chat, Yahoo Messenger, Skype, texting using mobile phones/devices); Photo Sharing (for example, Flickr, Photobucket, Picasa, Snapfish); Video Sharing (for example, YouTube), Wikis (for example, Wikipedia, Wikinews) and Online Multiplayer Games/Virtual Worlds (for example, World of Warcraft, Second Life). (See Chapter 3, section 3.2 and 3.3.1).

- Who uses social media?

Research shows that younger adults use social media more than older adults do, both in South Africa and internationally. Criminals, gangs and terrorists are also using it. The SAPS and international police departments use social media, and the Internet, to investigate and fight crime and gather intelligence. The SAPS has Twitter and official Facebook pages where information can be found or posted. (See Chapter 3, section 3.3.2).

- Which legislation is applicable to the Internet and social media?

South African and international legislation are in place. Some writers are, however, of the opinion that legislation is not adapting and developing at the same pace as the Internet and criminal activities. In South Africa, cybercrime is legislated by the ECTA. South African legislation applicable is the following:

YEAR	NUMBER	ACT
1965	Act 25 of 1965	Civil Proceedings Evidence
1977	Act 51 of 1977	The Criminal Procedure
1983	Act 57 of 1983	Computer Evidence
1987	Act 98 of 1987	Copyright
1992	Act 125 of 1992	Copyright Amendment
1992	Act 127 of 1992	Interception and Monitoring Prohibition
1993	Act 194 of 1993	Trademarks
1995	Act 68 of 1995	South African Police Services
1996	Act 33 of 1996	National Gambling
1996	Act 65 of 1996	Films and Publications
1996	Act 103 of 1996	Telecommunications
1996	Act 108 of 1996	The Constitution of the Republic of South Africa
1998	Act 67 of 1998	Open Democracy Bill
1999	Act 4 of 1999	Broadcasting
1999	Act 34 of 1999	Films and Publications Amendment
2000	Act 2 of 2000	The Promotion of Access to Information (PAIA)
2000	Act 13 of 2000	The Independent Communications Authority of South Africa (ICASA)
2002	Act 25 of 2002	The Electronic Communications and Transactions (ECTA)
2002	Act 70 of 2002	The regulation of Interception of Communications and Provision of Communication-Related Information (RICA)
2005	Act 36 of 2005	The Electronic Communications (ECA)
2009		The Protection of Personal Information Bill (PPI)
		Common Law

The following Acts were mentioned in Chapter 5:

YEAR	NUMBER	ACT	HEADING
1988	Act 45 of 1988	Law of Evidence Amendment Act	Hearsay and admissibility of evidence
1996	75 of 1996	International Cooperation in Criminal Matters (ICCMA), also referred to as the Cooperation Act	Search and seizure of electronic evidence in criminal cases
1996	Act 118 of 1996	Domestic Violence	Cybercrime & Cyber stalking
2004	Act 7 of 2004	National Gambling	Cybercrime & Online gambling
2008	Act 68 of 2008	Consumer Protection	Cybercrime & Phishing

(See Chapter 4 for international legislation).

(Chapter 4 and Chapter 5)

- Are there guidelines to use social media as a tool to solve crime?

Different social media networks have their own guidelines for law enforcement – for example, Facebook, Twitter, Google and YouTube have specific guidelines that must be followed by law enforcement authorities. They will only react when receiving subpoenas or court orders, or when receiving emergency disclosure requests, in accordance with relevant U.S. law. Other countries may apply for information, but these requests will be treated according to MLATS. Google will also provide information when there are joint investigations between the U.S. and other law enforcement agencies.

One of the processes followed by the SAPS is the so-called Section 205 – in terms of Section 205 of the CPA, whereby a local service provider can be requested to present evidence from cell phones.

Canada also has specific processes, guidelines and procedures in place.

There are specific guidelines in place, with regard to forms and requests, subpoenas, search warrants, ECPA court orders, Wiretap and Pen Register, and Trap and Trace. Google and iCloud l provide data through legal processes. There are also specific rules in place when applying for the extraction of data from Find My Iphone and Data from Pass Code Locked iOs Devices.

Training in social media is available for police officers working in specialised units, but not for detectives at station level. (See Chapter 4, sections 4.4 and 4.5, and Chapter 5, sections 5.3, 5.4 and 5.5).

7.3. GENERAL FINDINGS

Findings on target group: As indicated in the previous chapter (Chapter 6), the researcher found, during the focus group interviews, that the topic was quite new to most of the participants in the study. Most participants were familiar with WhatsApp, and had used the Section 205 process in their investigations, where they tracked and traced cell phones between towers and with cell numbers, or obtained data from the service providers to use in their cases. One participant indicated that he used the Internet on a daily basis for his investigations. None said that they ever retrieved evidence from Facebook or other social media networks. They could not explain how the process and the legal aspects worked.

The following questions were posed to the learners:

- Have you ever had cases that you investigated where social media were used to solve a specific crime?

  Yes – 14 (48%), No – 15 (52%).

  More than half the learners indicated that they had used social media to solve crimes.
- If yes, which social media networks (e.g. Facebook/Twitter/You Tube/WhatsApp/MixIt/any other) played a role?

WhatsApp – 10 (34,48%) / MTC (Namibia) – 1 (3,45%) / YouTube – 2 (6,9%) / E-TV Footage – 1 (3,45%) / Facebook – 4 (13,79%) / Twitter – 1 (3,45%) / SABC footage – 1 (3,45%) / Viper – 1 (3,45%) / Gumtree – 1 (3,45%).

WhatsApp was used most. It can be noted that some learners indicated more than one social media network being used) The conclusion can also be made that the figures for WhatsApp and Facebook separately are not significant, but when they are combined, equal 48%, which makes it more significant.

- Can you elaborate/explain how social media networks contributed to your case?
  More than half the learners had never had any cases where they used social media. The rest of the learners elaborated on their cases in broad terms. A total of 13 learners stated that they had used evidence from cell phones in their investigations. One learner indicated that Gumtree (Internet) and Facebook (Internet) were used during investigations. One learner explained that in a case where evidence was downloaded on YouTube, he and his team tracked down a person who took the original footage, and they then presented the cell phone used to court.
- Do you have access to the Internet at you place of work?
  Yes – 11 (38%), Yes, limited access – 3 (10%), No – 15 (52%).
  More than half the learners did not have any access to the Internet, three learners had limited access, and 11 learners had access.
- Do you know how to use Facebook/Twitter/YouTube/WhatsApp/MixIt or any other social media networks in the line of your investigations?
  More than half indicated 'yes'; however, most learners who indicated that they knew how to use social media in their investigations, probably did so because they knew how to use WhatsApp and the official investigative processes with regard to cell phones. Nobody could explain the legal process with regard to networks such as Facebook, and how to obtain evidence from it.
- Would you like to attend a programme that teaches you how to use social media as a tool to solve your cases in your line of work?
  All the learners responded positively.

- Unique operational challenges found in the SAPS are that members do not know how to collect digital evidence, there is a critical shortage of trained experts who can analyse and testify in court about digital evidence, and digital evidence must be handled properly. (See Chapter 5, section 5.7).
- There are cases reported where social media could assist law enforcement with information persons posted on their social media pages. It could provide evidence of crimes, and assist in finding suspects and missing persons. (See examples as per Chapter 4, section 4.8, and Chapter 5, section 5.6).
- There are different kinds of evidence. For the purposes of this research, electronic evidence was investigated. Electronic evidence is either real or documentary evidence – depending on the type of evidence submitted. It can be found on a number of devices, such as portable devices and personal computers. It can be found on social networking sites (for example, Facebook, MySpace, LinkedIn), from ISPs, in chatrooms, on websites and on external storage devices.

  Electronic evidence is admissible in court, under specific circumstances. It must be the best evidence that could be found. The production, presentation in the original form, and authenticity, are vital for it to be admissible in court. The presentation of electronic evidence could be problematic if it is not legitimate and accurate. It could be a difficult process to present it in court, because electronic evidence can be temporarily and easily lost or deleted. It can easily be created, stored, copied, transmitted, tampered with and modified.

  Standard processes in place to collect, preserve and analyse electronic evidence are carried out in line with international standards. It is important for the investigating officer to maintain the chain of custody, to ensure the admissibility of evidence in court. The investigating officer may make use of computer forensic experts for assistance. Internationally, Canada and the UK have proper systems in place, regulated by policies and legislation.

The presentation of electronic evidence can be problematic, because it can be perceived as hearsay evidence. Evidence must have probative value, it must be credible, and a printout must be accurately registered and processed. Computer-generated evidence is admissible, but postings or statements on social media could be evaluated in court, as hearsay. It may be admissible in exceptional circumstances and, according to section 221 of the CPA, in specific situations. In the UK, the procedure is found to be the same: the person creating the evidence must testify in court. The British Criminal Evidence Act 1965 makes provision for documentary hearsay. (See Chapter 4, sections 4.3 and 4.4, and Chapter 5, section 5.8 and 5.15).

- Both national and international law seek to protect the individual against unlawful intrusion into their private space. Legislation also enables law enforcers to obtain unlawful information/publications/communications, and make sure that perpetrators can be arrested and brought to justice. (See chapters 4 and 5).
- Different software used by police departments in their fight against crime are Caboodle, Digital Sandbox, Virtual Commander, everyday event management software, Geofencing, Snap Trends, Police Blotter Blogs, The Digital "Wanted Poster", Anonymous E-Tipsters, Social Media Stakeout, Thwarting Thugs in the Social Space, Tracking and Informing with Twitter, software used for triangulation between cell towers, GPS tracking, and the observation of individuals, through CCTV and software, to do voice recordings via a person's cellphone. (See Chapter 4, sections 4.6 and 4.7).

7.4. RECOMMENDATIONS

- International law enforcement agencies, and specialised units such as the ECU at the Division Crime Intelligence, are using social media in their investigations. The SAPS could expand its use of social media in the investigation of crime by benchmarking with international law enforcement agencies. Such processes should then be adjusted according to specific needs, and implemented accordingly.

- The SAPS is using social media to find missing persons. SOPs should be included in the training material.

- Users of social media should always be aware when they are waiving their right to privacy and their right to freedom of expression. Awareness campaigns on official SAPS social media platforms could be used for this purpose. Users could be informed of their rights, and also be made aware of the boundaries, as well as their liabilities. This information should be made known to members of the public, as well as SAPS members. Detectives at station level should have adequate knowledge about the subject, to ensure that they investigate crime properly.

- Millions of people are using social media. The SAPS could appoint members to monitor a number of platforms, such as social networks, blogs, mobile applications and others. Detectives should be introduced to these digital media through training programmes, information sessions, seminars and internal SAPS communication channels.

- Detectives should know who the users of social media are. They should use this knowledge to their advantage in the investigation of crimes. Benchmarking with other law enforcement agencies that also use social media, should take place, and their SOP's be implemented where possible.

- It was found that some writers are of the opinion that legislation is not adapting and changing at the same pace as the Internet and criminal activities; nonetheless, applicable legislation does exist. All SAPS members should be knowledgeable about existing legislation. Members should be introduced to the legislation through training programmes, information sessions, seminars and internal SAPS communication channels.

- Guidelines that are in place to use social media as a tool to solve crime, should be simplified. Step-by-step guidelines should be developed for SAPS members to use as a tool in the investigation and solving of crimes. Benchmarking could

be done with law enforcement agencies in Canada, the U.S. and the UK, to investigate their processes and find out how they could be adjusted and implemented in the SAPS.

- The gap between the training of members in specialised units, and detectives at station level, should be addressed. Training must be expanded to members first on crime scenes. Proper training material should be developed for such members. Members of specialised units could assist with development and training, because they deal with social media and crime on the Internet.

- Some participants indicated that they did not have access to the resources that would assist them in accessing the Internet and social media. Procurement and distribution policies should address this need. Funds should be budgeted for, and resources allocated.

- It was found that learners want to attend training programmes teaching them how to use social media as a tool in their line of work. Training material should be developed for detectives at station level. It could be added to the existing curriculum for the training of these detectives in the SAPS.

- It was found that members do not know how to deal with digital evidence, and that there is a critical shortage of trained experts. Training should address the challenges with regard to digital forensics.

- Cases were reported where social media could have assisted law enforcement in the investigation of crimes. Detectives should know about existing cases. Knowledge of how these investigations were executed could assist them in the investigation of their own cases.

- Various software exists that international law enforcement agencies are using in their fight against crime. Benchmarking should be done with law enforcements agencies in Canada, the U.S. and the UK, to see which programmes they are using. It could then be utilised by the SAPS as well.

- Suggestions for further research: The European Commission has proposed that there be a legal "right to be forgotten". Such a right would mean that Internet users could request that embarrassing or unwanted online content be permanently deleted from social networking sites such as Facebook (European Commission, 2015). This ruling might have an effect on the availability of information for law enforcement.

- Facebook is planning to open an office in Johannesburg, South Africa. This would then imply that investigating officers could apply the Section 205 process to obtain information from a local service provider. The process of investigation should, however, be further researched.

7.5. CONCLUSION

The researcher conducted extensive research on social media. The main objective was to find out how it could be used to investigate and solve crime and to what extent the SAPS is already using it in its fight against crime. A qualitative study was done, and data collected focused on group discussions and short questionnaires for the target group – namely, detectives in the SAPS. Literature consulted included hard-copy sources, online publications and accredited journals. Both personal and email interviews were conducted. The information obtained was processed and analysed. Random sampling was used, by asking a number of learners on the detective learning programme at SAPS Academy, Paarl, to participate. Participation was voluntary, and data was presented anonymously.

The findings suggest that the SAPS is utilising social media in the fight against crime, but at a specialised level, and not by detectives at station level. The SAPS is using it to find suspects and missing persons. Individuals have the right to privacy, and are protected by legislation. Posting information on the Internet and social media means that that information has been publicised and that the right to privacy may be forfeited. Social media is a wide communication platform for millions of people. There is specific legislation in place, but there is a widely-held view that legislation is not developing as rapidly as the Internet and crime. There

are guidelines in place for law enforcement officials who need to use social media in their investigations.

It is concluded that detectives at station level do not have sufficient knowledge and lack training in how to use social media to their advantage. They do not have the resources to do so. Proper training and implementation of guidelines are urgently needed.

LIST OF REFERENCES

2013 Survey Results, IACP Center for Social Media. 2013. From: http://www.iacpsocialmedia.org/Resources/Publications/2013SurveyResults.aspx# (accessed 16 June 2014).

About PERF. 2014. From: http://www.policeforum.org/about (accessed 17 June 2014).

Ajam, K. 2013. *SA man wins Facebook slander case - Crime & Courts | IOL News* | From: http://www.iol.co.za/news/crime-courts/sa-man-wins-facebook-slander- case-1.1463004 (accessed 17 July 2013).

Babbie, E.R. 2013. *The practice of social research*. 13th international edition. Belmont, CA: Wadsworth.

Bekker, P.M., Geldenhuys, T.G., Joubert, J.J., Swanepoel, J.P., Terblanche, S.S. & Van der Merwe, S.E. 2003. *Criminal procedure handbook*. 6th edition. Lansdowne: Juta.

Berg, B.L. 2004. *Qualitative research methods for the social science.* 3rd edition. London: Allyn & Bacon.

Bezuidenhout, N. 2013. *Cape gang shootout seen on YouTube*. IOL News, 24 July. From: http://www.iol.co.za/news/crime-courts/cape-gang-shootout-seen-on-youtube-1.1551812#.UiGRWyQaL4Y (accessed 31 August 2013).

Billboard at SAPS Academy Paarl (accessed 15 September 2014).

Boca Raton Police Department. 2014a. [Police Blotter Blog]. From: http://www.ci.boca-raton.fl.us/police/TopStories/blotter.pdf (accessed 14 October 2014).

Boca Raton Police Department. 2014b. [Web page/Home page]. From: http://www.ci.boca-raton.fl.us/police/index.shtm (accessed 14 October 2014).

Boyd, D.M. & Ellison, N.B. 2007. *Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication*, 13(1), October: 210-230 From: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (accessed 20 June 2013).

Boynton Beach Police Department. 2014. T*he Boynton Beach Police Department. Facebook Page.* From: https://www.facebook.com/boyntonbeachpolice (accessed 14 October 2014).

Braga, A.A., Flynn, E.A., Kelling, G.L. & Cole, C.M. 2011. *Moving the Work of Criminal Investigators towards Crime Control.* New Perspectives in Policing. Harvard Kennedy School. Program in Criminal Justice Police and Management. National Institute of Justice. Washington, DC (District of Columbia), United States: United States Department of Justice Office of Justice programs. March 2011:1-38.

Broadcasting Act … see South Africa. 1999a.

Brown. G. 2015. *Rape suspect caught due to Facebook post*. WREG, 14 August. From: http://wreg.com/2015/08/14/rape-suspect-caught-due-to-facbook-post/ (accessed 6 September 2015).

Brynard, P.A. & Hanekom, S.X. 2013. *Introduction to research in management-related fields*. 2nd edition. Pretoria: Van Schaik.

Bulmer, W. (wbulmer@kinsa.net). 2014. Research – Social media. Private email message to L. Turck (19 September 2014).

Casey, E. 2002. Error, uncertainty, and loss in digital evidence. *International journal of digital evidence,* 1(2). Summer 2002. From: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf (accessed 13 October 2014).

Civil Proceedings Evidence Act … see South Africa. 1965.

Cohen, L.S. 2010*. 6 Ways Law Enforcement Uses Social media to Fight Crime. Social Media*. From: http://mashable.com/2010/03/17/law-enforcement-social-media. (accessed 10 June 2010).

Collins Cobuild Essential English Dictionary. 1989. s.v. "social". London: Collins.

Collins Thesaurus A-Z Discovery Dictionary. 2005. s.v. "social". Glasgow: HarperCollins Publishers.

Computer Evidence Act … see South Africa. 1983.

Computer Misuse Act … see Laws of the United Kingdom. 1990.

Constitution of the Republic of South Africa … see South Africa. 1996a.

Consumer Protection Act … see South Africa. 2008.

Copyright Act… see South Africa. 1987.

Copyright Amendment Act … see South Africa. 1992a.

Criminal Evidence Act … see Laws of the United Kingdom. 1965.

Criminal Justice and Immigration Act … see Laws of the United Kingdom. 2008.

Criminal Procedure Act … see South Africa, 1977.

Cronjé, F. 2013. *Promotion of Access to Information Act of 2000 (PAIA)*. From: http://www.cyberlawsa.co.za/paia.html (accessed 8 June 2013).

Data Protection Act … see Laws of the United Kingdom. 1998a.

De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grass roots: for the social sciences and human service professions*. Fourth edition. Pretoria: Van Schaik.

Dean, G., Bell, P. & Newman, J. 2012. The dark side of social media: review of online terrorism. From: http://www.pakistansocietyofcriminology.com/publications/2012_08_10_4110.pdf (accessed 29 March 2016).

Dempsey, J.S. & Frost, L.S. 2012. *An Introduction to policing*. 6th international edition. New York: Delmar/Cengage Learning.

Dolley, C. 2011. *Facebook rapist' caught with kidnapped woman*. From: http://www.iol.co.za/news/crime-courts/fb-rapist-caught-with-kidnapped-woman-1.1153754#.Vew_mZoVj4Y (accessed 6 September 2015).

Domestic Violence Act … see South Africa. 1996b.

Duggan, M. & Brenner, J. 2013. *The demographics of social media users — 2012*. From: http://pewInternet.org/Reports/2013/Social-media-users.aspx (accessed 9 June 2013).

Ebersöhn, M. (planning.research@saps.org.za). 2013. Social Media and Crime Prevention. Private email message to L. Turck (23 September 2013).

Ebersöhn, M. (planning.research@saps.org.za). 2014. Social Media and Crime Prevention. Private email message to L. Turck (5 May 2014).

Ebizma. 2013. Top 15 Most Popular Social Networking Sites | June 2013. From: http://www.ebizmba.com/articles/social_-networking-websites (accessed 9 June 2013).

Electronic Commerce (EC Directive) Regulations … see Laws of the United Kingdom. 2002.

Electronic Communication and Transactions Act … see South Africa. 2002a.

Electronic Communications (ECA) Act … see South Africa. 2005.

Electronic Communications Privacy Act … see United States. 1986a.

EU Telecoms Data Protection Directive … see Laws of the United Kingdom. 1999.

European Commission. 2015. *Fact sheet on the "Right to be forgotten" ruling. (C131/11)*. From: http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf (accessed 9 September 2015).

Evans, J. & Wicks, J. 2015. *Viral video shows vigilantism, not xenophobia-police.* News24, 11 April. From: http://www.news24.com/SouthAfrica/News/Viral-video-shows-vigilantism-not-xenophobia-police-20150411 (accessed 15 June 2015).

Everett, W. 2011. *Social Networking & Labour Law. Presentation at the 2011* CCMA COMMISSIONERS INDABA. "On the Road a-Changing . . ." Lagoon Beach Hotel, 8 – 9 December 2011. From: http://www.ccma.org.za/UploadedMedia/P6%20SOCIAL%20NETWORKING%20AND%20EMPLOYMENT%20LAW.pdf (accessed 14 October 2014).

Facebook. 2015. *South African Police Service (SAPS Official Page) (Facebook)*. Facebook, 5 September. From: https://www.facebook.com/SAPoliceService (accessed 5 September 2015).

Facebook helps solve 45-year-old case [24 April]. 2013. From: http://www..news24.com/news24/World/News/Facebook-helps-solve-45-year-old-case-20130424 (accessed 8 June 2013).

Facebook screenshot (accessed 5 August 2014).

Fadilpašić, S. 2015. *Facebook to open office in South Africa*. itportal, 30 June. From: http://www.itproportal.com/2015/06/30/facebook-to-open-office-in-south-africa/ (accessed 6 September 2015).

Films and Publications Act … see South Africa. 1996c.

Films and Publications Amendment Act … see South Africa. 1999b.

Fin24. 2014. *Facebook hits 100 million mark in Africa*. Fin24tech. Reuters. Fin24, 8 September. From: http://www.fin24.com/Tech/Mobile/Facebook-hits-100-milion-mark-in-Africa (accessed 8 September 2014).

Fourth Amendment … see United States. 1791.

Freedom on the Net, South Africa. 2012. From: http://www.freedomhouse.org/report/freedom-net/2012/south-africa (accessed 18 July 2013).

Friendship 2.0 - MWeb research report. 2009. From: http://www.mweb.co.za/services/friendship/downloads/Friendship%202.0%20presentation%20for%20Microsite.pdf (accessed 19 July 2013).

Gereda, S.L. [**s.a**.] *The Electronic Communications and Transactions Act*. From: http://thornton.co.za/resources/telelaw12.pdf (accessed 5 September 2015).

Google Playstore. Application available on android operating system cell phones (accessed 4 September 2014).

Google Playstore screenshot (accessed 4 September 2014).

Governments demanded 38K FB users data. 2013. From: http://www.news24.com/Technology/News/Governmentsdemanded-38K-FB-users-data-20130827 (accessed 4 September 2013).

Govt requests Facebook, Google user info. 2013. *News24*, 4 September. From: http://www.news24.com/SouthAfrica/News/Govt-requests-Facebook-Google-user-info-20130904 (accessed 4 September 2013).

Hagy, D.W. 2007. *Investigations Involving the Internet and Computer Networks. Special report - National Institute for Justice, NCJ 210798*. January 2007. Washington, DC (District of Columbia), United States: United States Department of Justice Office of Justice Programs.

Henning, E., Van Rensburg, W. & Smit, B. 2004. *Finding your way in qualitative research*. Pretoria: Van Schaik.

Howard, P.N., Duffy, A., Freelon, D., Hussain, M., Mari, W. & Mazaid, M. 2011. *Opening Closed Regimes: What was the Role of Social Media during the Arab Spring*? Working paper 2011.1. Project on Information Technology & Political Islam pITPI.

Human Rights Act … see Laws of the United Kingdom. 1998b.

INCSR treaties and agreements report. 2012. *2012 International Narcotics Control Strategy Report (INCSR).* Bureau of International Narcotics and Law Enforcement Affairs. Report published on 7 March 2012. From: http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm (accessed 27 September 2014).

Independent Communications Authority of South Africa (ICASA) Act … see South Africa. 2000a.

Information for Law Enforcement Authorities | Facebook. 2013. From: https://www.facebook.com/safety/groups/law/guidelines/ (accessed 20 May 2013).

Interception and Monitoring Prohibition Act … see South Africa. 1992b.

International Cooperation in Criminal Matters (ICCMA), Act … see South Africa. 1996d.

Interpol. 2015a. *FAQs*. From: http://www.interpol.int/FAQs (accessed 15 June 2015).

Interpol. 2015b. *Member countries*. From: http://www.interpol.int/Member-countries/Africa/South-Africa (accessed 15 June 2015).

Interpol. 2015c. *Overview*. From: http://www.interpol.int/About-INTERPOL/Overview (accessed 15 June 2015).

Joubert, C. 2001. *Applied law for police officials*. 2nd edition. Lansdowne: Juta Law.

Kempen. A. 2015a. 2015. Dealing with Cyberspace challenges. *Servamus,* 108(3):18-20, March.

Kempen. A. 2015b. 2015. Tackling cybercrime and electronic crime in South Africa - The Electronic Crime Unit - Part 1. *Servamus*, 108(3):21-23, March.

KINSA. 2015. *Expanding our global footprint*. From: http://kinsa.net (accessed 15 June 2015).

Lambrechts, D. 2015. Correct procedure to be followed by South African authorities when it receives a request for assistance in criminal matters from abroad - *Tulip Diamond FZE vs Minister of Justice and Constitutional Development and Others* 2013 (2) SACR 433 (CC). *Servamus*, 108(3):67-69, May.

Latib, B.O. & Thuynsma, L. 2013. *Infringement of privacy*. WebberWentzel, 30 April. From: http://www.webberwentzel.com/wwb/content/en/ww/ww-in-the-news?oid=44187&sn=Detail-2011&pid=32749 (accessed 13 October 2013).

Lautier, J. 2013. *Southern Africa and cyber security*. Edition Africa Conflict Monthly Monitor | Consultancy Africa Intelligence (Pty) Ltd. July 2013. From: http://search.sabinet.co.za/WebZ/Authorize?sessionid=0:autho=fulltext:password=txetlluf&/AdvancedQuery?&next=images/ejour/acmm/acmm_jul_2013_a21.pdf (accessed 4 October 2014).

Law of Evidence Amendment Act … see South Africa. 1988.

Leedy, P.D. & Ormrod, J.E. 2014. *Practical research: planning and design*. Tenth edition. Harlow, Essex: Pearson Education.

Legal Process Guidelines. 2014. [Version dated 17 September 2014]. From: http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (accessed 19 September 2014).

Lehasa, K.C. 2008. *Factors influencing output in the four (4) year nurse training programme in the Free State Province*. MA dissertation. University of South Africa, Pretoria.

Lesame, S., Mbatha, B. & Sindane, S. 2011. *New media in the information society.* Cape Town: Van Schaik.

Lloyd, I.J. 2011. *Information technology law*. 6th edition. Oxford: Oxford University Press.

Man kills wife, posts photo on Facebook. 2013. From: http://www.news24.com/World/News/Man-kills-wife-posts-photo-on-Facebook-20130809 (accessed 9 August 2013).

Man targeted young girls on BBM, WhatsApp. 2014. From: http://www.news24.com/SouthAfrica/News/Man-targeted-young-girls-on-BBM-WhatsApp-20140804 (accessed 6 September 2015).

Mashiloane, L. 2014. *Piet Pieterse: SAPS intensifies cybercrime battle*. From: http://www.itweb.co.za/index.php?option=com_content&view=article&id=134890 (accessed 5 September 2015.

Mason, S. 2014. *Electronic evidence. Internet newsletter for lawyers*. From: http://www.infolaw.co.uk/newsletter/2014/07/electronic-evidence/ (accessed 13 October 2014).

Matula, S.M. 2013. *Policy gaps and technological deficiencies in social networking environments: Implications for information sharing.* From: http://dx.doi.org/10.4102/sajim.v15i1.521 (accessed 13 October 2014).

Melekian, B.K. & Wexler, C. 2013. *Social media and tactical considerations for law enforcement*. From: http://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/social%20media%20and%20tactical%20considerations%20for%20law%20enforcement%202013.pdf (accessed 15 June 2014).

Milo, D. & Stein, P. 2013. *A practical guide to media law*. Cape Town: LexisNexis.

M-Net. 2013. *Carteblanche*. 24 February. From: http://beta.mnet.co.za/carteblanche/Article.aspx?Id=4680&ShowId=1 (accessed 8 June 2013).

Murray, A. 2010. *Information Technology law*. *The law and society.* Oxford: Oxford University Press.

National Gambling Act … see South Africa. 1996e.

National Gambling Act … see South Africa. 2004.

Navy Command Leadership Social Media Handbook. 2012. Navy Mill: United States Navy.

Ngomane, A.R. 2010. *The use of electronic evidence in forensic investigation.* MA Dissertation. University of South Africa, Pretoria.

Open Democracy Bill Act … see South Africa. 1998.

Opperman, C.P. 2013. *Cyberlaw: Internet law in South Africa*. From: http://www.legalnet.co.za/cyberlaw/index.htm (accessed 8 June 2013).

Orenstein, A. 2012. *Friends, Gangbangers, Custody Disputants, Lend Me Your Passwords.* (Mississippi College Law Review; 2012, Vol. 31 Issue 2, p185-225, 41p. Court Cases: Lorraine v. Markel Am. Ins. Co.; 241 F.R.D. 534, 538) (D. Md. 2007) Available from: http://0-search.ebscohost.com.oasis.unisa.ac.za/login.aspx?direct=true&db=lgs&AN=84200666&scope=site (accessed 13 October 2014).

Osterburg, J.W. & Ward, R.H. 2010. *Criminal investigation: a method for reconstructing the past*. 6th edition. New Providence, NJ: Anderson Publishing.

Oxford Advanced Learner's Dictionary of Current English. 1995. s.v. "social", "media". Oxford: Oxford University Press.

Papadopoulos, S. & Snail, S. (eds.) 2012. *Cyberlaw@SA III The law of the internet in South Africa.* 3rd edition. Pretoria: Van Schaik.

Patzakis, J. 2014. *Overcoming potential legal challenges to the authentication of social media evidence*. From: http://www.x1.com/download/X1Discovery_whitepaper_Social_Media.pdf (accessed 2 October 2014).

Patzakis, J. & Murphy, B. 2011. *Key twitter metadata fields lawyers and ediscovery professionals need to be aware of weblog*. From: http://blog.x1discovery.com/2011/10/06/key-twitter-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of/ (accessed 16 October 2014).

Pen Register and Trap and Trace Statute … see United States. 1986b.

Pieterse, P. 2015. *Presentation on Cybercrime challenges in South Africa at the seminar: Is South Africa geared up for new cyberspace challenges?* From: http://www.issafrica.org/uploads/26-Jan-2015-Cybercrime-seminar-presentationspdf (accessed 18 June 2015).

Police and Criminal Evidence Act … see United Kingdom. 1984.

Police and Justice Act … see United Kingdom. 2006a.

Privacy and Electronic Communication Directive … see United Kingdom. 2003.

Privacy Protection Act … see United States. 1980.

Promotion of Access to Information (PAIA) Act … see South Africa. 2000b.

Protection from Harassment Act … see United Kingdom. 1997.

Protection of Children Act … see United Kingdom. 1978.

Protection of Personal Information Bill … see South Africa. 2009.

Regulation of Interception of Communications and Provision of Communication-related Information Act … see South Africa. 2002b.

Regulation of Investigatory Powers Act … see United Kingdom. 2000a.

Rheeder, J. 2011. *What you say on Facebook can get you fired*. From: http://www.polity.org.za/article/what-you-say-on-facebook-can-get-you-fired-2011-11-07 (accessed 14 October 2014).

Roane, B. 2013. *SAPS website hacked*. From: http://www.iol.co.za/news/crime-courts/saps-website-hacked-1.1520042 (accessed 8 June 2013).

Rogers, R. 2014. *Cyberspace emerges as law enforcement's new battleground*. From: http://www.contracostatimes.com/news/ci_25204778/cyberspace-emerges-law-enforcements-new-battleground (accessed 17 June 2014).

Roos, A. 2012. *Privacy In The Facebook Era: A South African Legal Perspective** (2012:129). The South African Law Journal. (2012) 129: 375-402. From: http://search.sabinet.co.za/WebZ/Authorize?sessionid=0:autho=fulltext:password=txetlluf&/AdvancedQuery?&next=images/ejour/ju_salj/ju_salj_v129_n2_a9.pdf (accessed 4 October 2014).

Schwikkard, P.J., Skeen, A.St.Q., Van der Merwe, S.E. 1997. *Principles of evidence*. Kenwyn: Juta.

Search: ISP List. [s.a.] From: http://www.search.org/resources/isp-list/ (accessed 15 June 2015).

Shaikh, S. 2013. *Digital Identity, Social media and Privacy Law in South Africa: Part One*. Education-copyright.org, 30 January. From: http://education-copyright.org/digital-identity-social-media-and-privacy-law-in-south-africa-part-one/ (accessed 31 August 2013).

SMILE Conference Omaha. 2013. Nebraska, September 24-26. From: http://smileconference.com/ (accessed 19 September 2013).

Social media overview. 2015. *What is social media*? From: http://webcomm.tufts.edu/social-media-overview13/ (accessed 10 November 2015).

Social Networking and Video Sharing Websites Policy PD 174. 2010. Lincolnshire Police - Policy Document ACPO Commissioning Officer: Chief Constable / Portfolio / Business-area Owner: Planning, Review and Innovation Manager / Department Responsible: Strategic Development Senior Owner: Marketing Manager: Effective Date: August 2010.

SocialSafe Limited. 2014. *6 tips for minimizing legal risk in social media*. SocialSafe - Social Media Law White Paper, March 2014.

Solomons, K. 2013. *SA's Shocking crime wave goes viral*. From: http://www.iol.co.za/news/crime-courts/sa-s-shocking-crime-wave-goes-viral-1.1557239#.UiGPMyQaL4Y (accessed 31 August 2013).

Sonderling, N.E. 2003. *Scoping and developing the potential for SAPS online service delivery*. MA Dissertation. University of Pretoria, Pretoria.

South Africa. 1996a. Constitution of the Republic of South Africa Act 108 of 1996. Pretoria: Government Printer.

South African Concise Oxford Dictionary. 2002. s.v. “definition”, “media”, "social". Cape Town: Oxford University Press Southern Africa.

South African Law Reform Commission. 2010. *Issue paper 27 Project 126. Electronic evidence in criminal and civil proceedings: admissibility and related issues*. From: http://www.justice.gov.za/salrc/ipapers/ip27_pr126_2010.pdf (accessed 8 June 2014).

South African Police Service. [s.a.] *Human Resource Development Annual Report 2009/2010*. Pretoria: SAPS Division Human Resource Development.

South African Police Service. 2008. *Memorandum: Resolving of crime learnership (ROC). Skills programme 1. Detective Learning Programme. Module 15 - Law of Evidence.* Pretoria: Commissioner of the SAPS. Police. Training Division, South African Police Service.

South African Police Service. 2013. *Cybercrime Unit*. From: http://intranet.saps.gov.za/about/components/cybercrime/home_page.htm (accessed 9 September 2013).

Stevens, S. 2009. *Making the case for using social media tools in policing*.pdf. Previously published at ConnectedCOPS.net. From: http://connectedcops.net/making-the-case-for-using-social-media-tools-in-policing/ (accessed 14 April 2016).

Stolley, G. 2015. *Bully allegedly slaps punches and knees pupil while teacher does nothing*. From: http://www.news24.com/SouthAfrica/News/Bully-allegedly-slaps-punches-and-knees-pupil-while-teacher-does-nothing-20150615 (accessed 6 September 2015).

Strutin, K. 2011. *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries. Pace Law Review*. From: http://0search.ebscohost.com.oasis.unisa.ac.za/login.aspx?direct=true&db=aph&AN=60797302&scope=site (accessed 13 October 2014).

Stuart, R. D. 2013. *Social Media: Establishing Criteria for Law Enforcement Use*. Feb 2013. From: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2013/february/social-media-establishing-criteria-for-law-

enforcement-use?utm_campaign=email-Immediate&utm_content=175293 (accessed 18 July 2013).

Symantec Cybercrime. 2013. From: http://www.symantec.com/corporate_responsibility/topic.jsp?id=cybercrime (accessed 19 July 2013).

Telecommunications Act … see South Africa. 1996f.

Terrorism Act … see United Kingdom. 2006b.

The Basics. [s.a.] *What is e-Discovery?* From: http://cdslegal.com/knowledge/the-basics-what-is-e-discovery/cds_-_complete_discovery_source (accessed 16 October 2014)

Trademarks Act … see South Africa. 1993.

Training, KINSA. 2015. From: http://kinsa.net/what-we-do/training/ (accessed 15 June 2015).

- *Transparency report*. 2014. From: https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (accessed 16 September 2014).
- *Transparency Report, user data requests.* 2014. From: https://www.google.com/transparencyreport/userdatarequests/countries/?t=table (accessed 16 September 2014).

Twitter Help Center. 2014. *Guidelines for law enforcement*. From: https://support.twitter.com/entries/41949-guidelines-for-law-enforcement# (accessed 13 September 2014).

UK Electronic Communications Act … see United Kingdom. 2000c.

Unisa. 2013. *Unisa Policy on Research Ethics*. From: http://www.unisa.ac.za/contents/colleges/col_agriculture_environ_sciences/docs/ResearchEthicsPolicyJan2013.pdf. (accessed 18 April 2014).

U.S. man jailed for Obama threat tweet. 2013. [News24]. From: //pinterest.com/pin/create/button/?url=http%3A%2F%2Fwww.news24.com%2FWorld%2FNews%2FUS-man-jailed-for-Obama-threat-tweet-20130620&media=&description=http://www.news24.com/sendToFriend.aspx?iframe&aid=eede5e58-dd7f-4cf5-9ef7-bc4898094525&cid=1073 (accessed 21 June 2013).

Van der Berg, C.J., Trainer at SAPS Academy Paarl. 2015. Statement to author, 6 February. Paarl.

Van der Berg, C.J., Trainer at SAPS Academy Paarl. 2016. Statement to author, 5 May. Paarl.

Van Dyk, C.E., Trainer and member at Monitoring and Evaluation Section at SAPS Academy Paarl. 2015. Statement to author, 10 April. Paarl.

Van Heerden, T.J. 1991. *Introduction to police science*. Third impression. Muckleneuk, Pretoria: University of South Africa.

Von Solms, B. 2015. *Presentation on Highlighting 3 crucial Cyber Security issues in SA*. Transnational Threats and International Crime Division. Copyright – Institute for Security Studies – 26 January 2015. From: http://www.issafrica.org/uploads/26-Jan-2015-Cybercrime-seminar-presentationspdf (accessed 18 June 2015).

Welgemoed, C., Trainer at SAPS Academy Paarl. 2015. Statement to author, 18 August. Paarl.

Welman, J.C. & Kruger, S.J. 2001. *Research methodology for the business and administrative sciences*. 2nd edition. Cape Town: Oxford University Press.

Welman, C., Kruger, F. & Mitchell, B. 2005. *Research methodology*. 3rd edition. Cape Town: Oxford University Press.

Wexler, C. 2012. *Critical Issues In Policing Series - "How Are Innovations in Technology Transforming Policing?*". Police Executive Research Forum, Washington, D.C. 20036. From: http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf (accessed 15 June 2014).

Wexler, C. 2014. *Critical Issues In Policing Series - The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime*. Police Executive Research Forum, Washington, D.C. 20036. From: http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf (accessed 16 June 2014).

What Are Research Objectives? 2014. From: http://www.ask.com/question/what-are-research-objectives (accessed 18 April 2014).

Wolff, R., McDevitt, J., & Stark, J. 2011. *Using social media to prevent gang violence and engage youth, Innovative Practices from the Senator Charles E. Shannon.* Jr. shannon-pub-9.pdf. Community Safety Initiative Series, March: 4. North-eastern University Institute on Race and Justice. From: http://www.mass.gov/eopss/funding-and-training/justice-and-prev/grants/shannon-csi/shannon-pub-9.pdf (accessed 14 April 2016).

Zeffert, D.T., Paizes, A.P., & Skeen, A St Q. 2003.*The South African Law of Evidence*. Durban: LexisNexis. Butterworths.

LIST OF ACTS: SOUTH AFRICA

South Africa. 1965. Civil Proceedings Evidence Act 25 of 1965. Pretoria: Government Printer.

South Africa. 1977. Criminal Procedure Act 51 of 1977. Pretoria: Government Printer.

South Africa. 1983. Computer Evidence Act 57 of 1983. Pretoria: Government Printer.

South Africa. 1987. Copyright Act 98 of 1987. Pretoria: Government Printer.

South Africa. 1988. Law of Evidence Amendment Act 45 of 1988. Pretoria: Government Printer.

South Africa. 1992a. Copyright Amendment Act 125 of 1992. Pretoria: Government Printer.

South Africa. 1992b. Interception and Monitoring Prohibition Act 127 of 1992. Pretoria: Government Printer.

South Africa. 1993. Trademarks Act 194 of 1993. Pretoria: Government Printer.

South Africa. 1995. South African Police Service Act 68 of 1995. Pretoria: Government Printer.

South Africa. 1996a. Constitution of the Republic of South Africa Act 108 of 1996. Pretoria: Government Printer.

South Africa. 1996b. Domestic Violence Act 118 of 1996. Pretoria: Government Printer.

South Africa. 1996c. Films and Publications Act 65 of 1996. Pretoria: Government Printer.

South Africa. 1996d. International Cooperation in Criminal Matters (ICCMA) Act 75 of 1996 (also referred to as the Cooperation Act). Pretoria: Government Printer.

South Africa. 1996e. National Gambling Act 33 of 1996. Pretoria: Government Printer.

South Africa. 1996f. Telecommunications Act 103 of 1996. Pretoria: Government Printer.

South Africa. 1998. Open Democracy Bill [B67 of 1998]. Pretoria: Government Printer.

South Africa. 1999a. Broadcasting Act 4 of 1999. Pretoria: Government Printer.

South Africa. 1999b. Films and Publications Amendment Act 34 of 1999. Pretoria: Government Printer.

South Africa. 2000a. Independent Communications Authority of South Africa (ICASA) Act 13 of 2000. Pretoria: Government Printer.

South Africa. 2000b. Promotion of Access to Information (PAIA) Act 2 of 2000. Pretoria: Government Printer.

South Africa. 2002a. Electronic Communications and Transactions Act 25 of 2002. Pretoria: Government Printer.

South Africa. 2002b. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Pretoria: Government Printer.

South Africa. 2004. National Gambling Act 7 of 2004. Pretoria: Government Printer.

South Africa. 2005. Electronic Communications (ECA) Act 36 of 2005. Pretoria: Government Printer.

South Africa. 2008. Consumer Protection Act 68 of 2008. Pretoria: Government Printer.

South Africa. 2009. The Protection of Personal Information Bill [B9 of 2009]. Pretoria: Government Printer.

UNITED KINGDOM

Laws of the United Kingdom. 1965. Criminal Evidence Act.

Laws of the United Kingdom. 1978. Protection of Children Act.

Laws of the United Kingdom. 1984. Police and Criminal Evidence Act.

Laws of the United Kingdom. 1990. Computer Misuse Act.

Laws of the United Kingdom. 1997. Protection from Harassment Act.

Laws of the United Kingdom. 1998a. Data Protection Act.

Laws of the United Kingdom. 1998b. Human Rights Act.

Laws of the United Kingdom. 1999. EU Telecoms Data Protection Directive.

Laws of the United Kingdom. 2000a. Regulation of Investigatory Powers Act.

Laws of the United Kingdom. 2000b. Terrorism Act.

Laws of the United Kingdom. 2000c. UK Electronic Communications Act.

Laws of the United Kingdom. 2002. Electronic Commerce (EC Directive) Regulations.

Laws of the United Kingdom. 2003. Privacy and Electronic Communications (EC Directive) Regulations.

Laws of the United Kingdom. 2006a. Police and Justice Act.

Laws of the United Kingdom. 2006b. Terrorism Act.

Laws of the United Kingdom. 2008. Criminal Justice and Immigration Act.

UNITED STATES

United States. 1791. Fourth amendment USA.

United States. 1968. Wiretap Act (Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §2510).

United States. 1980. Privacy Protection Act (Privacy Protection Act, 42 U.S.C.).

United States. 1986a. Electronic Communications Privacy Act (ECPA).

United States. 1986b. Pen Register and Trap and Trace Statute 18 U.S.C. Code §3121-3127.

United States. 1986c. Stored Communications Act (SCA), 18 U.S.C. Code §2701-2712.

Wiretap Act (Omnibus Crime Control and Safe Streets Act … see United States. 1968.

LIST OF COURT CASES

Damien O'Keefe v Williams Muir's Pty Ltd T/A Troy Williams. The Good Guys 2011 FWA 5311.

H v W (12/10142) 2013 ZAGPJHC 1; 2013 (2) SA 530 (GSJ); 2013 (5) BCLR 554 (GSJ); 2013 2 All SA 218 (GSJ) (30 January 2013). From: http://www.saflii.org/za/cases/ZAGPJHC/2013/1.html (accessed 17 October 2014).

Sedick & another v Krisray (Pty) Ltd [1] 2011 20 CCMA 8.7.1 and 2011 8 BALR 879 (CCMA).

Smith v Partners in Sexual Health (non-profit) 2011 32 ILJ 1470 (CCMA).

APPENDIX A

INTERVIEW SCHEDULE

AN INVESTIGATION INTO THE UTILISATION OF SOCIAL MEDIA BY THE SAPS IN RESOLVING CRIME

Captain L Turck is working at the SAPS Academy, Paarl and is conducting research on social media. The main objective will be to find out how social media could be used to investigate and solve crimes and to what extent the SAPS is already using it in its fight against crime. The researcher will conduct a qualitative study and collect data using focus groups discussions and short questionnaires for the target group, namely detectives in the SAPS. Literature consulted will include hard-copy sources, on-line publications and accredited journals. Information obtained will be processed and analysed. A report with findings and recommendations will be compiled.

The researcher undertakes to ensure voluntary participation and none of the participants will be harmed. Information obtained from participants will be treated as confidential.

Please take note that UNISA and SAPS will have access to the data.

The interview will take about 30 minutes in the preferred language to be English.

Will you please be so kind as to complete the following during the interview: [PLEASE ELABORATE AS MUCH AS POSSIBLE WHERE YOUR CAN]

PERSAL NUMBER	
RANK	
INITIAL AND SURNAME	
PROVINCE	
STATION	
CONTACT DETAILS	

Have you ever had cases that you investigated where social media were used to solve a specific crime?
If yes, which social network (eg. Facebook / Twitter / You Tube / WhatsApp / MixIt / any other) played a role?
Can you elaborate / explain how the Social Network contributed to your case?
Do you have access to the Internet at you place of work?
Do you know how to use Facebook / Twitter / You Tube / WhatsApp / MixIt / any other social networks in the line of your investigations?
Would you like to attend a programme that teaches you how to use Social Media as a tool to solve your cases in your line of work?

APPENDIX B

LETTER FOR APPROVAL

SUID-AFRIKAANSE POLISIEDIENS

SOUTH AFRICAN POLICE SERVICE

REFERENCE:	3/34/2
ENQUIRIES:	Col R Fakude Lt Col AR Symons
TELEPHONE:	012 334 3797 012 334 3771
FACSIMILE:	012 334 3714

OFFICE OF THE DIVISIONAL COMMISSIONER
DIVISION: HUMAN RESOURCE DEVELOPMENT

PRIVATE BAG X 177
PRETORIA
0001

The Head
STRATEGIC MANAGEMENT

RESEARCH REQUEST: AN INVESTIGATION INTO THE UTILISATION OF SOCIAL MEDIA BY THE SAPS IN RESOLVING CRIME: MAGISTER TECHNOLOGICAE: UNISA: RESEARCHER CAPTAIN L TURCK

1. Your 3/34/2 request received from your office with same heading dated 2014/09/18 has reference.
2. Provisional permission is granted for the research to be undertaken which will then be ratified once this office receives the completed and signed Undertaking document attached herewith.
3. It is trusted that you will find this to be in order.

Regards,

MAJOR GENERAL
ACTING DIVISIONAL COMMISSIONER: HUMAN RESOURCE DEVELOPMENT
HK SENTHUMULE

Date: 14/10/29

Page **1** of **1**

UMI

MASTERS THESIS
PUBLISH ABSTRACT ONLY AGREEMENT

M(I)
PAO
2001

Abstract no.

Do not write in this space

Vol/Issue

School Code

Abst. Length

PERSONAL DATA

1. Last Name: TURCK | First Name: LIZELLE | Middle Name:
2. Year of Birth (Optional): 1971
3. Country of Citizenship: REPUBLIC OF SOUTH AFRICA
4. Present Mailing Address
   Street address: 4 DAVID STREET, NORTHERN PAARL, PAARL, 7646

City	State/Province	Postal code	Country
PAARL	WESTERN CAPE	7646	SOUTH AFRICA

Future Mailing Address
Street address: 4 DAVID STREET, NORTHERN PAARL, PAARL, 7646

City	State/Province	Postal code	Country
PAARL	WESTERN CAPE	7646	SOUTH AFRICA

Effective date for future mailing address (mm dd yy) 2016-08-10

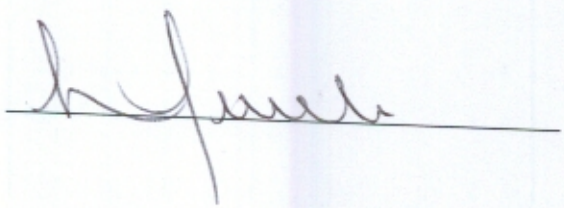
E-mail address: ttlizelle@gmail.com

MASTER'S DEGREE DATA

5. Full name of university conferring degree, and college or division if appropriate
   UNIVERSITY OF SOUTH AFRICA
6. Abbreviation for degree awarded
   MTech: Policing [Code 98613]
7. Year degree awarded
   2016

TITLE/SUBJECT AREA

8. Enter the title of thesis. If thesis is written in a language other than English, please specify which language and translate title into English. Language of text:
   Title: AN INVESTIGATION INTO THE UTILISATION OF SOCIAL MEDIA BY THE SAPS IN RESOLVING CRIME
9. Subject category of thesis. Please enter four-digit code from "Subject Categories" on following page. 0398
10. Please append an abstract of no more than 150 words describing the contents of your thesis. Your completion and submission of this form through your graduate school indicates your assent to UMI publication of your abstract. Formulas, diagrams and other illustrative materials are not recommended for abstracts appearing in *Masters Abstracts International*.

Author Signature:  Date: 2016-08-10

UNISA university of south africa

Stud no/nr: 3678-994-1
Navrae/Enq: M+D Eksamenkoördineerder
M+D Examination Coordinator
Tel: (012)441-5499/5500/5501

Ms L Turck
4 David Street
PAARL
7646

2016-07-06

Dear Ms Turck

I have pleasure in informing you that your dissertation has been accepted for the degree of **MTech in Policing**. You obtained a mark of 60% for the dissertation.

Please find enclosed a statement confirming your compliance with the requirements of the degree.

The degree will be awarded to you, provided you comply with the following requirement(s):-

- Submit the text of the dissertation in electronic format and the same text in a further two printed spine-glued hard cover copies, reflecting the full title of the dissertation and your name on both the cover and spine of the bound copies.

  When posted, the parcel containing the additional copies must please be marked for the attention of The Registrar, Record Management Division, M & D section, [Tel (012)429-3057 / 3506 / 3150 / 3486], or they may be handed in personally at the counter, Level 2 in Block B, Theo van Wijk Building (use the Gold Fields entrance), Preller Street, Muckleneuk Ridge, UNISA. The electronic format (preferably PDF, Word or WordPerfect) of the dissertation can be emailed to lib-drc@unisa.ac.za;

- complete and sign the enclosed agreement form with *ProQuest Information and Learning (University Microfilms Inc)* in respect of the publication of the summary and return it to the University.

If you have not already complied with the abovementioned requirement(s), you must please do so before **12 August 2016**.

Yours faithfully

for THE EXECUTIVE DEAN: COLLEGE OF GRADUATE STUDIES

/ejg
[MD RESULTS]

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za