

**EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME
CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM
JOHANNESBURG AND TSHWANE, GAUTENG**

**By
SHEPERD MOYO**

**submitted in accordance with the requirements
for the degree of**

MAGISTER TECHNOLOGIAE

in

SECURITY MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor: Prof. A.deV. Minnaar

February 2019

COPYRIGHT

All rights reserved jointly by the University of South Africa (UNISA) and Mr S Moyo. In terms of the **Copyright Act 98 of 1978**, no part of this material may be reproduced, stored in a retrieval system, transmitted in any form or be published, redistributed or screened by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission from UNISA. However, permission to use in these ways any material in this work that is derived from other sources must be obtained from the original source. For academic and research purposes original information may be used and referred to as long as it is properly referenced, and the source acknowledged as such.

DECLARATION FORM

Student Number: **36945323**

I, **SHEPERD MOYO**, declare that this dissertation titled:

EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG, is my own work and that all the sources that have been used or quoted have been indicated and acknowledged by means of complete and accurate references.

I further declare that I submitted this dissertation to the Turnitin Originality Checking Software Programme and that it falls within accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at UNISA for another qualification or at any other higher education institution.



Signature:

(Mr S. MOYO)

28-02-2019

Date:

ACKNOWLEDGEMENTS

Writing a dissertation is hard work and such a research study is never completed without the assistance from others. Although this research study appears under the name of a single author, many people have contributed to the completion of this study.

A very special thank you to my wife, Nomsa Ndou, my daughter, Mellicia Moyo and my sister, Onica Kulube, for their assistance and continual encouragement. Without your help, I could not have started nor completed this project successfully.

The help I received from my supervisor, Prof Anthony Minnaar, was invaluable and is immensely appreciated. You were always kind and patient enough throughout the study's challenges and offered me guidance, constructive critique and insight during the whole long process.

The researcher also acknowledges and thank the UNISA education scholarship administrators for endowing and sponsoring the study programme. I, in particular, would like to acknowledge how much I gained from my association with colleagues at UNISA; to name just a few: Prof Kris Pillay, Ms Nomsa Cebekhulu and Ms Judith Motha.

Exceptional thanks are due to three people whose ever-stimulating company, breadth of knowledge and variety of experience have done so much over many years to widen my horizons and alert me to new possibilities: Prof Minnaar, Prof Pillay and Prof NP Dastile (Chair of the Department of Criminology and Security Science).

I am very grateful to all those participants/respondents for taking part in the research study and who volunteered to prudently respond to survey questionnaires, interviews (face-to-face), and honoured my appointments with them.

ABSTRACT

This research evaluates crime prevention effects/impact of open-street closed circuit television (CCTV) surveillance systems as installed in the selected areas (research sites) of the cities of Johannesburg and Tshwane in the Gauteng Province of South Africa on crimes occurring in these surveilled areas. Currently, CCTV surveillance systems are a common sight in many of the urban areas of South Africa. The principal aim of this study was to explore the evaluation of CCTV for crime prevention, reduction and control. The results show that, despite a lack of empirical evidence as to the value of CCTV surveillance systems in preventing or reducing crime, there is strong public support for these systems and that the foundation for much of this support lies in the perceptions/feelings of members of the public of greater safety generated in areas with CCTV coverage. The method of sampling used was a purposive non-probability sampling approach. Participants were selected for interviews based on their knowledge and experience of CCTV systems. The results show that, despite this lack of empirical evidence, CCTV appears to be a viable option for crime prevention and control when integrated with evidence-based strategies rather than as a stand-alone tactic in order to achieve crime control benefits.

Keywords: Closed-Circuit Television (CCTV) Surveillance Systems; public safety and security; deterrence; crime prevention; surveillance and privacy.

ACRONYMS

BAC:	Business Against Crime
CBD:	Central Business District
CCTV:	Closed-Circuit Television
CPF	Community Police Forum
CPU	Central Processing Unit
CSIR:	Council for Scientific and Industrial Research
DDoS:	Deliberate Denial of Service
DNS:	Domain Name System
DVR:	Digital Video Recorder
GPSJ:	Governance Public Safety Justice
GPU:	Graphic Processing Unit
ICPC:	International Centre for the Prevention Crime
IoT	Internet of Things
ISS:	Institute for Security Studies
ITU:	International Telecommunications Union
IUDF:	Integrated Urban Development Framework
MTC:	Metropolitan Trading Company
NCPC:	National Crime Prevention Council
NDP:	National Development Plan
NICE:	National Initiative for Cyber Education
NVR:	Network Video Recorder
OECD:	Organisation of Economic Co-operation and Development
POPI:	Protection of Personal Information Act
SIMS:	Security Information Management System
VCA:	Video Content Analysis
VPN:	Virtual Private Network
VOCS:	Victims of Crime Survey

TABLE OF CONTENTS

CHAPTER 1: GENERAL ORIENTATION OF STUDY, PROBLEM STATEMENT AND MOTIVATION/RATIONALE FOR THE RESEARCH

1.1	INTRODUCTION	1
1.2	PROBLEM STATEMENT	10
1.3	RESEARCH AIMS, OBJECTIVES AND PURPOSE	12
1.4	RESEARCH QUESTIONS	13
1.5	STUDY AREA: BACKGROUND AND SETTING	14
1.6	SIGNIFICANCE OF THE STUDY	17
1.7	DEFINITIONS OF KEY TERMS AND CONCEPTS	17
1.8	CHAPTER OUTLINES	20

CHAPTER 2: RESEARCH METHODOLOGY AND RESEARCH DESIGN

2.1	INTRODUCTION	22
2.2	RESEARCH DESIGN	22
2.3	RESEARCH APPROACH	23
2.4	THEORETICAL AND CONCEPTUAL FRAMEWORK	25
2.4.1	Phenomenological Theory	25
2.4.2	Five environmental criminological theories	26
2.4.3	Case study approach	31
2.5	RESEARCH METHODS AND DATA COLLECTION TOOLS USED	31
2.5.1	Document analysis/literature review	32
2.5.2	Face-to-face interviews	34
2.5.3	Street survey questionnaires	37
2.5.4	Onsite observation	38
2.6	TARGET POPULATION, SAMPLING AND SELECTING OF INTERVIEW PARTICIPANTS	39
2.6.1	Target population	39
2.6.2	Purposive sampling	39
2.7	DATA ANALYSIS	42

2.7.1	Qualitative content analysis	43
2.7.2	Data coding	43
2.8	VALIDITY AND RELIABILITY	44
2.8.1	Validity	44
2.8.2	Reliability	45
2.19	ETHICAL CONSIDERATIONS	48
2.10	LIMITATIONS OF THE STUDY	52
2.11	CONCLUSION	53

CHAPTER 3: LITERATURE STUDY: CCTV SURVEILLANCE SYSTEMS, CRIME PREVENTION AND SECURITY

3.1	INTRODUCTION	54
3.2	THEORETICAL UNDERPINNINGS	57
3.3	THE PROLIFERATION OF CCTV	58
3.4	EVIDENCE OF CAMERA SURVEILLANCE EFFECTIVENESS	61
3.5	THE USE OF CCTV SURVEILLANCE AND ALLIED TECHNOLOGY FOR PUBLIC SAFETY AND THE IDENTIFICATION OF CRIMINALS	66
3.6	CRIME PREVENTION	71
3.7	CCTV SURVEILLANCE SYSTEMS AND CRIME PREVENTION	74
3.7.1	CCTV technologies: Facial recognition systems	77
3.7.2	The role of international research: Impact of CCTV surveillance	78
3.8	CYBERSECURITY AND CCTV	79
3.8.1	The mechanism of crime reduction	80
3.8.2	CCTV systems as a security concept	81
3.8.3	Cyber threats to control rooms and CCTV surveillance operations	81
3.8.4	Deliberate Denial of Services (DDoS)	83
3.8.5	Some preventative cybersecurity measures	83
3.8.6	Risk planning for cyber protection	84
3.9	LAWS AND POLICIES FOR CYBERSECURITY	86

3.10	CYBERSECURITY, CYBERCRIME, INFORMATION SECURITY AND PRIVACY ISSUES RELATING TO THE USE OF CCTV SURVEILLANCE SYSTEMS	89
3.10.1	Privacy issues vs CCTV surveillance systems	90
3.10.2	The data protection legal framework in South Africa	91
3.10.3	What are data protection principles?	93
3.10.4	How do data protection principles relate to cybercrime?	94
3.10.5	International instruments for data privacy and protection	95
3.10.6	The General Data Protection Regulation of the European Union	98
3.10.7	CCTV surveillance and value adding to public spaces	98
3.10.8	Criticising surveillance and surveillance critique: Why privacy and humanism are necessary but insufficient	100
3.11	CONCLUDING REMARKS	102

CHAPTER 4: RESEARCH FINDINGS: DATA ANALYSIS AND INTERPRETATION

4.1	INTRODUCTION	104
4.1.1	Interview and survey questionnaires	105
4.2	DATA ANALYSIS AND DISCUSSION: SCHEDULE OF INTERVIEW QUESTIONS	107
4.2.1	Schedule of Interview Questions: Private security control rooms: CCTV surveillance operations (Annexure G)	107
4.2.2	Operational processes followed in control rooms for CCTV surveillance	121
4.2.3	Response to suspicious activities observed	123
4.2.4	Schedule of Interview Questions: CPFs and residential areas: CCTV surveillance operations (Annexure H)	133
4.2.5	Support for CCTV	148
4.2.6	Issue of privacy	148
4.2.7	Analysis of the different survey samples	148
4.3	COMPARATIVE ANALYSIS	149
4.3.1	Views about CCTV	151

4.3.2	Civil liberties	154
4.3.3	Information gathering	160
4.3.4	Residents' attitudes towards CCTV	163
4.4	DATA ANALYSIS AND DISCUSSION: STREET SURVEY QUESTIONNAIRE (ANNEXURE I)	166
4.4.1	Analysis of street survey questionnaires	171
4.4.2	Deductions	172
4.4.3	Street survey findings: Some conclusions	178
4.5	SIGNIFICANCE OF FINDINGS	179
4.6	CONCLUSIONS	181
4.7	RECOMMENDATIONS	182
4.8	FUTURE RESEARCH	183

LIST OF REFERENCES	185
---------------------------	------------

ANNEXURES

Annexure A:	UNISA Research Ethics Approval Letter	203
Annexure B:	Turnitin Similarity Index Report	205
Annexure C:	Language Editor Confirmation Letter	206
Annexure D:	Request permission to do research letter [DRAFT]	207
Annexure E:	Participant Information Sheet	210
Annexure F:	Proforma Informed Consent Form	214
Annexure G:	Schedule of Interview Questions: Private security control rooms: CCTV surveillance operations	215
Annexure H:	Schedule of Interview Questions: CPFs and residential areas: CCTV surveillance operations	223
Annexure I:	Street Survey Questionnaire	229

LIST OF TABLES

Table 1.1	Gender composition of CCTV operators	109
Table 1.2	Age categories of CCTV operators	110
Table 1.3	Highest educational qualification (NQF levels)	112
Table 1.4	Years of experience working in the private security industry sector	113
Table 1.5	Occupational position in the company	114
Table 1.6	Years of experience in current position	115
Table 1.7	Sites where CCTV are installed	117
Table 1.8	Shopping centre/mall	118
Table 1.9	Residential neighbourhood	118
Table 1.10	Central Business Districts	119
Table 1.11	Gated neighbourhoods	119
Table 1.12	Private security estates	120
Table 1.13	Business premises	120
Table 1.14	Factory/industrial site	121
Table 1.15	Number of cases used within time period	130
Table 1.16	Crimes in order of priority of cases used	131
Table 1.17	Gender composition of CPFs and individuals in residential areas	134
Table 1.18	Age categories of respondents	135
Table 1.19	Highest educational qualification	136
Table 1.20	Where CCTV installed in neighbourhood/residential areas	136
Table 1.21	Shopping centre/mall	138
Table 1.22	Residential neighbourhoods	139
Table 1.23	Central business districts	140
Table 1.24	Gated neighbourhoods	141
Table 1.25	Private security estate	142
Table 1.26	Business premises	143
Table 1.27	Factory/industrial site	144
Table 1.28	Gender	167
Table 1.29	Race composition of respondents	168

LIST OF FIGURES

Figure 1.1	Gender composition of CCTV operators	110
Figure 1.2	Age categories of CCTV operators	111
Figure 1.3	Work position in the company	114
Figure 1.4	Gender composition of CPF members and individuals in residential areas	134
Figure 1.5	Age categories of CPF members and individuals in residential areas	135
Figure 1.6	Where CCTV installed in neighbourhood/residential area	137
Figure 1.7	Shopping centre/mall	138
Figure 1.8	Residential neighbourhood	139
Figure 1.9	Gated neighbourhoods	141
Figure 1.10	Private security estates	142
Figure 1.11	Business premises	143
Figure 1.12	Factory/industrial site	144
Figure 1.13	Gender composition of respondents	167
Figure 1.14	Race composition of respondents	168
Figure 1.15	Effectiveness of CCTV	169
Figure 1.16	Impact on crime levels	169
Figure 1.17	Privacy issues	170

LIST OF IMAGES

Image 1.1	A street pole with CCTV cameras mounted at the top	18
Image 1.2	Typical CCTV installation in a suburb	19

CHAPTER 1

GENERAL ORIENTATION OF STUDY, PROBLEM STATEMENT AND MOTIVATION/RATIONALE FOR THE RESEARCH

1.1 INTRODUCTION

This chapter presents the problem statement, motivation/rationale, background, significance and purpose of the study, the context of why research on Closed-Circuit Television (CCTV) surveillance systems was deemed necessary. This is followed by a section outlining key concepts and definitions of terms used primarily in this research study. There are a variety of different approaches to crime prevention that differ in terms of the focus of the intervention, the types of activities that are delivered, the theory behind how those activities are designed to bring about the desired results and the mechanisms that are applied. In this research study project, attention/focus will be given to the use of closed-circuit television camera surveillance systems.

The way in which CCTV influences a community is determined by a set of assumptions about CCTV and the way it works. It therefore falls upon research studies to test these assumptions by measuring levels of support, perceptions of how CCTV works, and the factors which may influence these. These assumptions about CCTV must be assessed within the framework of the characteristics and experiences of the individuals who live in these areas. Previous studies that have measured the level of victimisation, fear of crime and avoidance specifically in areas covered by CCTV have done so in non-residential settings. Few studies have measured respondents' actual knowledge of how CCTV works, and the link between people's level of knowledge and support for CCTV.

CCTV cameras are primarily used to monitor and record images of what takes place in specific locations in real time (Duncan, 2018a: 14). CCTV cameras and surveillance systems are today firmly entrenched in modern society, not just in terms of their widespread presence in public places, but also as a key part of community safety, policing and national public security policy (Gerrard & Thomson, 2011: 10-12). Public

CCTV schemes are frequently installed to reassure the public that something (prevention/reduction) is being done about crime (McCahill & Norris, 2002: 23 & 56; Gill & Spriggs, 2005: 18-20; Ratcliffe, 2006: 45 & 65). CCTV has several potential applications for public safety, and has been deployed with the intention variously of preventing crime, detecting offences, improving the response to emergencies, assisting in the management of places and reducing public fear of crime (Ratcliffe, 2011: 15).

The images collected by CCTV cameras are usually sent to a control room where they are monitored by an operative there, and then also simultaneously recorded on video tape or stored as digital information. The cameras can be fixed or set to scan an area, or they can be remotely operated by controllers (e.g. instructed to either 'pan, tilt or zoom' as required). Monitors (system operators) can themselves be watched by controllers (supervisors or managers in the control room) or left unmonitored. The recorded information can be stored and/or reviewed by those who have access to the recordings at their convenience.

The widespread introduction and diffusion of CCTV cameras and systems in public places across South Africa has not gone unnoticed (Minnaar, 2006: 4-5). CCTV cameras are now a common sight almost everywhere, such as on public highways and in shopping malls and arcades (Minnaar, 2006a: 35).

Progressively, the use of public space CCTV has become a "normal feature of public life" with the daily blanket surveillance of the movement of persons in public spaces (Duncan, 2018b: np). In South Africa, where the police daily fight a deadly war against crime, surveillance technology is increasingly being used by local municipalities to augment an understaffed and under-resourced police force. Increasingly, these cameras are being loaded with 'smart' capabilities, such as Automatic Number Plate Recognition (ANPR) and facial recognition software. The addition of video analysis tools to CCTV surveillance systems has provided additional and refined analysis of collected video footage (Duncan, 2018b: np). Such analysis permits CCTV to be

become 'smart dataveillance devices' that are able, via artificial intelligence analytics, to conduct 'investigations' through the gathering and processing of analysed data. This process makes peoples' movements highly visible to the authorities. Such additional analytical surveillance measures are meant to assist in 'smart' policing, whereby police use information tools to enhance the effectiveness of policing.

An example from 2017 illustrates the use of CCTV video as evidence in a court of law. In 2013 the internationally renowned artist, Zwelethu Mthethwa, was accused of beating 23-year-old sex worker, Nokuphila Kumalo, to death. In Mthethwa's trial, Judge Patricia Goliath accepted crucial CCTV footage that captured Mthethwa kicking and beating Kumalo in a street of the Cape Town suburb, Woodstock. She subsequently died from her injuries. CCTV street video footage captured the assault and the police positively identified Mthethwa as both the driver of the Porsche seen pulling over in Ravenscraig Road and the person who proceeded to assault Kumalo. Substantiating the presence of the vehicle parked in Ravenscraig Road at the time of the assault was information provided by Tracker.¹ Mthethwa's defence team attacked the authenticity of the CCTV video footage, but the court found that they failed to prove that the images had either been manipulated or tampered with. Accordingly, Judge Goliath accepted the public street CCTV recording of the murder as "unimpeachable" and "conclusively accepted it as evidence". Furthermore, Goliath stated in her pre-sentencing judgement that such CCTV video images had become "crucial in collecting evidence and finding the truth in criminal cases" (Anon, 2017: np).

A criminal investigation can be thought of as a series of questions: *Who* was involved in an incident? *Where* did it happen? *What* happened? *When* did it happen? *Why* did it happen? and *How* were any offences committed? These questions, are based on and known as the '5WH' Investigation Model (Cook, Hill & Hibbit, 2016: 75; Stelfox, 2009: 80). CCTV may be useful in answering at least two of these questions, namely:

¹ Tracker has been the leading vehicle tracking company in South Africa since 1996 and provides a vehicle tracking installed device, particularly to combat vehicle hijackings, which tracks via satellite tracking (see www.tracker.co.za).

What happened; and who was involved (La Vigne, Lowry, Markman & Dwyer, 2011: 18).

According to Duncan (2018a):

“The need for human monitoring places a natural limit on the analysis of camera footage. But, with digital tools of analysis, this is changing. When linked to a computer loaded with software capable of algorithmic analysis, huge amounts of footage can be analysed. These camera-based surveillance systems can capture information about a person’s physical location. Some may only provide real time information, while others may record information for further analysis” (Duncan, 2018a: 32).

But the danger of such surveillance systems is that governments of authoritarian bent can misuse this collected data of people’s movements, political activities and associations (Duncan, 2018a: 33).

For public street police investigations of CCTV digital video images to remain admissible in courts of law, there needs to be “... a transparency of a process and a holistic approach [within] the management, application and use of public street [CCTV surveillance] systems” (Brooks & Corkill, 2014: 220-225).

Invasive styles of information analysis, such as number plate recognition and biometric facial identification software, are being introduced in new hi-tech CCTV surveillance cameras to improve their capabilities. Few concerns, let alone from members of the public, are being raised about the surveillance analytical implications for the protection of privacy rights in public areas (Duncan, 2018a: 52). But CCTV surveillance system installations continue apace in public areas, with many of these installations being justified by municipal authorities that their installation is intended solely or largely for the purposes of reducing criminal activity in urban city centres (Lyon, 2011: 41).

CCTV is often seen and mainly used as a panacea or technical solution to security problems in crime prevention and control. Surveillance equipment, especially cameras and access-controlled devices, continue to be increasingly introduced into public and private spaces. Residents use the equipment in their daily lives in places where they are both operators and targets of the systems. CCTV in Central Business Districts (CBD) in South Africa has largely been used for the purpose of crime prevention, deterrence and crime control (Minnaar, 2007: 174-175). Understanding the attitudes of members of the public towards the impact CCTV has on their privacy, crime deterrence, prevention and social disorder, is an essential, but complex, consideration for policy makers, where public trust plays a central role. The difficulties of assessing the impact of CCTV on crime is difficult given the fact that the authorities have not endeavoured to obtain private impact assessments (including on privacy). This suggests that the public is forced to depend upon the state's version of whether CCTV systems are successful or not, and whether their version of events, normally for public relations (PR) purposes, emphasises only the positive impact of Closed-Circuit Television (CCTV), (Karakus, McGarrell & Basıbuyuk, 2010: 175-179).

According to Minnaar (2006):

“The ‘outsourcing by default’ has extended to the provision of CCTV surveillance in a number of Central Business Districts (CBDs) in South Africa. Such outsourcing and the funding of installation and running costs has been a boon to the SAPS in that while they do not impinge on policing functions on the ground, they provide an additional support service for them without requiring any financial outlay or expensive infrastructure. Accordingly, the police have encouraged such anti-crime surveillance and monitoring services without outsourcing or losing any policing functions” (Minnaar, 2006: 2).

In the early days of surveillance studies, many academics and researchers ‘embraced’ Foucault’s (1977: 56) elaboration of ‘panoptic’ surveillance, “a metaphor for the

dispersal into wider society of a disciplinary mode of power” (Kietzman & Angel, 2010: 138). The term influenced, and continues to do so, a large portion of the resulting research publications on the subject:

“... owing to the conceptualisation of power and governmentality that underpins it. Despite its appeal, many² in the field of surveillance studies question the utility of the panopticon as a model of contemporary surveillance” (Chivers, 2016: 71).

According to Taylor (2010: 209), “some authors³ have made the argument that CCTV is simply a logical and straight forward policy response to tackle crime and disorder, whereas those who [highlight] the inconclusiveness of [research] findings ...” about surveillance and the use of CCTV “or question [their] validity” are “often portrayed as enemies of the public interest” (Davies, 1996:153).

When discussing national security and/or the protection of citizens, the relationship between privacy and security is often described as a “trade-off” or a “balancing act” particularly in relation to the introduction of new surveillance technologies or practices (Lyon, 2011: 12). For example, the European Security Research Advisory Board (ESRAB) (2006: 23) prioritises technology development, particularly surveillance technologies, in its efforts to increase security. This immediately raises questions about privacy and data protection. However, others have argued that the metaphor of a ‘trade-off’ or ‘balance’ between privacy and security misrepresents the primary issues, since “the erosion of privacy creates new insecurities and privacy is a social good in and of itself” (Goold, 2009: 6).

In some instances, privacy may be seen to have eroded in relation to the increasing surveillance of individuals (e.g. communication-based surveillance) as highlighted by the 2013 United States (US) National Security Agency (NSA) scandal, which pointed

² For example: Haggerty and Gaszo (2005: 169-187); Lyon, (2003: 23); Dupont, (2008: 34).

³ For example: Welsh and Farrington, (2009: 89).

towards the increased surveillance of civilians in the US. This was revealed by the release of confidential documents by Edward Snowden – a data and systems analyst contracted to the NSA with security clearance (Greenwald, 2014: 42).

Furthermore, European policy commitments, such as the Stockholm Programme,⁴ argue that, in addition to security, privacy and data protection are fundamental rights that must be adequately protected while ensuring security. Therefore, some elements of the European policy framework seem to be moving away from a balanced metaphor (Barnard-Wills, 2013: 170-171).

Given this tension within policy documents, there has been an examination of the ways in which previous public opinion surveys conceptualised and operationalised the terms privacy, trust, security and surveillance (i.e. the use of surveillance technologies to enhance security) to determine whether they cohesively and appropriately measure public attitudes in order to adequately inform policy-makers and other stakeholders. As a result, there have been Europe-wide surveys of citizens' attitudes towards privacy, security, trust and surveillance (Hustinx, 2010: 15).

The growth of CCTV in South African public and private spaces mirrors broader global trends as:

“[r]ollouts [of CCTV] tend to ‘follow the money’. In other words, they tend to follow patterns of wealth in the major metropolitan cities in South Africa. This contributes to the enclosure of city spaces by private capital, and consequently to the privatisation of public spaces and the reproduction of inequalities” (Duncan, 2018a: 7).

The widest dissemination of CCTV systems has occurred in the United Kingdom (UK) (Caplan & Kennedy, 2010: 51) and in South Africa the use and implementation of public

⁴ See Cassarino, (2010: 50); and European Policy Centre, 2013; for more detail on the Stockholm Programme.

open street Closed Circuit Television (CCTV) surveillance systems in Central Business Districts (CBDs) solely for the purpose of crime control (reducing street crime) or crime prevention (deterrence) has been a relatively new (mid-1990s) intervention within the broader context of crime prevention programmes (Minnaar, 2006: 3-5). One of the drawbacks to its implementation for this purpose has been its costs and the inability of the South African Police Service (SAPS) to fund such implementation in the light of other more pressing priorities and demands on its finances and resources (Minnaar 2006: 4-8). However, the initiative to start implementing and linking CCTV surveillance systems in CBDs in the major metropolitan cities of South Africa to local police services was taken in the mid-1990s by Business Against Crime of South Africa (BACSA) (Minnaar, 2006: 4-5).

The extent of this proliferation has led some commentators and academics to argue that the UK is now the most surveilled country in the world. In 1999, Norris and Armstrong (1999: 45 & 62), estimated that 540 town councils had installed Home Office-funded CCTV surveillance programmes in their town centres. Although there are no specific numbers for the prevalence of CCTV cameras, estimates of installed numbers in the UK alone range from 1.9 million to 4.3 million (Gerrard & Thomson, 2011: 10). As early as 2002 McCahill and Norris put the estimated number of publicly- and privately-operated cameras in the UK at 4.2 million (McCahill & Norris, 2002: 34).⁵ Although the precise number of cameras can be debated the existence of the CCTV 'revolution' cannot. Consequently, CCTV and the surveillance practices and relationships embedded in the technology are a key feature of modern society.

While South Africa tracks, to a considerable degree, international trends in the development of CCTV, it is very important that, in local terms, the contextualisation of this worldwide trend be analysed critically. David Lyon, the internationally recognised scholar on surveillance studies and Director of the Surveillance Studies Centre at

⁵ But in 2012 Norris had revised this estimate and had stated that the figure might only be about 1.85 million operational cameras in the UK. This reduction being largely due to local town councils not continuing the funding of operational costs after the UK Home Office had funded the initial installation costs of such CCTV surveillance systems largely in city and town Central Business Districts.

Queens University in Kingston, Canada, noted that "... while surveillance techniques are increasingly globalised, local and regional cultural contexts mediate the experience of surveillance in different ways" (Lyon, 2011: 35)

Criminological literature on public CCTV was initially concerned with the basic question of whether CCTV led to a reduction in offending. Nevertheless, overviews of CCTV evaluations (Philips, 1999: 16; Welsh & Farrington, 2002: 19) confirm that, irrespective of a large volume of research done on CCTV implementation around the world, "... results continue to be ambiguous" (Penberthy, 2001: 89). McCahill and Norris (2002: 16) points out that the "identification and exclusion of known or suspected" persons or the application of predictive policing is currently practiced in public spaces.

CCTV can be used as a reactive mode of policing. In other words, suspects or criminal offenders can be identified, tracked and/or subsequently traced. Laura, (2001: 11) maintains that investigators of crimes are uncertain concerning the effective use of CCTV surveillance in the investigation of crime. The private sector and businesses also lack a clear understanding about the utility worth of CCTV in the investigation of crime (Welsh & Farrington, 1999: 500). Businesspeople only want to monitor their workers to prevent stealing and do not want to assist the police to reduce crime (Laura, 2001: 17). McCahill and Norris (2002: 17) also discussed the "new penology as the actuarial, seeking to regulate the danger, as opposed to the old penology that concentrated on an individual criminal and diagnosis of the crime". Norris and Armstrong (1999: 63), maintain that CCTV has exhibited its effectiveness. Accordingly, even more CCTV installations are needed where the crime levels remain high. However, Matchett (2003: 3) holds that CCTV cameras alone are not capable of protecting property from theft or vandalism. The cameras only gather and store information principally for use as evidence if required in any forthcoming court case for prosecution purposes, and are regarded as technology and equipment that assist crime prevention and law enforcement agencies to police better and respond quicker to a 'crime-in-progress'.

According to the study, reported by Caplan and Kennedy (2010: 196), although there is no significant relationship between general IT and crime fighting and deterrence, the productivity of the police increases when the adaptation to using IT rises. The findings of this research will be of significance to scholars undertaking studies in the area of CCTV Surveillance Systems. The logic of CCTV, put simply, is that because (rational) offenders know they are being watched they will consequently decide not to risk committing crimes or deviant acts, and if they do they are conscious there will be an image that can help identify them and be used as evidence to support a prosecution (Lyon, 2011: 12). Such rationality by offenders will likely lead to decreases in crime and social disorder. Evidence of effectiveness from the reviews of CCTV paint “a somewhat mixed picture” (Ratcliffe, 2006: 35; Eck, 2002: 610-615) in that some studies show it has had an effect of some sort, while others show a negative effect, or a neutral one. It depends on many different factors and, the evidence suggests that CCTV works most effectively when bundled together with a package of other situational preventative measures (Home Office, 1994, as cited in Ratcliffe, 2006: 35). In other words, CCTV is useful when used as synergy in integration. As CCTV is adopted as a security technology, would-be users will be able to make informed decisions prior to installation and usage.

1.2 PROBLEM STATEMENT

Globally, surveillance systems have been synonymous with detection and deterrence of criminal activities. Despite the enormous potential that exists in surveillance systems, the public continues to play down the importance of these systems as a key element in crime prevention in the area under study. The problem in the study therefore rests on the premise that awareness of the effectiveness of surveillance systems is still significantly high in the study area despite the lack of evaluation benefits that can be connected to them. Proponents of CCTV believe that it is “effective in facilitating immediate responses to incidents, combating certain types of crime and reducing fear of crime” (McCahill & Norris, 2002: 72). Critics, however, put forward the counterargument that there are major and noteworthy negatives to the use of CCTV

in public spaces. A significant objection being that CCTV may “target already vulnerable sections of the population and result in social exclusion” (Lyon 2011: 30).

Other concerns about the installation, implementation and usage of CCTV surveillance systems relate to the possibility that CCTV surveillance will be used to “undermine individual freedoms and facilitate oppressive forms of social control” (Norris & Armstrong, 1999: 47). “Smart” policing has become the means for combatting street crime. This policing model uses Information and Communication Technologies (ICTs) to enhance policing efforts. The South African Police Service (SAPS), some South African metropolitan municipalities (e.g. Cape Town, Durban, Johannesburg and Tshwane) and private companies are teaming up to use data-driven technologies, such as CCTV surveillance systems, with added technology, such as intelligent facial recognition and ANPR, in the fight against crime.

This study has the potential to improve the overall understanding of the role that CCTV plays in crime management and makes recommendations that justify the investment in and systematic use of these devices to boost safety in urban city centres. Moreover, this study can increase community awareness of the reliability of CCTV cameras and thereby influence the way in which law enforcement agencies as well as private security companies implement and manage crime prevention initiatives in communities where CCTV has been installed. South Africa has followed international trends in street-level police investigation and embraced technologies whose influence on crime fighting and crime intelligence information gathering are, at best, unclear and inconclusive. Research by Welsh and Farrington (1999: 35) reveals mixed responses about the usage of CCTV surveillance systems, namely, that it has:

- a positive effect (decrease in offences);
- an undesirable effect (increase in crime); and
- no effect, or unclear evidence (Welsh & Farrington, 2002: 13).

It should be noted, moreover, that attempts to link the implementation of CCTV directly to changes in the overall crime rate are problematic. It is for this reason that the researcher has undertaken a study into the evaluation of CCTV camera systems for crime control and prevention in the Johannesburg and Tshwane municipal areas. Such research can help avoid the 'knee jerk' installation of CCTV following a sensational crime incident, particularly in affluent residential areas.

In this research project, the problem statement is therefore about evaluating the use of CCTV surveillance systems for crime control and prevention in selected residential areas in Johannesburg and Tshwane (Pretoria) in the Gauteng Province of South Africa.

1.3 RESEARCH AIMS, OBJECTIVES AND PURPOSE

The broad aim of this research study is:

At the broadest level, the aim of this research study is to give a clear sense of what can reliably be believed to be true about the effects/impact of CCTV surveillance systems, based on the existing evidence; to link these findings to a wider set of questions about the implementation and operationalisation in selected areas (research sites) of the two selected cities (Johannesburg and Tshwane). This includes considerations at the level of policy and highlighting outstanding issues and areas where further research might be needed.

The primary aim of this study then is to analyse the implementation of CCTV system as a crime prevention tool with a view to suggest the secure framework for South Africa environment.

The purpose of the present study is to evaluate the use of CCTV surveillance systems for crime control and prevention. Furthermore, to explore the usage and benefit of CCTV surveillance systems with a view to determining their value within the community from the perspectives of Community Police Forums (CPFs), CCTV

Operators and residential areas impact on crime, value as both a crime prevention measure and as an aid to police.

The study's objectives are as follows:

- to analyse the capabilities of CCTV systems as crime prevention tool from technology been introduced and widely used in Johannesburg/Tshwane in conjunction with international literature.
- to examine the current CCTV system implementation in South Africa at the public acceptability level.

1.4 RESEARCH QUESTIONS

The primary research question for this research is the following:

- What is the contribution that installed CCTV surveillance systems can make towards crime prevention and control?
- In other words: What was the impact of CCTV surveillance in the selected research areas (Johannesburg and Tshwane)?
- Examining the effectiveness of current CCTV systems implementation in Johannesburg and Tshwane.

Secondary/ancillary questions to the primary research question were formulated to broadly deal with such research issues as:

- What were the residents/CCTV operators/security officers' experiences with public CCTV surveillance?
- What has been the impact that CCTV has had on crime in general?

- What has been the impact of public CCTV surveillance on the views of respondents regarding the privacy rights of individuals?
- In what way can CCTV video footage be used as a surveillance technique in crime prevention and control?
- In what way do respondents think CCTV video footage can be admitted as evidence in court?

These research questions chiefly guided the progression of the study, in that they were always considered, referred to, and, if needed, clarification questions were posed to respondents, as the study unfolded. Answers to these questions were sought and provided in the research findings chapter of this study.

1.5 STUDY AREA: BACKGROUND AND SETTING

In this research study two sites were selected, namely the cities of Johannesburg and Tshwane (Pretoria) situated in the Gauteng Province of South Africa.

Johannesburg – or as it is more commonly known: ‘Joburg’ – is the largest city in South Africa and the provincial capital of the Gauteng Province. Gauteng is the wealthiest province in the country, being both the industrial heartland and financial centre, not only of South Africa, but of the African continent as well. Johannesburg is one of the 50 largest cities in the world and the largest city in the world not sited on the coast, a lake or a river (World Population Review, 2019a: np). According to Statistics South Africa the latest population estimates for the Johannesburg metropolitan area are around 5, 6 million (Statistics South Africa (StatsSA), 2018: 40).

While the population estimate for the Tshwane Metropolitan Area – the Administrative Capital of South Africa – was put at approximately 2, 47 million at the end of 2018. The City of Tshwane Metropolitan Municipality is the metropolitan_municipality that

forms the local government of northern Gauteng Province. The Metropolitan area is centred on the city of Tshwane with surrounding towns and localities included in the local government area. The Tshwane municipality is home to the Tshwane University of Technology; the largest distance education university in Africa (the University of South Africa, more commonly known by its acronym, UNISA); the University of Pretoria, one of South Africa's leading research and teaching universities; and the Sefako Makgatho Health Sciences University (formerly known as the Medical University of Southern Africa, at the Medunsa Campus of the University of Limpopo) situated in Ga-Rankuwa, Pretoria North. The two state research councils: the Human Sciences Research Council (HSRC) and the South African Council for Scientific and Industrial Research (CSIR), are also in the Tshwane municipal area. The combined two city metropolitan population (Johannesburg and Tshwane) being therefore just over 8 million out of a total for Gauteng Province of 14.7 million (StatsSA, 2018a: 2; 15 & 17; World Population Review, 2019b: np).

Unfortunately the city centre of Johannesburg and in particular the precincts of Newton / Hillbrow / Braamfontein, has over the years built up (and it must be said) a deserved reputation for being crime ridden and extremely unsafe, (Minnaar, 2006: 16). The persistent public image of the area was strongly that of being derelict, dysfunctional and having a crime problem. Typical inner-city decay conditions with its associated overcrowding of residential buildings, continual increases in crime, especially street crime, drug dealing and vehicle hijacking, was experienced in these areas during the early and mid-1990s (Leggett, 2002: 68).

In the post-1994 years, the population mix of the Johannesburg CBD area changed dramatically with many foreign migrants (some of them undocumented and irregular immigrants) coming into the area. With the rising levels of crime in the area, the Hillbrow Police Station was identified as one of the about 140 (out of approximately 1 200) problem ('hot spot') or priority crime police stations in South Africa. Foreign embassies and consulates in South Africa routinely warned their citizens traveling to the country to avoid the area, especially in the late-night hours. Consequently, central

Johannesburg is generally perceived to be a 'dangerous place' populated by a high number of criminals.

With this background the installation of public (open street) crime control CCTV surveillance systems in the area became a high priority. Braamfontein is regarded as Johannesburg's Central Business District (CBD) and includes municipal council offices; Wits University; private colleges, such as Damelin; businesses; and numerous retail stores and the Nelson Mandela Bridge, which crosses over 42 railway lines and links the two main business areas of Johannesburg: Braamfontein and Newtown. Unfortunately, the city centre of Johannesburg and the precincts of Newtown, Hillbrow and Braamfontein, have become the home of many apartment buildings and so-called 'high-rises' but, at the same time, they continue currently to experience the accompanying high-levels of urban crime with an earned reputation for being very unsafe. The public viewed the area as "being derelict, dysfunctional and having a crime problem ... [with] typical inner-city decay conditions with its associated overcrowding of residential buildings" that has persistent street crime, such as drug dealing and vehicle hijacking (Leggett, 2002: 56).

Similarly to Johannesburg, the Tshwane Metropolitan Municipality also experiences high levels of crime. At least 319 CCTV cameras, covering Marabastad, the CBD, Sunnyside, Brooklyn, Waterkloof and Centurion have been installed (2018). These areas also include the Union Buildings area and the Hatfield and Arcadia areas, where most high commissions, the diplomatic community and embassies are situated. However, due to long-running court disputes concerning the awarding to private companies of the tender to operate and monitor the CBD installed cameras, "...they're not being monitored" (i.e. not operational). Although the operational systems were effective in the past in combating crime and enhancing safety the neglect of the CBD system in particular has put the public at risk and a predicted rise in smash-and-grabs, cable theft, robberies and hijackings could result from the inactive systems (Swart, 2018: 54).

1.6 SIGNIFICANCE OF THE STUDY

This research study will provide knowledge about the usage of CCTV as crime prevention tool and will enable creation of industry-wide best practices for the development, deployment, evaluation, and integration of policies related to the ethical use of CCTV in crime prevention initiatives. The researcher undertook this study project in the belief that students, policy makers and practitioners need to have a strong grasp of the thinking behind the strategies and tactics that are used to try to prevent crime and CCTV as a situational crime prevention strategy.

Much of the analysis presented in this study is from the review of collected documents and publications. The empirical evidence which informs the findings presented in the latter part of the study is from a series of interviews with CCTV operators, policy-makers (CPFs and individuals in residential areas and service providers, inter alia private security companies in selected areas of Johannesburg and Tshwane, conducted during the latter part of 2018 and the first two months of 2019). In total 40 interviews were conducted with CCTV operators, (e.g. CCTV control room managers or controllers and other interested parties. Forty interviews were also conducted with members of local CPFs, including community representatives associated with CCTV provision in the selected local authority research site areas. The researcher will provide knowledge about the usage of CCTV as crime prevention tool.

1.7 DEFINITIONS OF KEY TERMS AND CONCEPTS

This section provides general definitions of terms related to the study. According to Creswell, (2014: 2), there are certain concepts that are central to any inquiry. The concepts that follow are crucial to this study and are explained in order to simplify what was envisaged.

Closed-Circuit Television (CCTV)

At the most basic level, CCTV can be defined as surveillance systems composed of a “network of cameras and components for monitoring, recording and transmitting video images” (McCahill & Norris, 2002: 38). Caplan, Kennedy and Petrossian (2011),

replicated and expanded somewhat on this definition by indicating that CCTV could be: “any instrument, apparatus, equipment, or other device that is connected electronically from the image capture device to the display device that is capable of being used to visually observe an activity” (Caplan et al, 2011: 257-270).

Image 1.1: A street pole with CCTV cameras mounted at the top



(Photo by Victor Garcia, 2019).

The above type of CCTV camera has an impressive high-tech license plate recognition feature that can scan the number plates of about 480 passing vehicles per minute (Parker & Federl, 1997). Then, by using fast built-in internet connectivity, the vehicle number plate images are checked against the SAPS' database of stolen vehicles, forged plates and even suspects on the wanted criminals list.

Image 1.2: Typical CCTV installation in a suburb



(Photo by Victor Garcia, 2019).

The above image is of a typical CCTV camera installation in residential suburbs or along streets.

Crime prevention

Crime prevention is a term describing techniques used for reducing victimisation as well as deterring criminals and preventing further crimes being perpetrated by them (Gill, 2016: 43). It is applied specifically to efforts made by governments to reduce crime, enforce the law and maintain criminal justice. Obviously, crime prevention is including any initiative or policy which reduces or eliminates the aggregate level of victimisation or the risk of individual criminal participation (Bowers & Johnson 2016: 133). It includes government and community-based programmes to reduce the

incidents of risk factors correlated with criminal participation, the rate of victimisation, as well as efforts to reduce perceptions/fear of crime (Van Rooyen, 2013: 17). Accordingly, crime prevention comprises of strategies and measures that seek to reduce the risk of crimes occurring and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes (United Nations Office on Drugs and Crime (UNODC), 2010: 45).

Evidence

Gilbert (2004: 58) defines evidence as anything properly admissible in a court of law, which will aid the function of criminal proceedings in establishing guilt or innocence.

Investigation

According to Marais and Van Rooyen (2013: 17), investigation is the systematic search for the truth with a basis of objective and subjective traces.

Personal data

According to the Protection of Personal Information Act (Act 4 of 2013) (known as the POPI Act), personal information means information relating to an identifiable, living, natural person or non-juristic person (e.g. a company).

Surveillance

According to National Instruction 3/2010 of the South African Police Service (SAPS, 2010: 1), surveillance is a covert method used to observe people continuously, including places and properties, with the purpose of gathering information.

1.8 CHAPTER OUTLINES

Chapter 1: General orientation

This chapter serves as an introduction and background motivation for the study. It clarifies important concepts, establishes a brief motivation for the study and outlines the problem statement. The researcher introduces the phenomenon, explains the

rationale of the study, problem statement, puts forth research aims and objectives, research questions and key theoretical concepts are clarified and sets the course of the dissertation. This chapter also gives some geographic context of Johannesburg and Tshwane to give some context about the locations under discussion throughout this study.

Chapter 2: Research methodology and design

Chapter Two outlines the research methodology adopted. The researcher opted for a qualitative approach utilising both inductive analysis and empirical design. The chapter further presents details of the research design, target population, sample and sampling procedures, description of research instruments, validity and reliability of instruments, data collection procedures, data analysis techniques and ethical considerations. The theoretical underpinnings for the use of CCTV will be another area that was examined in this chapter.

Chapter 3: Literature review: CCTV surveillance

This Chapter examines existing literature relating to CCTV, both in the South African jurisdiction and from an international perspective. In addition, the legislative position regarding public (street) CCTV systems from an operational, regulatory and data protection perspective and the current guidelines and operating protocols for public CCTV systems were examined and outlined in this chapter.

Chapter 4: Research findings: data analysis and interpretation

Chapter Four presents the findings of the research and an analysis and discussion of those results, impact, significance, implications for crime prevention initiatives. It also provides an analysis and interpretation of the interviews conducted and the street survey questionnaires that were administered.

CHAPTER 2

RESEARCH METHODOLOGY AND RESEARCH DESIGN

2.1 INTRODUCTION

The study involved evaluating the use, impact and effectiveness of Closed-Circuit Television (CCTV) Surveillance Systems in crime management and the level of public perceptions about its effectiveness in deterrence, detection, delay and response to criminal activities in both central business districts and residential areas, as well as public streets in the areas in the two selected research sites (Johannesburg and Tshwane). Accordingly, several research methodologies were implemented and applied for the collection of the requisite research information and data.

Creswell (2013: 56) argues that the choice of method is influenced by numerous factors including whether the intent is to detail the type of information to be collected in advance or whether to allow it to emerge from the study. Creswell further asserts that one needs to consider the full range of data collection possibilities (Creswell, 2013: 30).

2.2 RESEARCH DESIGN

After careful deliberation, the researcher felt that this study would be best served and suited by using both an exploratory and evaluation research design, primarily through a qualitative research approach (Creswell, 2014: 23).

Subsidiary to this was a quantitative approach as applied by applying coding and statistical analysis to responses, for the street survey questionnaires administered. Then, the research design is best described as the use of a 'mixed-methods' approach. The notion of mixed methods or multi-methods approaches is an approach that brings together the value and benefits of both qualitative and quantitative approaches, whilst at the same time providing a middle solution for many (research) problems of interest (Creswell, 2013: 113).

By mainly adopting a qualitative research approach, the researcher felt that this would assist in answering different types of questions, the collection of research information/data and undertake document analysis.

The current study was further shaped by using an inductive research design. The research analysis method employed was implemented through detailed one-on-one interviews based on a schedule of interview questions and applied analysis to responses in order to arrive at resulting findings of the research. The simplest definition of an 'interview' is a "conversation where questions are asked and the corresponding answers are given and it involves two parties: the interviewer and interviewee" (Creswell, 2013: 50). In the qualitative paradigm, interviews are often seen as one of the best ways to "enter into the other person's perspective" (Patton, 2000: 3410). Consequently, the research was designed to achieve the aims and objectives as set out by the researcher in Chapter 1.

In addition, based on a reading of Davidson (2000: 45), a phenomenological methodology was identified as the best research design theoretical approach for this type of study. This theoretical design was chosen for the purpose of describing the meaning of people's lived experiences of a concept or phenomenon. Hence, by focusing on identifying and analysing what all the participants have in common as they experience a phenomenon for a better overall understanding of participants' 'lived experiences' (Leedy & Ormrod, 2010: 18). (See more detail on the chosen theoretical framework outlined in a later section below).

2.3 RESEARCH APPROACH

Baškarada (2014: 12) is of the opinion that the "qualitative research paradigm has increasingly served as a unique option for knowledge sharing and academic debate over the years". An interview guide and questionnaire design, with open-ended questions, was used to explore the usage of CCTV surveillance systems for anticipated benefits of crime prevention and control.

The review of the literature related to the use of CCTV surveillance systems for crime prevention and control in public and private space revealed that there are a myriad of CCTV technologies currently in use by law enforcement agencies. Yet, no uniform standard for CCTV evaluation exists that has, so far, been followed. The preliminary intention of this research study was to gather data regarding the views and opinions of research participants about the utilisation of CCTV surveillance in crime prevention and control. Accordingly, the researcher elected to primarily adopt a qualitative approach to assist the researcher in obtaining a deeper understanding of the issues being investigated. This decision was based on the choice and understanding that such an approach is non-numerical (i.e. non-statistical methods of enquiry and analysis of social phenomena) (Creswell, 2014: 23), though findings may be presented in a graph/tabular format.

Subsidiary to this was a quantitative approach as applied by applying coding and statistical analysis to responses, for the street survey questionnaires administered. Then the research design is best described as the use of a 'mixed-methods' approach. The notion of mixed methods or multi-methods approaches is an approach that brings together the value and benefits of both qualitative and quantitative approaches, whilst at the same time providing a middle solution for many (research) problems of interest (Creswell, 2013: 113).

By mainly adopting a qualitative research approach, the researcher felt that this would assist in answering different types of questions, collect data and undertake document analysis. This type of research approach is conducted in natural settings (Creswell, 2014: 23), in other words researchers collect data in the field at site where participants' experience the issue or problem under study. The data collected is non-numeric as compared to a purely quantitative approach.

As a result, the researcher undertook to visit participants at their workstations subject to pre-arrangement/appointments made and certain circumstances when permission was granted. The issue of permission is crucial since the researcher wanted to collect,

by means of examining on-site documents and observing behaviour in a natural setting (of interviewees).

2.4 THEORETICAL AND CONCEPTUAL FRAMEWORK

The views, beliefs and thoughts of residents and the key representatives of both residents and operators (in control rooms) regarding CCTV surveillance to be reached by following a string of constructionism/interpretivism/phenomenological theoretical framework with reference to the following factors:

- The study examines a relatively small, purposive sample;
- The study measures intensively with relatively unstructured instruments; and
- The results of the research are presented mainly in words (textual thematic analysis of responses) (Creswell, 2013: 13).

It is hoped that the results will reflect realities as perceived by the participants/respondents/interviewees. According to the purpose of the research, this study will then largely follow an exploratory/descriptive study path. According to Babbie, (2011: 58), “[a]n exploratory study intends to explore what is happening; to seek new insights; to ask questions and to assess the phenomena in a new light”. This intended exploratory study will be valuable particularly since, in South Africa, there has been limited research undertaken on the research topic (CCTV surveillance impact on crime prevention and crime reduction) and there is very little information known about the phenomena per se (see further discussion on studies and published literature in Chapter 3).

2.4.1 Phenomenological Theory

The above includes using the Phenomenological Theory as the qualitative approach to investigate the phenomenon of CCTV surveillance systems. The operative term in a phenomenological study includes descriptive methodology to measure and

investigate the perceptions, awareness of the target population and selection of an appropriate sampling size. The descriptive method was suited to this type of study and measured and investigated what existed through the lived experiences of the subjects. A phenomenological study was chosen for several reasons: because it gives the meaning of lived experiences for individuals and focuses on common experiences of participants through the collection of data (Creswell, 2013: 59 & 68).

“Phenomenology provides a deep understanding of a phenomenon as experienced by several individuals” (Creswell, 2013: 62). Since it is concerned with the meaning of people’s lived experiences of a concept or phenomenon, the researcher employed this research design which focuses on identifying and analysing what the participants have in common as they experience a phenomenon. According to Welman and Kruger (1999: 189), “the phenomenologists are concerned with understanding social and psychological phenomena from the perspectives of people involved”. This is to be done by reducing “individual experiences with a phenomenon to a description of universal essence” (Creswell, 2013: 23) or, in other words, a “grasp of the very nature of the thing” (Creswell, 2014: 56). Specifically, the researcher utilised Psychological Phenomenology (also termed Empirical or Transcendental) as expounded by Moustakas (1994: 67, as cited in Creswell, 2013: 54), which focuses less on the interpretations of the subjects and more on a description of the experiences of the participants.

2.4.2 Five environmental criminological theories

Five environmental criminological approaches were used to explain how CCTV can, theoretically, reduce crime, namely:

- i) rational choice;
- ii) routine activities;
- iii) crime pattern analysis;
- iv) situational crime prevention (as deterrence); and
- v) Crime Prevention Through Environmental Design (CPTED).

i) Rational Choice Theory

Cornish and Clarke (2003: 41 & 50) postulated the Rational Choice Theory, which is based on the assumption that “offenders seek to advantage themselves by their criminal behaviour”. Rational Choice Theory, similar to the Routine Activity Theory, is formulated on the concept of the offender being a rational actor undertaking a cost benefit analysis at a given time and place to assess whether there is the opportunity to offend.

The main tenets of the Rational Choice Theory being that adversaries act rationally when planning a crime by weighing the risks, rewards and effort needed to commit their crime(s) (Clarke, 1997: 15).

The Rational Choice Crime Prevention Theory, developed by Roland Clarke, explains that adversaries using a hedonistic calculus during their decision-making process in selecting targets will act in their own best interests. Under this circumstance, security officers should therefore, understand this calculus, manipulate it and use it to their advantage. In view of this, Rational Choice Theory denies the existence of any kind of action or force other than the purely rational and calculating offender (Clarke, 1997: 34).

However, despite this portrayal of offenders as rational decision makers who base their actions on the costs and benefits they perceive in the contemplated activity, research suggests that offenders do not necessarily construct detailed plans for each offence (Steven, 2010: 51). Rather, rational choices and preconceived plans may be set into motion when the offender happens to come across a situation or target which fits the general description of an appropriate target.

Accordingly, CCTV surveillance is grounded in the criminological theory that suggests potential offenders are less likely to commit crime if they believe they are being watched or have a greater risk of being apprehended.

ii) Routine Activity Theory

Routine Activity Theory, postulated by Cohen and Felson (1979: 588-608), posited that for a predatory crime to occur three elements must be present, namely: a likely or motivated offender; a suitable target and the absence of a capable guardian. Felson (1987: 915) subsequently refined the theory with the addition of a fourth element, that of the “intimate handler”.

From a routine activities’ viewpoint, it is proposed that camera surveillance acts as a capable guardian. Given the presence of a capable guardian, offending behaviour will not occur even if a likely offender and suitable target converge in space and time (Cohen & Felson, 1979: 588-608; Felson, 1987: 925). Routine Activity Theory explains the occurrence of a crime due to the spatio-temporal convergence of three elements: A motivated offender, a suitable target (victim), and the lack of capable guardianship.

The basic premise of Routine Activity Theory is that the changes in routine activities associated with the increase in small households and two-income families, has increased the opportunity for property crimes mostly. Naturally, the density of offenders, attractive targets, and ineffective guardianship is not randomly distributed across space. Some places offer more crime opportunities than others.

In this theoretical context then, the CCTV security camera is a proxy for guardianship.

iii) Crime Pattern Theory

Crime Pattern Theory takes into consideration both routine activity and rational choice theories and explores the dynamic of criminals becoming aware of opportunities for crime in the course of their daily routine activities rather than making a special trip to perpetrate specific crimes (Brantingham & Brantingham, 1993: 128).

iv) Situational crime prevention

One of the principal advocates of Rational Choice Theory, Ron Clarke, also championed the situational crime prevention approach. The situational crime

prevention approach, under-pinned by the rational choice, routine activities and crime pattern analysis theories, seeks to make objects “crime resistant” via managed methods of crime prevention, including target hardening, environmental design, surveillance and crime pattern analytics.

Situational prevention comprises of opportunity-reducing measures that are:

- directed at highly specific forms of crime;
- involve the management, design or manipulation of the immediate environment in as systematic and permanent way as possible;
- make crime more difficult and riskier, or less rewarding and excusable as judged by a wide range of offenders (Clarke, 1997: 40).

From a situational crime prevention viewpoint, it is proposed that CCTV increases the perceived risks associated with offending in locations under camera surveillance since it increases the likelihood of detection (Clarke, 1997: 31 & 45).

Clarke and Eck (2003: 18-27) outlined the twenty-five techniques of situational crime prevention which fall into five main groups, through which the techniques achieve their preventive effect, namely: increasing the effort to commit crime; increasing the risks; reducing the rewards; reducing provocations; and removing excuses.

CCTV is a type of situational crime prevention strategy in which levels of formal surveillance are increased within a targeted area (Cornish & Clarke, 2003: 67; Welsh & Farrington, 2009a: 717). Situational crime prevention is focused on preventing crime by reducing criminal opportunities in a targeted area and increasing the risk of offending through modification of the physical environment (Clarke, 1995: 176). The situational prevention of crime is mainly rooted in the rational choice perspective, in which crime is considered to be “purposive, in which behaviour designed to meet the

offender's commonplace needs" (Clarke, 1995: 180). According to Welsh and Farrington, (2009: 40), the suggested strategic aspects of CCTV schemes may be as important as the environmental setting. In addition, Piza (2018: 16) noted that because CCTV sites are permanent fixtures (hard wired to physical structures and configured to wireless communication networks), moving locations after use, would require additional costs. Agencies usually install cameras at locations of their choice, without giving prior consideration for these detracting factors.

The above theories allow one either to focus on offenders or victims, but they do not focus exclusively on either of them, since overall, they are concerned with the convergence of offenders and victims in place and time.

v) Crime Prevention Through Environmental Design (CPTED)

The theoretical concept of Crime Prevention Through Environmental Design (CPTED) is also relevant in the context of CCTV surveillance and should not be overlooked. Following earlier work by Jacobs (1961: 80), CPTED was developed by Jeffrey (1971: 56) who coined the phrase: "crime prevention through environmental design" and Newman (1972: 13) who developed the idea of "defensible space". CPTED is concerned with designing out crime generating factors from the built environment and surveillance is one of its integral principles.

McCahill and Norris (2002: 78), for instance, have postulated three theoretical approaches to the use of CCTV surveillance. Firstly, they draw on sociological literature and Michel Foucault's analysis of Bentham's Panopticon, where they link the disciplinary potential of the Panopticon to the use of mass surveillance systems. Norris and Armstrong (1999: 60) argue that the extent to which CCTV systems mirror panoptic principles in their operation and effects depends on a number of issues including the fact that the area being monitored is not a closed space; that the watchers are not generally in a position to directly intervene; and that the watchers have little if any information on those being observed.

2.4.3 Case study approach

In addition, to the exploratory, inductive study design and using the phenomenological paradigm, this study was complemented by utilising case studies as a research methodology to fulfil the overall aim of the research.

This case study seeks to understand and interpret how stakeholders in selected areas make use of CCTV surveillance systems for crime prevention and control by considering their lived experiences. It is an approach that will enable the research questions to be answered by providing a rich picture of the actual conditions surrounding CCTV surveillance practices in the identified case studies. The target population for this research would be CCTV surveillance monitors, Community Police Forum members and the public.

In the research site areas, selected case studies were used to evaluate the use of CCTV surveillance systems for crime control and prevention in the selected research site areas in the cities of Johannesburg and Pretoria (Tshwane) in the Gauteng Province.

Babbie and Mouton (2001: 21), argue that the objective of case study research is to “investigate the dynamics of some single-bounded systems, typically of a social nature, such as a family, group, community and participants in a project”. Yin (1994: 34), states that a case study permits a research study to “retain the holistic and meaningful characteristics of real-life events”.

2.5 RESEARCH METHODS AND DATA COLLECTION TOOLS USED

Data collection methods relates to how the data were collected (Creswell, 2013: 45). Primary and secondary data was collected by the researcher. According to Creswell (2013: 39), primary data refers to original data obtained first-hand by the researcher. Conversely, secondary data is data obtained/found in secondary sources (for example: logbooks, incident registers, case dockets and literature or information

collected by individuals or agencies and institutions, other than by the researcher themselves (Creswell, 2014: 49).

The researcher used a combination of both, which led to the application of the concept of triangulation. Triangulation, according to Leedy and Ormrod (2010: 50), triangulation or the use of multiple methods, as a plan of action, raises sociologists above the personal biases that stem from one single methodology. The combination of multiple (mixed) methods and techniques can overcome the deficiencies that can flow from utilising only one method/approach.

Welman and Kruger (2001: 67), state that the purpose of using triangulation is to use the results from each utilized method of data collection and attempt to corroborate the resulting findings according to each method's analyses as applied to the collected research information.

For the research information/data collection for this study the researcher used the following methods and instruments of data collection:

- document analysis (including review of available published literature);
- face-to-face interviews (based on standardised schedules of interview questions) (see Annexures G &H);
- street survey questionnaires (see Annexure I); and
- onsite observation.

2.5.1 Document analysis/literature review

In doing literature searches, the researcher decided to break down the topic into the main concepts of the study, such as:

- surveillance;
- closed circuit television (CCTV); and
- private security control rooms.

With these core search terms, the researcher visited the various resource centres of the university to locate available material on the selected title/research topic. Several relevant books and journal articles on the chosen topic were found. The researcher consulted the Open Shelf collection catalogue at Unisa library, under the search term: 'surveillance'. Additional searches of electronic bibliographic databases, as well as manual searches of CCTV evaluations study bibliographies were undertaken. As the research study progressed, the researcher conducted further manual searches of each study/publication obtained for potential inclusion.

The following databases were searched: Criminal Justice Abstracts and National Criminal Justice Reference Service (NCJRS).⁶ These databases were selected since they had the most comprehensive coverage of criminological, criminal justice and social science published literature.

The researcher also checked relevant journals, intranet and internet, including websites dealing with surveillance studies' issues, including criminal justice websites on a broad range of topics relating to CCTV (in particular of literature reviews on the effectiveness of CCTV in preventing crime; admissibility and evidence; and issues of the privacy of information); for any material relevant to the topic under research.

The researcher also extensively perused journals, such as *Surveillance and Society* and local newspaper articles, in search for any information on the use of CCTV surveillance systems for crime control and prevention.

In addition, both published and unpublished reports were considered in these searches.

⁶ See National Criminal Justice Reference Services (NCJRS), Office of Justice Programs (OJP) of the US Department of Justice (DoJ) publications/abstracts lists available at: <https://www.ncjrs.gov/App/Publications/AlphaList.aspx#>.

By reviewing all available related literature, such as books, periodicals and online journals and studies, provided the researcher with an in-depth background and meaningful answers to the research problems.

2.5.2 Face-to-face interviews

In structured face-to-face interviews the interviewer asks each respondent the same questions in the same way. This is the most basic and most common face-to-face interview type. A structured interview may include open-ended and closed-ended questions. This type of interview is usually used for large projects for which the researcher wants the same data to be collected from each respondent (Zorn, 2010: 35). This was not the researcher's choice for this study. For this study semi-structured interviews were preferred by the researcher since they offered convenience (Creswell, 2013: 27) and assist in the correct gathering of focused, qualitative textual data (Leedy & Ormrod, 2010: 12). Another advantage of their usage being that semi-structured interviews are "fairly reliable and easy to analyse" (Creswell, 2014: 30). This method offers a balance between the flexibility of an open-ended interview and the focus of a structured ethnographic survey questionnaire (Creswell, 2013: 50). Information from research methodology literature on qualitative research suggests that a total of 25 to 35 interviews is enough to conduct research using the qualitative approach (Creswell, 2014: 39).

The aim of the usage (in this study) of a face-to-face research interview instrument was for the better identification of insights into an issue (study topic) from the perspective of participants/respondents (Creswell, 2014: 34). In this study the researcher used face-to-face interviews based on a standardised schedule of interview questions as the primary research information collection method. Among those identified to be interviewed included: CCTV operators (in control rooms); private security companies; and individuals (both residents and members of local CPF) in residential areas. Accordingly, a schedule of interview questions (see annexures G & H), (two sets slightly differing in accordance with target populations identified for interviewing) was prepared for implementation in the field.

The developed schedule of interview questions contained a series of mostly open-ended questions based on the topic of study (there were a few close-ended questions, largely in the biographical information section (Section A), but some close-ended questions were followed by a secondary open-ended question requesting motivation for the answer in the close-ended question. Accordingly, the researcher opted for semi-structured face-to-face interviews with CCTV operators, and a similar one with some changed questions with a different focus for residents and members of local CPFs for residential areas. (Annexures G & H).

The schedules of interview questions consisted of 39 (Annexure G) and 33 questions (Annexure H) respectively, with the last 32 (Annexure G) and 30 questions (Annexure H) asked the participants to state their perception of CCTV's role and objectives within their company's operations or organisation to which affiliated. The intent was to understand whether the participants perceived a difference between roles and objectives, and if there was a different perception at the various work levels (Annexure G) and respondents (Annexure H) about the installation of CCTV surveillance cameras in their neighbourhood/residential area.

The researcher, in undertaking each individual interview, attempted to create a positive and conducive atmosphere for the interview, namely by: Firstly, introducing himself to the identified potential interviewee. Secondly, by stating the aims, objectives and purpose of the study, as well as his relation (postgraduate research student) to the research study.

During the interviews the researcher implemented the following:

- used mainly open-ended questions in order to obtain lengthy and descriptive answers rather than using close-ended questions (i.e. those that only require 'yes' or 'no' answer);

- avoided posing leading or ambiguous questions;
- used terms that participants could easily understand, given their knowledge, language skills, cultural background, age, gender, etc.;
- was mindful of the social or cultural contexts of all questions posed to the interviewees;
- tried to have a one-on-one interaction with the interviewee (Creswell, 2014: 41).
- tried to understand something from the subjects' point of view and to uncover the meaning of their experiences (Pandey & Pandey, 2015: 1-30); and
- if permission granted use was made of a digital audio recorder for verbal recording purposes (for facilitating ease of later transcribing of interviews). If such permission was not granted the researcher made fieldnotes of the interviewee responses.

Furthermore, during the interviews, interviewees/respondents were free to express their views even on topics not included in the schedule of interview questions. Finally, the researcher endeavoured throughout the interview process to allow the interviews to flow smoothly.

This semi-structured interview format allowed the interviewer to pose some open-ended questions and the interviewee to express his/her opinion freely. This required both the interviewer and the interviewee to be at ease to create an interview environment similar to a discussion or 'brainstorming' session on the given topic. This interview technique allowed the researcher to delve deeper into the knowledge and information seeking process compared to other methods, such as surveys/focus groups (Creswell, 2013: 67).

Although the face-to-face interviews, used in this study, focused on key topics, there was also the opportunity provided to interviewees to discuss, in more detail, some areas of interest (Creswell, 2013: 41). A further advantage of the face-to-face interview technique was that it allows for the clarification of responses by probing (sometimes prompted by clarifying (additional) questions posed by the researcher), which tend to result in fewer missing responses (Creswell, 2014: 68).

This means that the responses are, correctly, from the participant's perspective, not influenced by the researcher doing the interview. The primary benefit of personal interviews is that they encompass personal and direct interaction between interviewees and the interviewer. This also helps to exclude non-response rates (Creswell, 2014: 53).

By using this method, it was hoped to gain a better understanding of the research topic and the further exploring of issues raised by interviewees/participants. Study participants were given the opportunity to choose a location of their own convenience for the interview. All interviews, upon permission being granted to do so, were digitally recorded and then later electronically transcribed. All interviews were transcribed verbatim and, although certain semantics were eliminated, most were left intact (verbatim) as they were recorded. This method enabled the researcher to engage the participant in conversation about a topic in response to the interviewer asking open-ended questions (Creswell, 2013: 41; Kumar, 2011: 90).

2.5.3 Street survey questionnaires

Questionnaire design

The researcher adapted a researcher-assisted self-completion questionnaire (RASCQ) with a paper-and-pencil approach/methodology as based on the street survey questionnaire developed by Minnaar (2008: 1). To answer survey questionnaires, respondents need to comprehend a question, recall the relevant information, evaluate the link between the retrieved information and the question, and communicate their responses (Bowling, 2005: 67). In comparison to self-completed

questionnaires (SCQ), RASCQ reduces the cognitive burden related to the comprehension of questions since the researcher in this study read and clarified questions to the respondents who had agreed to participate, answered questions from respondents, and utilised images (of CCTV cameras on a cellphone) to aid respondents' understanding of the survey questionnaire used in this study.

During the interviews (and the site observations), the researcher made field notes to assist the researcher to analyse the gathered data.

2.5.4 Onsite observation

The researcher also carried out observational methods of data collection and evaluations by observing how individual residents/members of local CPFs residential areas, and CCTV control room operators at private security companies were engaging in their surveillance activities. Four types of data were recorded during the observational period.⁷ The observation period lasted five days, from 10-15 December 2018. At the same time, attention was paid during observation periods, to CCTV's deterrent effect with reference to four types of crime incidents (namely: theft from persons; vehicle theft; burglary; and robbery) occurring in the observation site area and within a 100m (328 feet) radius of each CCTV surveillance camera (for target and control purposes). The quantitative observational period data included information on shift data – number of operators per shift; types of people entering the control room and length of monitoring duties; targeted incident data. In other words: how and why the surveillance was initiated; by whom; characteristics data of observed subjects – age, sex and appearance of individuals from targeted incidents; and deployment data – whether deployment was necessitated and the outcome of any deployment action. Crime data were obtained from control room logbooks and adjacent police stations.

⁷ These categories are closely related to Norris and Armstrong's (1999: 56) study of 592 hours of observation.

2.6 TARGET POPULATION, SAMPLING AND SELECTING OF INTERVIEW PARTICIPANTS

2.6.1 Target population

The researcher decided, because of logical challenges and cost-effectiveness, not to use the whole population of the two selected cities (Johannesburg and Tshwane) for the study and intentionally chose selected areas in Johannesburg and Tshwane for investigation and for conducting research. The target population in this research consisted of CCTV control room operators and members of local CPFs and individuals in the selected residential areas.

2.6.2 Purposive sampling

In this study the researcher used purposive, non-probability sampling, with each member of the target population having a limited chance to be included in the sample but with each member of the sample having the same chance to be chosen (Welman & Kruger, 200: 31). This is consistent with David and Sutton (2011: 196), who defined purposive sampling as a non-probability procedure in which the researcher selects the units of analysis (in this study: members of local CPFs; CCTV operators and individuals from residential areas) to be observed on the basis of the researcher's own judgement about which one from the sample will be the most useful because they have the needed information of interest. On the hand other Leedy and Ormrod (2010: 196) define sampling as the process by which a sub-group from the universe/population is selected from the larger population group which meets the characteristics of the target group from which the researcher seeks information. Sampling is further defined as the process of selecting certain members or a sub-set of the population to draw statistical inferences from them and to estimate characteristics of the whole population (Creswell, 2014: 35).

The researcher primarily utilised purposive sampling techniques so that participants were recruited according to pre-selected criteria relevant to the research questions/characteristics of the sample. Respondents were selected by the researcher at random (non-probability sampling). In other words, the researcher determined the

sample by choosing the respondents according to characteristics in a non-random formula. The researcher used this sampling approach since the selected respondents have features or characteristics which will enable detailed exploration and understanding of the central themes and questions which the researcher wishes to study on CCTV surveillance systems.

In addition, the researcher, after initial contact with a respondent, relied on chain referral sampling (Snowball Sampling) to get hold of more research participants for this research study.

Sampling of CCTV operators

In order to obtain the required data for this study, a request permission to undertake research letter (see Annexure D) was sent to ten companies located in the geographic areas of Johannesburg and Tshwane. Five companies approved the request for their employees to be interviewed and provide information to the researcher. Granted permission was followed by the setting up of appointments with selected CCTV controllers for the purpose of interviewing them. Interviews were arranged with via company directors/control room managers with CCTV operator interviewees being the primary unit of analysis in order to trace additional participants or informants. In other words, Snowball Sampling, as a sampling method of expanding the sample was used by asking one informant or participant to recommend others for interviewing (Creswell, 2013: 42). The purposive sample interviewees were requested to give, at their discretion, the names and contact details of persons based in commerce, industry and/or government who were: a) co-responsible for implementation of CCTV surveillance systems. This included community police forums, church organisations, etc. In order to ensure ethical research was implemented, all potential interviewees were provided with a copy of the Participant Information Sheet (Annexure E) and the Informed Consent Form (Annexure F) to read (Kvale, 1996: 89; Creswell, 2013: 59).

A total of forty participants for the above target population category were interviewed using these face-to-face interviews.

Sampling of CPF members

A total of 40 CPF members/residents were sampled from selected areas of interest in Johannesburg and Tshwane. While 50 were approached and contacted only 40 respondents managed to honour the appointments. These respondents were interviewed at their choice of venue. As for above all participants from this category were first provided with a copy of the Participant Information Sheet and the Informed Consent Form to read. The researcher used the schedule of interview questions designed for this category of participants (Annexure H) to elicit information from them.

Sampling of individuals in CBD streets and residential areas

The researcher administered the street survey questionnaire to elicit information from individuals randomly approached in CBD streets and selected residential areas of Johannesburg and Tshwane. A total of 50 individuals were interviewed using a paper-and-pencil approach of the self-completed street survey questionnaire.

All the survey questionnaires were carried out in a random manner at each location. The researcher was not associated with any of the selected locations and did not personally know any of the survey respondents. The researcher approached likely participants by visiting their workplaces, commercial and residential areas respectively. If the participants provided an initial positive response and volunteered for participation, they were given a copy of the Participant Information Sheet and the Informed Consent Form to read. Once they had read these two forms, they were asked if they understood the research within the context of the letter/information sheet, that participation was voluntary, that they can withdraw at any time during the survey and whether they have any further questions. They were then asked to participate in the research. Although the researcher was present during the initial commitment by the participant to complete the survey questionnaire, the researcher gave no incentives, suggestions or ideas to the participants about how to answer the questions. The only advice offered was to respond to the questions as honestly as possible and that there was no right or wrong answer. The participant was advised that all answers are correct, as the survey was about perceptions and opinions.

2.7 DATA ANALYSIS

Data analysis is a systematic and essentially taxonomic process of sorting and classifying the data that have been collected (Bogdan & Biklen, 2006: 66).

All interviews were transcribed by the researcher which provided the opportunity for the researcher to reflect on the data gathered and to identify emerging themes and patterns. open-ended questions and comments generated by the respondents were analysed in a similar manner to the data gathered from the interview process. This is in consistent to a statement by Boeijie (2010: 76), who defined data analysis as the process of systematically searching and arranging the interview scripts, fieldnotes and other materials that the researcher has accumulated to increase his own understanding of them, to enable the researcher to present to others.

The researcher undertook thematic analysis. Accordingly, the researcher sorted and categorised field notes, interview transcripts in a systematic way. The aim is to transform raw data into findings. Participants responses were subjected to: Thematic / content analysis generating 'codes' that describe themes in the text, such as 'safety'; 'crime prevention'; and privacy. The researcher made use of interview schedules of questions and a questionnaire design. This alleviated the challenges of misprint by participants and it was self-administered by the researcher taking into consideration narrative expressions/responses by participants. After the completion of interviews, the researcher applied data checks, check for outliers and edited the raw research data to identify and clarify any data points that may hamper the accuracy of the results.

In accordance with this principle, the researcher organised the data obtained by breaking down the research questions by concepts, with the use of index cards, and further breaking down the large bodies of text into smaller units such as phrases. The researcher read the data several times to obtain a perspective of the whole and wrote down notes on the data. Themes and sub-themes were identified, and the data was organised according to these themes, which gave the researcher a general sense of the emerging patterns of the data.

2.7.1 Qualitative content analysis

In this study, the researcher made use of the data analysis spiral method (Creswell, 2013: 65). In accordance with this principle, the researcher organised the data – which he obtained by breaking down the research questions by concepts, with the use of index cards, and by breaking down the large bodies of text into smaller units, such as phrases. The researcher read the data several times to obtain a perspective of the whole dataset and wrote down notes on each section of the data. Themes and sub-themes were identified, and the data was organised according to these themes, which gave the researcher a general sense of patterns of the data. The researcher then integrated and summarised the data for the reader (Creswell, 2014: 45).

2.7.2 Data coding

The collected interview responses were transcribed and collated in accordance with the schedules of interview questions and street survey questionnaire themes/categories. Within specific questions with multiple responses, those relevant to the analysis were coded to obtain an overview statistical analysis to go with the textual analysis and interpretation applied.

For each question a coding scheme was designed based on the categories (quantitative). For analysing qualitative data, the researcher went through a process called content analysis of the contents of an interview in order to identify the main theme. This process involves several steps:

- 1st Step: Identify the main theme;
- 2nd Step: Assign code to main theme;
- 3rd Step: Classify responses under the main theme;
- 4th Step: Integrate themes and response into the text of report.

A file with divisions for the various interviews was opened and the following hard copy documentation was filed with the following information:

- notes made during the interview;
- the field notes made after each interview;
- any notes or sketches that a participant made during the interview, which the participant gave to the researcher;
- any additional information that the participant offered during the interview, for example, brochures, pamphlets or company operational and/or policy documents;
- any notes made during the 'data analysis' process, e.g. grouping of units of meaning into themes;
- the draft transcriptions and analysis of the interview presented after the first interview to the participants for validation; and
- confirmation of correctness and/or commentary by the participant about the transcript and "analyses" of the interview.

2.8 VALIDITY AND RELIABILITY

2.8.1 Validity

Validity concerns the accuracy of the questions asked, the data collected and the explanation offered. Generally, it relates to the data and the analysis used in the research (Denscombe, 2002: 100). According to Melville and Goddard (1996: 37), validity means that the measurements used in the research are correct. Bailey (1996: 238) is of the opinion that one can determine accuracy in considering validity. Validity further refers to the degree to which evidence and theory support the interpretation of test scores entailed by use of tests (Creswell, 2014: 45). The validity of a research instrument (e.g. interview schedule of questions or a survey questionnaire) is the extent to which it measures what is supposed to be measured and that the participants interpret the questions as the researcher intended (Creswell, 2014: 34). According to

Babbie and Mouton (2001: 34), validity is the accuracy and meaningfulness of inferences, which are based on the research results. It is the degree to which results obtained from the analysis of the data represent the variables of the study (Babbie & Mouton, 2001: 38). This view is also replicated by Creswell (2013), who provided the following categories of validity that are paramount in any research study:

- Content validity: The content of the data collected provides adequate coverage of the investigative questions guiding the research study (answer research questions).
- Criterion validity: The measures used for prediction and/or estimation are relevant, free from bias, reliable and existing (answers are true reflection of respondents' perceptions).
- Construct validity: The data reveals the true answers provided by respondents (answers given are actual answers of respondents) (Creswell, 2013: 318-321).

2.8.2 Reliability

Reliability is the ability of a research instrument to consistently measure characteristics of interest over time. It is the degree to which a research instrument yields consistent results or data after repeated trials. If a researcher administers a test to a subject twice and gets the same score on the second administration as the first test, then there is built-in reliability of the instrument (Creswell, 2014: 18). Reliability is concerned with consistency, dependability or stability of a test (Babbie & Mouton, 2011: 72).

The researcher measured the reliability of the questionnaires to determine their consistency in testing what they were intended to measure. To establish reliability, survey questions and face-to-face pre-arranged and predetermined questions (schedule of interview questions and questionnaire design) was moderated by Prof Minnaar (supervisor of the research study). In order to ensure trustworthiness and authenticity of data, information obtained from interviews, literature study and

document analysis (such as incident registers and occurrence books) was used in a combined manner to establish patterns and trends (Creswell, 2014: 49). The researcher looked for common themes in the information collected through the following two methods:

- interviews; and
- literature studies.

The reliability and accuracy of the data was further enhanced by the fact that all participants were interviewed with the same questions contained in the same schedule of interview questions and questionnaire. The researcher, moreover, ensured further reliability by personally evaluating all the results and conducting all the interviews himself. This ensured that they were all conducted in the same way. Feedback was sought from colleagues in the field of study to determine whether they agreed or disagreed that the research had made appropriate interpretations and had drawn valid conclusions from the collected data. Conclusions were then taken back to the participants after the analysis to validate whether they agreed with the conclusions, and for them to evaluate whether the conclusions made sense in their own experiences (Leedy & Ormrod, 2010: 100).

Additionally, before administering in the field, to establish validity and reliability of the research instruments, a panel of nine experts in the field of security science were used to test them. The panel members were given the initial schedule of interview questions and the survey questionnaire as a pre-test and requested to read the questions for validity and construct. According to Rea and Parker (2005), a pre-test is a smaller scale distribution of the questionnaire to a convenience group, in this case the panel of experts (Rea & Parker, 2005:56).

The panellists then returned the questionnaires with written comments and these questions were also moderated by the supervisor from the original survey. Five questions were eliminated from the final research version of the research instruments.

These five being redundant and unnecessary and not directly related to the subject matter of the study. Corrected versions of the questionnaires were finalised and included in the questionnaires' design, and accordingly prepared for test distribution (self-administered by researcher) to the respondents.

To measure the correctness of this research, the researcher conducted interviews, case studies and consulted literature. The researcher conducted personal interviews with the samples, and their responses were recorded. To ensure validity of the literature, the researcher used only information that was obtained from literature consulted, which was relevant to address the research questions and the aim of the study. Leedy and Ormrod (2010: 99) explain that a multi-trait multi-method is made use of when two or more different characteristics are each measured using two or more different approaches. The researcher used the triangulation approach of analysis and applied it to the collected data, which constitutes a multi-trait- multi-method, whereby data is collected from multiple sources. Triangulation, as explained by Leedy and Ormrod (2010: 99), will further enhance validity whereby multiple sources of data are collected, namely: literature, interviews, surveys and site observation and perusal of available relevant literature on the topic. All the interpretations, analysis and conclusions were made based on data gathered from the interviews, literature and case studies (Babbie & Mouton, 2001: 110). The research instruments used were validated in terms of qualitative content analysis. The content related technique measures the degree to which the questions' items reflected the specific areas covered. In order to ensure trustworthiness and authenticity of data, information obtained from interviews, survey and literature consulted was used in a combined manner to establish patterns and trends (Creswell, 2014: 49; Bouma, 1993: 47). The researcher looked for common themes in the information collected by the application of analysis and coding to the data.

2.9 ETHICAL CONSIDERATIONS

Leedy and Ormrod (2010: 101-104) explain that most ethical issues pertaining to research studies are covered in the following categories:

According to Creswell (2009:87) and Leedy and Ormrod (2010:101-104), ethical guidelines must be followed by the researcher at all times. The researcher did adhere to the following ethical issues during research:

- Protection from harm: All participants were safeguarded from physical harm. The researcher conducted the interviews under circumstances where the participants were comfortable and not exposed to stress or embarrassment.
- Informed consent: All respondents was informed on what the research study is about. Participation in this study was voluntary. Participants were given sufficient information concerning the research in order to help them to make an informed decision regarding their participation. Participants could withdraw at any stage. The necessary consent from the participants was obtained in writing.
- Right to privacy: participants were assured that responses given will be treated with confidentiality No response by a participant will be disclosed in a manner that exposes the specific participant. The researcher allocated a code number to participants to honour their privacy.
- Honesty with professional colleagues. Researcher did not fabricate data to support a specific finding. All sources used in this research are acknowledged to avoid plagiarism.
- The researcher ensured that identifying information on the survey, including the identities of the research participants and their affiliated institutions, remained confidential.

All participants in the interviews and survey questionnaire participation were first provided with a copy of the Participant Information Sheet and the Informed Consent Form to read. Therefore, all persons interviewed were given enough information regarding the research project and their consent obtained prior to each interview. In addition, each interviewee was informed that their participation was voluntary and the researcher also provided an assurance that all views and opinions expressed would be anonymous and used for this research only, i.e. no identities of participants would be revealed.

The researcher was also conscious of his own position in personally knowing some interviewees (from previous work experiences in the private security industry). However, the researcher was also confident that this did not in any way present any ethical dilemmas for the research or be a restriction to participants interviewed at their place of work areas or impact on their willingness to provide information.

Kvale (1996: 67) remarked that, in order to ensure ethical research, one must make use of informed consent (Kvale, 1996: 15). Bailey (1996: 45) further observes that deception might prevent insights, whereas honesty, coupled with confidentiality, reduces suspicion and promotes sincere responses. The informed consent form was explained to all participants at the beginning of each interview. Most potential subjects signed the agreement and those who did not, were not pressured to further participate in the study. All participants who voluntarily agreed to participate also were in accord with its content and signed accordingly.

In the light of the above the researcher had then informed all participants – the residents from selected areas, CPF members, security personnel of private security companies and the CCTV operators/data controllers in these companies' control rooms – of the purpose, nature, data collection methods and extent of the research prior to undertaking any interviews or survey. The acceptance of participation was then obtained via a signed informed consent form (see Annexure F).

Accordingly, all potential participants received:

- a signed cover letter informing them of the purpose of study and any implications of their participation (Annexure E). The researcher handed it out to participants to read and provided clarity where necessary;
- a hardcopy handed out by the researcher of the informed consent form (Annexure F) to read and the researcher provided clarity where necessary;
- the option to remain anonymous, i.e. they did not need to give their names, or they could provide a pseudonym; and
- individual interviewee responses were identified in the researcher records by a number assigned to each interviewee/respondent to protect interviewee identities;

Since the ethics of the researcher and the research itself determine the quality of the research inquiry, the researcher had to bear in mind some considerations. Ethical approval was obtained from the College of Law Ethics Review Committee of the University of South Africa (UNISA) (see Annexure A). The research complied with all the ethical codes as set by the committee. The researcher undertook and affirmed not to illegally use or misrepresent any material in the publication of the research study material/collected information and to give proper acknowledgement to any information used. The researcher pronounces that there is no conflict of interests that may endanger the capability to assume the research in a methodical and principled manner. The researcher pronounces that there is no obliteration of partakers' individual human rights or contravention of contributors' benefits and that the appropriate equality in the selection standards of contributors has been measured.

Prior to the commencement of the study, ethical principles in research need to be applied. The current study was subject to certain ethical issues. As was mentioned

earlier, all participants signed their informed consent acceptance forms regarding their participation in the research. Several ethical considerations were considered during the research, primarily the protection of participants' identity (guarantee of anonymity) taking part in the study. It was a requirement that participation in the study was voluntary, that the researcher would not disclose their identities, that an overview of the study was given by the researcher to each participant and that all participants were 18-years and older. Although the questionnaire was designed to be as simple and easy to complete as possible, it was still anticipated that some participants might have experienced some level of stress. To reduce this, it was stated that no question could be answered incorrectly, i.e. that there were no right or wrong answers. These issues were clearly detailed in the study's introductory Participant Information Letter. Participants were only selected if they volunteered and if they complied with the target population criteria.

There were no financial incentives to complete the survey, or researcher bias or deception made during the completion of the interview questionnaires or surveys. It was made clear to the participants that they could withdraw from the study at any time. Also, that their completed interview questionnaire and/or survey questionnaires would remain strictly confidential; that they would not be quoted(i.e. be identified) in any way or form in the resulting research report in a way that might reveal their identities or work affiliations or that the survey information would be released to any other person or organisation.

Creswell (2013: 67) states that the researcher has an obligation to respect the rights, needs, values and desires of the informants. Respect for persons requires that subjects be given the opportunity to choose what shall or shall not happen to them. The researcher informed the participants – the residents and security CCTV operators/data controllers – of the purpose, nature, data collection methods, and extent of the research prior to commencement.

Researchers must be ethically responsible. As Degu and Yigzaw, (2006: 80) explain these:

“Your duty as a researcher is founded on your own set of moral principles. As a researcher you will have a duty to yourself and to the individual who is participating in the research. So even if the outcome of the proposed research is for a good cause, if it involves the researcher lying or deceiving his subjects in some way, then this would be regarded as unethical. The rights [of] the individual are assumed to be all-important, thus a subject’s right to refuse must be upheld whatever the consequences for the research”.

Therefore, the first responsibility of the researcher must be to the individual participants and secondly to report as honestly and accurately as possible what was said by them (Strydom, 2011: 114). The research findings for this study were reported honestly and as accurately as possible.

2.10 LIMITATIONS OF THE STUDY

Despite the resulting findings from this research study, there are several important gaps in our knowledge of the topic in the South African context. One of the primary shortcomings in this respect being that the study was limited by the use only of purposive sampling method employed by the researcher. This study was conducted without using experimental control areas comparing the success of the camera installation on crime in one area, to a similar area without intervention (Taylor, 2010: 34). All the fieldwork research was conducted in selected areas of only two cities, namely: Johannesburg and Tshwane. Purposive sampling provides non-probability samples which receive selection based on the characteristics which are present within a specific population target group and related to the overall focus (topic selection) of this study. It is a process that is sometimes referred to as selective, subjective or judgmental sampling, but the actual structure involved remains the same. The selection criteria the researcher uses can be very arbitrary and are almost always subjective. As a result, firstly, it is unknown whether open-street CCTV works well or

not in non-selected areas. Secondly, it should be made clear that this was an evaluation of selected areas only hence the study's findings cannot be claimed to be representative of *all* CCTV surveillance schemes countrywide. As such, since such a small sample population is often used, a small variation in the sample will cause deviance in the results. With probabilistic sampling, the general probability or odds of a good representation of the population are well established and known. With non-probability data, the general population may not be sampled correctly. It may be harder to evaluate what has been achieved since purposive sampling can be so subjective. It would be methodologically inaccurate to simply apply the findings from this study to the general population. The onus is on the researcher to interpret and discuss the research findings within the context of the research and methodological limitations that are often unavoidable in many of the surveillance studies on CCTV (Welsh & Farrington, 2006: 76).

These limitations include issues relating to sampling and data collection, as well as data quality and analysis. A third methodological criticism is that as a qualitative interpretivist, the researcher had to accept that argument that the descriptive narrative presented is but *one* view of social reality, written from *one* particular perspective. Another individual, researching the same setting, may well have uncovered an alternative set of findings, due to his/her philosophical or theoretical standpoint, personal values and prejudice.

2.11 CONCLUSION

This chapter outlined the research methodology, research design and approach, research methods and research instruments used in the collection of research information/data. It also dealt with the data analysis methods applied to the collected information. Furthermore, ethical considerations involved in the study were presented. In addition, the validity and reliability of information and how it was ensured was discussed. Finally, the limitations in the study were briefly outlined.

CHAPTER 3

LITERATURE STUDY: CCTV SURVEILLANCE SYSTEMS, CRIME PREVENTION AND SECURITY

3.1 INTRODUCTION

CCTV camera surveillance is probably the most rapidly spreading and, at the same time, one of the most controversial instruments in security policing today. This fast-developing technology basically enables an ubiquitous surveillance of public and private space, and security agents benefit from its enhanced capabilities for detecting or retracing criminal activities. Camera surveillance signifies:

- a general extension of public surveillance systems;
- a shift from direct, personal or print surveillance to remote, electronically transmitted, and even computer-enhanced self-monitoring, visual surveillance;
- second-generation CCTV accelerates this process by providing digitalised images that can be automatically processed by recognition software, increasing the scope of surveillance and potentially also reducing monitoring costs (see Norris & Armstrong, 1999; Surette, 2005).
- focusing on the surveillance and deterrence function of CCTV, the economics of CCTV surveillance, based on the traditional economic approach to crime, implies that the dissemination of CCTV camera surveillance enhances control capacities and leads to a partial replacement of human capital by technological investments, thereby increasing the productivity and efficiency of policing behaviour, and thus ultimately reduce crime in the monitored area by deterrence (Department of the Premier and Cabinet, 1999: 1-8).

Although research on CCTV was once sparse/limited, the state of the literature can no longer be described as such. The number of CCTV evaluations has increased

significantly over time. Furthermore, even though public surveillance research in general has been previously described as “methodologically weak, ” with more than 55 percent of studies having less than a comparable experimental-control area design (Welsh, Peel, Farrington, Elffers & Braga, 2011: 82), but of recent times rigorous designs have been increasingly used in the study of CCTV (Welsh et al, 2011: 90). In examining the crime prevention potential of CCTV surveillance cameras. Deterrence Theory provides the blueprint for research in this area, (Clarke, 1997: 23; Welsh & Farrington, 2007: 90; 2009: 43). Under the Deterrence Theory CCTV surveillance system leads to crime prevention because offenders believe cameras may be monitoring their actions, putting them at a disadvantage, with a greater likelihood of apprehension by law agencies (Piza, 2018: 56). In South Africa, and the world at large, there has occurred an exponential increase in the adoption of this technology for crime prevention and control (Reaves, 2015: 46). A study of the available literature reveals that the evaluation of CCTV surveillance systems impact in the US has taken place (see Caplan et al, 2011: 260; La Vigne et al, 2011: 67; Mazerolle, Hurly & Chamlin, 2002: 123). Reaching a firm consensus on the crime prevention capacity of CCTV is somewhat difficult (Caplan et al, 2011: 267), while numerous evaluations have reported some positive outcomes (Ratcliffe, 2009: 46-52). It is reported in literature that CCTV surveillance systems has not produced consistent benefits and, in many instances, there has been little or no evidence of crime reductions (Caplan et al, 2011: 270; Farrington et al, 2007: 45; Gill & Spriggs, 2005: 40).

Given these findings, it is difficult to anticipate the performance of CCTV upon installation. While previous works have called for the identification of precise contexts in which CCTV best performs (Caplan et al, 2011: 269; Gill & Spriggs, 2005; Phillips, 1999: 42); Ratcliffe, 2009: 48-50, Welsh & Farrington, 2002: 75). little has been developed in the sense of ‘best practices’. Inconsistent findings may be due to differences in the utility of individual operations and characteristics of target areas La Vigne et al, 2011: 67). However, Caplan et al (2011: 265) suggested that limitations of common research methodologies may have also contributed to the uncertainty. Estimates from the United Kingdom suggest the presence of over 4.2 million cameras,

a ratio of 1 per every 14 citizens (Piza, 2016: 20). In the United States, 49 percent of local police departments report using CCTV, with usage increasing to 87 percent for agencies serving jurisdictions with populations of 250 000 or more (Reaves, 2015: 72).

Complicating matters in the research on CCTV surveillance is the fact that while research designs have improved over time, the overall body of CCTV research has been classified as methodologically weak (Caplan et al, 2011: 260). In South Africa, CCTV is used in almost all commercial venues, such as hotels, casinos, banks, retail stores, airports, financial institutions, mines, garages, hospitals and shopping centres (Minnaar, 2006: 3).

The United Kingdom, universally regarded as the most surveilled society in the world, provides a substantial portion of the available literature. Further reports from the European Union, United States of America, Canada and Australia are also examined. Unfortunately, from a South Africa perspective, the available literature is rather minimal. Apart from Minnaar (2006), most studies have been carried out by the media and, to date, these reports have not been universally published but have, rather, been retained within the media organisations archives for their own operational reasons (Duncan, 2018a: 34).

One of the drawbacks to the implementation of CCTV surveillance systems in South Africa has been its costs and the inability of the SAPS to fund such implementation in the light of other more pressing priorities and demands on its finances and resources (Minnaar, 2006: 3-5).

A number of reasons/motivation for, have been suggested for the use of CCTV in public spaces, with proponents advocating their potential to deter crime and criminal behaviour, facilitate police and other law enforcement agencies to more effectively analysis in the investigation of crime and facilitate the prosecution and detection of crime. Conversely, opponents argue that they are ineffective as a deterrent (Piza, 2012; Caplan et al, 2011: 256). The literature further emphasis on theories

underpinning the use of CCTV, evaluations of selected studies into the effectiveness and impact of CCTV, governance / regulation and the proliferation of CCTV including the role of government, the media and the public in general. This literature review provides an analytical summary of related theories within CCTV and security. With the need to implement crime prevention strategies containing stronger security measures that are affordable for most municipalities and town councils. This statement above was replicated by Welsh et al (2011: 34), who stated that law enforcement agencies around the world are increasingly making use of the technology of CCTV surveillance systems to improve operational efficiencies, to extend their reach and reduce costs. Welsh et al (2011: 12) further suggested that CCTV surveillance systems have been adopted and adapted for use in public spaces around the world. Many of these systems were initially installed for their presumed deterrent effect on crime and promoted for their beneficial impact on the public's fear of crime. However, at the time they were implemented, there was a dearth of scientific evidence that either supported or disproved these claims. Therefore, there is a need for an independent assessment of whether there is a relationship between the presence of CCTV in the city and public safety. This research study is a response to that need and describes what is known about the effect of CCTV on the public's feeling of safety (Norris & Armstrong, 2012: 56). While a range of potential crime prevention mechanisms have been theorised for CCTV the practical application of CCTV predominately relates to deterrence (Farrington et al, 2007: 42; Ratcliffe, 2006: 72). From a situational crime prevention perspective, notions of deterrence are rooted in the Rational Choice Theory of criminality (Cornish & Clarke, 2003: 72). Whereas deterministic theories view crime as an inevitable byproduct of social ills, rational choice considers crime as "purposive behavior designed to meet the offender's commonplace needs" (Clarke, 1997: 9-10).

3.2 Theoretical underpinnings

Before examining the reasons behind the application and impact of CCTV systems, it is worthwhile to explore the theoretical foundations upon which its use is based. According to Clarke (1998: 90), the development of what Garland (1990: 146) termed "criminological research", was focussed on the individual, why certain people commit

crimes in terms of the “new criminologies of everyday life”. Previously, most crime and what can be done to prevent them from offending formed the basis of crime prevention research. According to Eck and Weisburd, (2011: 45) theories of crime can be divided into those that seek to understand criminal behaviour from the offender perspective and those that examine the criminal event itself. From the 1970s onwards several new crime theories began to emerge (Cornish & Clarke, 2003: 74). These included routine activity, rational choice and crime pattern analysis theories and Crime Prevention Through Environmental Design (CPTED) (as outlined in more detail in Chapter Two).

This theoretical paradigm is supported by Foucault’s Theory of Panopticon, as propagated by Bentham. Some critics have gone so far as to draw Bentham’s general panel principles from the regime for the panopticon. The panopticon was illustrated as a prison facility designed in a way that all prisoners are visible and, at the same time, the guards, jailers or supervisors, will always be able to watch the inmates (Bentham, 1791: 95). Thus, the prisoners could always be seen by the supervisor, but they could not see the supervisor. This characteristic of panopticon has been likened to the concept of surveillance. Thus, CCTV’s primary function, from the above analysis, is to identify both perpetrator and victim (if there is one physically present) or, at the very least, the location of the offence (crime) in progress while being conscious of the perpetrator/s. Its secondary role is deterrence, in other words, the ability to stop any further criminal activity (Eck & Weisburd, 2015: 45).

3.3 The Proliferation of CCTV

Since the early 1980s there has been a rapid rise and spread of CCTV surveillance systems throughout societies worldwide, particularly in the UK (McCahill & Norris, 2002: 45). This proliferation has, to a lesser extent, occurred in South Africa. However, this spread can be attributed to several factors. According to Minnaar, (2006: 3) CCTV in South Africa as a prevention, surveillance and detection measure was nothing new. In South Africa early use of CCTV was implemented by the mining industry on diamond mines and at gold/precious metals refineries, largely to prevent the smuggling and pilfering of diamonds and precious metals from these facilities and

mines. The gambling industry (casinos) in South Africa was also one of the first to use CCTV for surveillance purposes of gamblers and patrons in their establishments. But these uses were largely 'in-house' and on private property. At a later stage its benefits were recognised by the private security industry who utilised it for the provision of surveillance and access control largely at commercial and business premises or private residences (and more recently at so-called 'security villages/estates') (Minnaar, 2006: 3-5).

In discussing CCTV's effect on auto theft Caplan et al (2011: 270). stated that car thieves faced a greater risk of detection in CCTV areas because different camera viewsheds could readily identify a stolen vehicle as it travels through the city. The lack of effect on the other crime categories also reflects the general trend in the literature, as CCTV has not consistently reduced street-level crime in public places. However, examples of successful public systems are not completely absent (Caplan et al, 2011: 265). Welsh and Farrington (2009a: 60) found that CCTV worked best when integrated alongside other crime control strategies and when camera coverage was high. This is consistent with La Vigne et al (2011: 20), who found that police departments that realized crime reductions through CCTV largely incorporated proactive police activities into their operations. This suggest that anyone who want to make use of CCTV should include evidence-based strategies for CCTV to be effective (Piza, 2015: 12). The initiative to start implementing and linking CCTV surveillance systems in CBDs in the major metropolitan cities of South Africa to local police services was taken in the mid-1990s by Business Against Crime of South Africa (BACSA) (Minnaar, 2006: 2).

The 2006 research study by Minnaar, using case study overviews from four South African CBD areas (Cape Town, Johannesburg, Pretoria (Tshwane) and Durban), traced the use of CCTV as crime control or prevention surveillance, how such CCTV systems were implemented, the rationale behind their implementation and the operationalising of them in terms of preventing street crime and its uses in other surveillance. In addition, the study also examined CCTV use from the perspective of

the growth and commercialisation of the management of these services, and the co-operation and co-ordination structures in partnership with the (SAPS. Furthermore, the 2006 Minnaar study reviewed the purported impact on the reduction of crime of these systems in CBDs and finally the application of public crime surveillance by the CCTV control room operators (private security) in co-operation with the police (response team) and the role CCTV surveillance systems play in the observation, recording, arrest and conviction of suspects.

CCTV surveillance systems are often portrayed as the all-purpose (panacea) security tool that greatly enhances the level of protection and asset against security risks. But as Minnaar (2007) concluded:

“the South African CBD CCTV systems are not the panacea for all crime or wholly responsible for crime reduction in surveilled areas. Rather that such systems are but one cog in an overall crime reduction programme and provide support surveillance systems to the overall approach of crime fighting by making them more efficient, effective (in deterring criminals) and responsive (quicker) in catching offenders” (Minnaar, 2007: 20-21).

However, the security industry promotes the performance of public street surveillance:

“CCTV continues to be the buzz word around the world, [with] most [city] councils look to [other cities] ... experiences for arguments to convince stakeholders of the importance of the gadgetry” (Adam, 1998: 30).

Research has shown that public street surveillance provides a decrease in levels of crime (Norris & Armstrong, 1999: 34). However, research has also shown that this may only be for a short period of time and only in certain crime categories (Norris & Armstrong, 1999: 80: 19; Painter & Tilley, 1999: 18; Ditton, 1999: 40; Short & Ditton, 1998: 46; Waters, 1996; Brown, 1995: 46; Tilley, 1993: 12). Society views public street surveillance as a social benefit, which outweighs the perceived social risk or invasion

of privacy rights. Therefore, it is important that there is a method to measure CCTV surveillance systems application and impact on crime prevention and control and hence, social acceptance of public street CCTV surveillance.

3.4 EVIDENCE OF CAMERA SURVEILLANCE EFFECTIVENESS

Williams and Johnstone (2000: 67) observed that there are:

“instances of systematic, selective racial and socio-economic profiling by CCTV system operators who aim their cameras at social groups that they subjectively judge as being high-risk or more likely to behave defiantly, especially young black males”.

Discriminatory CCTV monitoring and a tendency towards racial and ethnic profiling in evidence gathering and law enforcement actions were also observed by Short and Ditton (1998: 84); Norris and Armstrong (1999: 90); and Norris (2001: 22). On news media, images taken from CCTV video footage cause public anxiety and influence public perceptions of the risks regarding violent street crime. This results in raising public demands for the further extension of CCTV surveillance systems in city centres (Jermyn, 2004: 71-72; Surette, 2005: 15). Brown's (1995: 52) assessment of the CCTV systems in the city centres of Birmingham and Newcastle (in the UK) illustrated that the displacement of crime from these areas did occur. The existing evidence regarding CCTV effectiveness is focused predominantly on the prevention of crime. The evidence backing CCTV effectiveness, as a situational crime prevention measure, is mixed. In the following section, this evidence is briefly summarised and discussed in order to outline the issues that need to be considered when evaluating CCTV in the context of crime prevention. The empirical key findings regarding the effect of CCTV on crime are summarised below. First, most of the studies that show CCTV to have a restraining effect on criminal activity were: i) carried out in the United Kingdom; and ii) concentrated on camera surveillance as applied to car parks (see the meta-analyses by Welsh & Farrington, 2003: 70; 2009a & 2009b: 32).

Furthermore, most existing CCTV evaluations originate from the United Kingdom. Almost all studies from other geographic areas, such as the United States or Scandinavia, do not provide clear evidence of it having a moderating effect on crime (see Welsh & Farrington, 2009a: 50 & 2009b: 13; Ratcliffe, Taniguchi and Taylor 2009: 747-753). In addition, the impact of CCTV is directly linked to what kind of crime is being observed and monitored. By impacting on the expected costs of criminal activities suffered by the criminal, this type of surveillance by CCTV systems appears more applicable to combating planned or premeditated criminal behaviour, such as property-related offences (e.g. vehicle crime), but slightly less directly on burglary, simple theft, shoplifting and arson, than at preventing impulsive emotion-based violence (e.g. domestic violence, assault and battery). This is a partial explanation of why CCTV generally operates more effectively in car parks than on public squares and in mass transport services. Moreover, the location of a CCTV surveillance system is crucial to its effectiveness. While crime seems to be controllable (to some extent) by CCTV in small, enclosed or, at least, well-defined areas with limited and controlled access points (such as parking lots and car parks), there is hardly any significant evidence regarding highly frequented public spaces with open access (such as 'hot spots' in city centres) (Welsh & Farrington, 2009a: 41; 2009b: 67). Interestingly, the latter areas are exactly the ones where the application of CCTV is currently spreading most rapidly (Gill & Spriggs, 2005: 8; Cavoukian, 2008: 55). In this context, additional factors, such as the number and types of cameras (pan, tilt, zoom, multiplexing; resolution; fixed versus re-deployable), density of camera coverage of an area; control room operations (staffing; 24/7 versus passive monitoring, i.e. automatic recording when activated by certain activity, not real-time monitoring at all; and whether software analytical technology has been loaded on system), system management skills; objectives as formulated in the operational plan of the scheme are implemented; and the involvement of the police and other law enforcement agents. All these factors have an impact on the efficiency and success of any CCTV system. However, these listed factors are often based on perceptions and limited evidence substantiation (Welsh & Farrington, 2008: 20). It is obvious that there is a need for further research to assist in

identifying the factors and operational characteristics that make CCTV surveillance schemes a success or a failure.

Information on these important implementation aspects should be provided by future CCTV studies, especially as these systems and their operations are not static but are modified and upgraded from time to time. CCTV generally has an ex-post investigative utility, at least if the recordings are stored and the relevant visual information is easily searchable (Gill & Spriggs, 2005: 56). This potential was successfully exploited when tracing the perpetrators of the second London bombings in 2005. However, there is also evidence of an experience-based adaptation in criminal behaviour patterns. This undermines the suitability of CCTV as a crime-prevention and evidence-gathering tool (Welsh & Farrington, 2009: 20). The general agreement surrounding the use of CCTV cameras was that they were a useful tool in the fight against crime (Norris & Armstrong 1999: 72). The literature suggests several reasons for using CCTV surveillance systems in public spaces, namely:

- use as an investigative tool after the commission of a crime;
- an effective psychological deterrent to potential offenders;
- aids in the early detection of crime thereby facilitating a larger share of crime to be brought directly to the notice of the police or security personnel;
- early detection facilitates the co-ordination of responses to incidents as they are occurring and the implementation of strategies to reduce the level of harm to victims;
- CCTV may improve rates of arrest and successful prosecution of offenders by facilitating the more effective deployment of officers and the gathering of evidence; and

- the presence of CCTV could reassure the public and thus increase feelings of safety or reduce fear of crime (Brooks & Corkill, 2014: 220).

There are many publications dealing with the relationship between crime prevention and control and CCTV surveillance system. In fact, CCTV has been so disappointingly poor at bringing down crime levels the world over, that UK academic, Clive Norris, 1999: 90 has even referred to its continued spread as “the success of failure”. In the case of Khayelitsha in Cape Town, the police made use of CCTV evidence a mere five times over a ten-year period. Privacy regulators generally insist that public CCTV cameras are signposted, whether they are operated by state or private actors, and that these signs include information about the data controller responsible for operating them and the contact details. This allows people to contact the controller to enforce their privacy rights if they so wish. In central London, signs warn people that ANPR is in operation (Duncan, 2018a: 45). Yet in South Africa, signage on CCTV cameras is inadequate or non-existent. This means that the public is forced to rely on the state’s claims about effectiveness (Duncan, 2018a: 46).

Furthermore, the admissibility of CCTV footage as evidence in court remains unclear. In one of the most CCTV-saturated cities in the world, namely, London, CCTV has not contributed significantly to prosecutions, which has reduced its usefulness as an investigatory tool. Cape Town and Johannesburg have been introducing smart CCTV cameras fitted with ANPR and Johannesburg has also expressed interest in incorporating facial recognition into its camera systems. Facial recognition carries with it the risks of false positives or false negatives which means that innocent people may be identified falsely, while guilty people may not. A police study has also suggested that the technology may have built-in racial and age biases because the algorithms used for facial recognition have more difficulty identifying black and younger people accurately. A 2016 report from Georgetown Law’s Center on Privacy and Technology found that half of all Americans are in police facial recognition databases, meaning that algorithms pick suspects from virtual line-ups of 117 million mostly law-abiding citizens (Caplan et al, 2011: 273). These problems increase the potential for falsely

accusing people of a crime based on race or age, leading to racial or age profiling. If state agencies are acquiring this software for law enforcement purposes, then they should include accuracy as a key requirement in any tender documents. Most controversially, some countries (such as Australia) are exploring using facial recognition in CCTV cameras in public spaces, to scan and identify ordinary passers-by in real time. This is a truly frightening prospect, as it means that pedestrians can have no expectation of privacy in public spaces whatsoever. Your movements constitute personal information, which you have a right to exercise control over in terms of the Protection of Personal Information Act (POPI) (Bygrave, 2014: 52; Roos, 2007: 421). However, the police, spy agencies and private security companies are likely to argue that the Act does not cover criminal justice and national security issues (Act No. 4 of 2013: 60). The Act applies to these areas if it can be shown that existing privacy protections are inadequate, and smart CCTV roll-out is practically unregulated currently. This right is becoming increasingly important, as information about a person's movements can reveal a great deal about a person's personal, social and political activities. Increasingly, these cameras are being loaded with 'smart' capabilities such as Automatic Number Recognition (ANPR) and facial recognition software (Duncan, 2018a: 81). Secondary information was mostly obtained from articles in the journal *Surveillance & Society*. In the United Kingdom, CCTV technology, as a surveillance system, started many years before the United States, and has been more widely adopted there. As a result, there is a much larger body of knowledge assessing the extent to which the introduction of electronic surveillance in a place reduces crime in the United Kingdom than there is for the United States. In the search for evaluation studies about surveillance, more than a dozen for the United Kingdom were located, but only a mere handful for the United States (Armitage, 2002: 67).

3.5 THE USE OF CCTV SURVEILLANCE AND ALLIED TECHNOLOGY FOR PUBLIC SAFETY AND THE IDENTIFICATION OF CRIMINALS

The installation of CCTV systems in South Africa is mostly done in the CBDs and buildings for public safety reasons. Most of the cameras are targeted at places where there are entrances and exit doors. For example, banking halls and ATMs have cameras that are strategically mounted in various locations especially facing the counters where money is delivered. Busy shopping malls are also common areas for CCTV installation, supermarkets, and bus and train terminals. Other places include car parks, busy streets and even libraries. Nowadays, even churches have been placed under surveillance (Norris & Armstrong, 1999: 89). But a closer look at the technology strongly indicates that it could lead to false arrests, the targeting of innocent citizens, and unfair discrimination against minority groups (Norris & Armstrong, 1999: 90). In Great Britain, facial recognition technology has, in fact, led to false arrests and the targeting of thousands of innocent people. In May 2018, British lobby group, Big Brother Watch, obtained information about the use of facial recognition from 35 UK police departments by making lawful requests for information. In their May 2018 report, they found that: “[t]he overwhelming majority of the police’s ‘matches’ using automated facial recognition to date have been inaccurate ... leading to the storage of biometric photos of thousands of innocent people” (Big Brother Watch, 2018: 3). In other words, these people were wrongly identified as “persons-of-interest” (to law enforcement agencies) or criminals. It also emerged that the London Metropolitan Police has the worst record, with the accuracy of its automated facial recognition “matches” of less than two percent, which means that they had incorrectly identified innocent members of the public in 98 percent of the matches (Big Brother Watch, 2018: 3). (In South Africa, such requests can be made through the Promotion of Access to Information Act, which allows South Africans to request information from a state body or private entity in order to exercise or protect constitutional rights (Swart, 2018: 60).

The last 20 years in South Africa has seen the establishment and growth of CCTV surveillance systems in various large cities and towns, including Johannesburg,

Pretoria, Cape Town, Nelson Mandela Bay (Port Elizabeth) and eThekweni (Durban). The City of Johannesburg, for instance, paid R50-million to have its CCTV system installed in 2008 with the City Council reporting at the beginning of 2018 that it costs about R1 million monthly to run and maintain the system (Swart, 2018: 65).

In 2016, as part of its “safer cities” initiative, the City of Johannesburg announced a major upgrade to its existing CCTV camera network system – one that they said would use smart technology, including automatic number plate and intelligent facial recognition – in the Central Business District and would be rolled out in other public spaces as the system was expanded in order to keep law and order (Duncan, 2018a: 56). But by the end of 2017, the City Council had not yet enacted the necessary by-law requiring that signage alerting the public to the presence of CCTV surveillance be erected at entrances to those areas where the system was installed – a legal measure and key privacy protection requirement. In 2018, the City Council was still in the process of finalising a policy on the roll-out of CCTV, coupled with a master safety and security plan. At this stage, it was pointed out that, although the policy was at a draft stage, the technology had run ahead of the policy. For instance, the new modified ANPR systems allow the police to match vehicle number plates picked up on CCTV to a vehicle’s owner, and then further link the vehicle to SAPS crime databases if it has been used in a crime. Facial recognition allows them to identify a person from a facial database if s/he has been committing crimes in public spaces. Facial recognition software has also become controversial as it has used personal data gathered for one purpose, for another purpose, and not necessarily with a data subject’s consent (a basic requirement of data protection law) (Lyon, 2011: 61).

Advanced new facial recognition technology adds intelligence to surveillance systems, allowing for proactive monitoring and control 24/7, automated facial wrapping and recognition, and even highly accurate identification. These modified and added on features to basic CCTV surveillance systems appear to be excellent crime fighting tools. Marius Coetzee, CEO of the South African-based identity specialist company

IDECO, added a further dimension by saying that, by adding intelligent facial recognition technology to existing CCTV surveillance systems,

“retailers could not just count how many customers looked at a particular area of the store, but also determine how many customers came back more than once, conversions, customer demographics, and how they reacted to the products – based on their facial expressions” (Sibiya, 2018: 56).

Coetzee further mentioned another example of its use:

“At stadiums and public events, [it] can be deployed to identify troublemakers, manage risk or identify and protect VIPs. For safety and security, intelligent facial recognition allows authorities to list people of interest and be notified when they pass a camera; or secure a region of interest by triggering an alert when an unauthorised person enters that area” (Sibiya, 2018: 62).

Coetzee further added that:

“You can ‘wrap’ a face, extract the features and expressions, produce an identikit of the individual, identify the person and recognise them every time they pass a camera, identify who they associate with and track how they move through the organisation [or track them walking in the streets]” (Sibiya, 2018: 67).

Coetzee concluded that, with the new generation of intelligent facial recognition technology, “... there is so much more information [that can be] added to the video feed” to a CCTV surveillance system by upgrading to this technology (Sibiya, 2018: 69).

In 2017, Johannesburg did not renew its CCTV surveillance operations contract with Omega Risk Solutions – the company that had run Johannesburg’s operations since

the CCTV system's inception in 2008. But the cancellation of the Omega contract and the relocation of the control room left the whole system vulnerable. Up to now, Johannesburg has relied on human operators to conduct surveillance. However, the cancellation of the Omega contract led to the retrenchment of many of their most experienced and trained operators who had, over the years, received extensive CCTV control room operator training, with most having seven to nine years of experience (Sibiya, 2018: 70).

Eventually, in July 2018, Johannesburg started on the first phase of the high-tech upgrade (initially announced in 2016) to its current CCTV system which, at the time, comprised 450 cameras mainly installed in its crime-ridden CBD and the surrounding areas. The first phase involved the installation of an additional 50 cameras, "fitted with the latest and smartest technology" making a total of 500 cameras installed (Swart, 2018: np).⁸ However, the whole management of the multi-million hi-tech upgrade was outsourced to a third party by the Metropolitan Trading Company (MTC), which managed the so-called Intelligence Video Analytic Platform Project on behalf of the Johannesburg Metropolitan Police Department (JMPD). According to MTC's field service technician, Siphon Phakathi, the new cameras would be installed in JMPD-identified high-crime "hotspots" and have built-in fibre networks and WiFi connectivity, as well as facial recognition capability. Besides facial recognition, the CCTV system could be used to detect when there is suspicious movement or activity, for instance a sudden gathering of a crowd on a street corner or eruption of a commotion, i.e. utilising pattern analysis of any sort of activity or people movement. This new "intelligent" technology would enable the system to pick up "... if the same person keeps on passing or moving in the same area multiple times ... the pattern" would be discerned and the control room would accordingly be alerted. In addition, the new system with number plate recognition would also assist "to detect a suspicious car that drives

⁸ Heidi Swart is a journalist who, for this researched story in the *Daily Maverick*, was commissioned by the Media Policy and Democracy Project, an initiative of the University of Johannesburg's Department of Journalism, Film and TV and Unisa's Department of Communication Science.

around the neighbourhood”. Furthermore, the new cameras provided a much “sharper image of a suspect” (Phakathi, 2018: 90).

To understand how the new Johannesburg CCTV system would work in practice, the *Daily Maverick* journalist, Heidi Swart, sent the City of Johannesburg detailed questions regarding the cost of the new systems, the problems inherent to facial recognition technology, the safeguards they would have in place to ensure footage and data was not leaked from their operations room, as well as an inquiry about complaints from the public that the current system is not functioning properly (Swart, 2018: np). The response from the City Council, via JMPD’s spokesperson, Snr Supt. Wayne Minnaar, was that the new CCTV “contributes significantly towards the safety in the Johannesburg CBD, therefore detail of its functioning is confidential, and information may not be divulged for security reasons” (Wayne Minnaar as cited in Swart, 2018: 40).

In contrast, to try and establish if it would work, Swart interviewed three security industry experts, all of whom wished to remain anonymous. Between the three of them, they had over four decades of experience in the business and share an intimate knowledge of urban and state visual surveillance in South Africa. The consensus of these experts was that, in South Africa, this type of technology would not work, since South Africa’s vehicular traffic and pedestrian flows are too irregular and unpredictable. “People could gather on a street corner at any moment for any reason, or similarly break out into a jog. Jaywalking is practically a national pastime” (Anonymous, as cited Swart, 2018: np). Furthermore, to prevent the type of bias and inaccuracy that comes with hi-tech CCTV programmable solutions, the human CCTV operators require proper training in suspicious activity “behavioural aspects and body language to pick up on crime indicators that could be signs that a crime has the potential to occur, or is in progress” (Anonymous, as cited Swart, 2018: 50).

3.6 CRIME PREVENTION

Many countries have implemented crime prevention initiatives for several years, and numerous examples exist where such projects have succeeded in bringing down crime levels. The National Institute of Justice (NIJ) in the United States of America provides examples of effective and promising programmes and practices in criminal justice, juvenile justice, and crime victim services. The NIJ has compiled profiles of a range of crime prevention initiatives evaluated globally and classifies them as effective, promising or no effect.

In the UK, crime prevention discourses are often a reflection of what Garland (1996: 349) terms the “Responsibil[is]ation Strategy”, which is an attempt to implement “social” and “situational” forms of crime prevention as a means of “reordering the conduct of everyday life right across the social field” (Garland, 1996: 454). Garland, however, notes that the success of implementing a responsabilisation agenda quickly became constrained by issues surrounding the setting up effective multiagency co-ordinated action for crime prevention. Even when sufficient capacity and willingness does exist, questions have been asked about the validity of such approaches, particularly when they are used to hide deficits in frontline policing and crime control. Of particular interest is Garland’s (1996) description of responsabilisation strategies, which involve the “central government seeking to act upon crime not in a direct fashion through state agencies (police, courts, prisons, social work, etc.) but instead acting indirectly, seeking to activate action on the part of non-state agencies and organizations” (Garland, 1996: 452). Despite this, crime prevention schemes of different varieties and forms are relatively common.

Crime prevention aims to address some of the causes of crime. One way to explain this approach is to refer to the so-called problem analysis triangle, also known as the crime triangle. Crime prevention initiatives could focus on the victims, the offenders or the location (environment), for instance:

- Victims: Initiatives could aim to reduce the vulnerability of certain individuals, groups of people or communities;
- Offenders: Initiatives could focus on the reasons why certain individuals or groups of people are at risk of committing crime;
- The environment: Initiatives could address the physical characteristics or other situational factors of specific locations or areas that increase opportunities for crime. Possible interventions could involve law enforcement, situational crime prevention and social crime prevention approaches (National Institute of Justice (NIJ), [sa]. np).

Often a combination of these three approaches has a better chance of delivering results. (It has its origins in one of the central theories of environmental criminology – Routine Activity Theory – developed by Cohen and Felson (1979: 588-608). According to this theory, certain types of crime could only occur when a likely (or motivated) offender and suitable (or vulnerable) target (property) or victim (person) are present at the same place at the same time. In addition, there should be an absence of effective control or protective measures, such as someone responsible for preventing the crime from happening or people willing to intervene.

Being a multi-sectoral, multi-disciplinary and integrated endeavour, crime prevention has been defined by Ekblom (2005: 216) as an: “...intervention in the causes of criminal and disorderly events to reduce the risks of their occurrence and/or the potential seriousness of their consequences” (Ekblom, 2011: 220). Also, according to Sherman (1992: 78): “crime prevention is the attempt to reduce, deter crime and criminals”. There is clear evidence that well-planned crime prevention strategies not only prevent crime and victimisation, but also promote community safety and contribute to sustainable development of countries (Ekholm, 2013: 12).

In South Africa, different crime prevention projects and programmes have also been implemented in various communities. Crime is not just a reality for South Africans, it is an obsession. The crime discourse in South Africa appears to be banal – people talk about it all the time in the same way that people elsewhere talk about the weather. It recognises that crime can “dominate the public psyche, contributing to counter-productive public anxiety, fear and helplessness” (Baghel & Mayr, 2007: 234). It also underlines that public perceptions of crime place an undue burden on policy makers to address these crime priorities. “Prevention is the first imperative of justice” (Ekhom, 2013: 45), and from the perspective of society, the best and most useful activity that law enforcement agencies can carry out is crime prevention.

Crime prevention has come to mean many different things to many different people. The National Crime Prevention Strategy (SAPS, 1996: 79) recognises the importance of addressing the fear of crime via policing. In the context of CCTV these initiatives can include the following:

- Law enforcement: targeted visible police patrols; supplemented by patrols by security guards or police reservists; Bye-law enforcement; training of response units for CCTV systems and private security guards;
- Social crime prevention: educational programmes for children which raise awareness, for example, about child abuse; community neighbourhood watch programmes; provision of recreational facilities to occupy the youth; victim support centres;
- Situational crime prevention: city centre CCTV systems; improving street lighting in townships and in CBDs; supporting street layout that encourages use by pedestrians; designing streets, buildings, parks, etc. to reduce opportunities for street crimes, such as mugging and violent crimes (e.g. vehicle hijackings or rape).

Often a combination of these three approaches has a better chance of delivering results.

3.7 CCTV SURVEILLANCE SYSTEMS AND CRIME PREVENTION

From Foucault's description and analysis of the Panopticon and from the opinions of the theorists (as outlined above), it can be suggested that CCTV helps in crime prevention. CCTV has generally found its theoretical justification from situational crime prevention and the Rational Choice Theory that states that offenders make decisions about their intending offence situations. CCTV surveillance systems serve many functions and are used in both public and private settings (Armitage et al, 1999: 41).

Karim (2007: 32) has also observed that the Routine Activities Theory: “demonstrates the method through which motivated adversaries (threats) find suitable targets (assets) and opportunities (vulnerabilities) during their routine activities”. Therefore, Karim further opined that, for a “criminal activity to become reality, the adversary, target and opportunity must converge in time and space for the crime to occur” (Karim, 2007: 15). In view of this, the need for security operatives to find opportunities that may interest the potential offender, through intelligence gathering, surveys, criminal profiling and all manner of vulnerability assessments, becomes imperative.

As a form of situational crime prevention, CCTV surveillance seeks to prevent both personal and property crime and can be used in place of, or in addition to, police. Public surveillance cameras monitor, record, and transmit images of a specific area of interest and are either monitored remotely by security personnel or preprogramed to scan the specified area (La Vigne et al, 2011: 51). Routine Activity Theory, as postulated by Cohen and Felson (1979: 588-608), posited that for a predatory crime to occur three elements must be present: a likely or motivated offender; a suitable target; and the absence of a capable guardian. Felson (1987: 911-931) subsequently refined the theory with the addition of a fourth element, that of the “intimate handler”. It is believed that the increased surveillance provided by CCTV will reduce crime and increase arrest, without displacing crime to other nearby areas where CCTV is not in

use (Ratcliffe, 2009: 49-55). Cornish and Clarke (2003: 80) postulated the Rational Choice Theory, which is based on the assumption that: “offenders seek to advantage themselves by their criminal behaviour”. Rational Choice Theory, like Routine Activity Theory, is formulated on the concept of the offender being a rational actor undertaking a cost benefit analysis at a given time and place to assess whether there is the opportunity to offend. CCTV cameras are placed in areas where they are thought to be most effective, which typically includes highly populated towns, city centers, car parks, or various other high-crime areas (Welsh & Farrington 2008: 17).

Throughout the world CCTV cameras are installed in streets and businesses with the stated goal of reducing crime and increasing public safety. It is argued that CCTV (especially if well publicised) may prevent crime since potential offenders are deterred by the increased subjective probability of their detection. Also, CCTV may increase the true probability of detection, may increase pedestrian usage of places and hence further increase the true and subjective probabilities, may encourage potential victims to take security precautions, and may direct police and security personnel to intervene to prevent crime (Armitage, Smyth & Pease, 1999: 226-227).

Another possibility is that CCTV could signal improvements in the area and hence increase community pride, community cohesion, and informal social control, which in turn might decrease crime. CCTV surveillance cameras or video surveillance cameras (as they are also known) serve many functions and are used in both public and private settings. The prevention of personal and property crime is among the primary objectives in public space. As an intervention targeted at crime, CCTV is a type of situational crime prevention. Programmes and policies designed to prevent crime can include the police making an arrest as part of an operation to deal with gang problems, a court sanction to a secure correctional facility, or, in the extreme, a death penalty sentence. CCTV is considered to be one of the technologies adopted by law enforcement agencies to deal with the effect of alleviating shortcomings in the investigation of crimes. More often, though, crime prevention refers to efforts to prevent crime or criminal offending in the first instance – before the act has been committed.

Both forms of crime prevention share a common goal of trying to prevent the occurrence of a future criminal act, but what further distinguishes crime prevention from crime control is that prevention takes place outside of the confines of the formal justice system. These measures are more correctly referred to as crime control or repression.

The prevention of personal and property crime is among the primary objectives in public spaces. As an intervention targeted at crime, CCTV may prevent crime because potential offenders are deterred by their increased subjective probability of being detected (Welsh & Farrington, 2009: 65). This implies that the presence of CCTV could cause potential offenders not to commit a crime as the risk outweighs the benefits. Therefore, CCTV reduces offenders' opportunities to commit crimes. CCTV could also cause crime to increase. It could give potential victims a false sense of security and make them more vulnerable because they relax their vigilance or stop taking precautions, such as walking in groups at night and not wearing expensive jewellery. This shows that one cannot predict the actions of others even with the presence of CCTV everywhere (Welsh & Farrington, 2008: 12).

This means that the offender must be made aware of the added surveillance for it to achieve its desired effect. Advocates of public surveillance systems also maintain that such systems can increase perceptions of safety among members of the public, and additionally reassure them to make increased use of public spaces they know have CCTV surveillance systems in place (La Vigne et al, 2011: 56). By means of the increases in people visiting such surveilled public spaces, more individuals can potentially serve as witnesses to crimes, presenting the possibility of greater crime reduction. As described by Cornish and Clarke (2003: 41-42), CCTV is a form of "formal surveillance", meaning that not only can CCTV replace police or security officers (and often does) but it can also improve their capabilities, i.e. improve response times and accurately identify locations to which they can rapidly respond to real time crimes-in-progress (Welsh & Farrington, 2008: 17).

In addition to acting as a deterrent, CCTV cameras can alert police of crimes as they happen ('real time'), which can enable officers to respond quicker and more efficiently (La Vigne et al, 2011: 57). On a larger scale, the use of CCTV also presents the possibility of aiding the criminal justice system, since CCTV video footage of a crime may help in investigations and prosecutions (La Vigne et al, 2011: 85).

3.7.1 CCTV technologies: Facial recognition systems

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source (Duncan, 2018a: 72). One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems and can be compared to other biometrics, such as fingerprint or eye iris recognition systems. Popular recognition algorithms include *Eigenface*, *Fisherface*, the Hidden Markov Model, and the neuronal motivated dynamic link matching (Duncan, 2018a: 67).

A newly emerging trend, claimed to achieve previously unseen accuracies, is three-dimensional face recognition. Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. Tests on the FERET database, the widely used industry benchmark, showed that this approach is substantially more reliable than previous algorithms. There are also several potential uses for facial recognition that are currently being developed. For example, the technology could be used as a security measure at ATM's; instead of using a bank card or personal identification number, the ATM would capture an image of your face, and compare it to your photo in the bank database to confirm your identity. This same concept could also be applied to computers; by using a webcam to capture a digital image of yourself, your face could replace your password to log-in.

3.7.2 The role of international research: Impact of CCTV surveillance

CCTV camera networks can provide warning signs of potential criminal offences and act as a responsive instrument. CCTV can monitor crowds and individuals, respond to threats and thus notify the operator (in a central control room) of unsafe, dangerous or criminal conduct and activities during and after the occurrence of an event (McCahill & Norris, 2002: 34). Video observation cameras have been extremely useful in recognising offenders. For example: in the 1993 Bishopsgate bombing (in London, UK) as well as the series of bombings on the London underground on 7 July 2005 (Switzerland Federal Department of Police and Justice, 2007: 72).

Video surveillance cameras can also assist the authorities in other criminal acts. For instance, in Barcelona, video surveillance cameras on the metro rails enabled authorities to find a young Spanish man who had forcefully attacked a Latino American man in the metro (Cambon, 2007: 102). Such occasions have spread awareness on the viability of CCTV surveillance systems as a security device. This has enticed countries, such as Germany, to introduce CCTV networks in public transit frameworks in case of similar incidents occurring on their rail systems (bombings/assaults etc.). Such CCTV networks offer constant surveillance in places where humans cannot see, i.e. underground tunnels of trains. In the case of an incident (e.g. a fire), this innovation can inform control operators and lead to rapid response(s) to any such situation arising and can also indicate a way out (escape) from a fire in progress on the underground (Müller & Boos, 2004: 173). Innumerable studies show that CCTV networks are a successful administration device since they are more affordable than police officers physically on the beat and are more productive in recognising or forestalling criminal offenses. Wear Babwin (2007: 101) states that, not at all like security officers, cameras are not subject to weariness or loss of focus and accordingly give continuous and consistent effort. Accordingly, the financial burden of the underlying cost of acquiring and introducing a CCTV network of cameras is impeded by its long-haul proficiency over utilising extra police officers who might be less significant. Goold (2009: 3-6) directed an investigation to analyse whether the association and administration of a

CCTV network conspires to influence how observation was completed. Goold's work uncovered negative and positive results. In a few cases, the implementation and administration of introduced CCTV frameworks without consulting with the police, or if the police took control of the system, the effects/results were restricted.

3.8 CYBERSECURITY AND CCTV

This literature review outlines many simple innovative tactics by cyber criminals that have led to unprecedented outcomes of cybercrime as a global threat activity. Security control rooms and CCTV surveillance operations are no exception to cyberattacks by criminals that can compromise the data (video images stored in databases) that might be shared for crime intelligence purposes with law enforcement agencies by the private security companies managing such surveillance operations. Such sensitive digital information, as well as other data, can be accessed by criminal hackers.⁹ Since CCTV surveillance operations operate largely via online internet electronic platforms, this makes all the stored information vulnerable to hackers. In other words, digital online data that is not properly secured by high levels of cybersecurity is vulnerable to criminal exploitation, or even industrial espionage by rivals. When a computer or network is the target, source tool or the medium of crime, such a criminal activity is referred to as computer crime, hi-tech crime, e-crime or electronic crime. In this regard, CCTV that uses computer networks in operations, i.e. in data gathering for law enforcement agencies (Norris & Armstrong, 1999: 52), are potentially liable to be compromised by cybercriminals in a cyberattack (see Minnaar, 2014: 16, for more detail of cyberattacks and cybersecurity vulnerabilities).

Digital technology provides this connectivity and gives its users many valuable benefits. New technologies create new criminal opportunities and new types of crime. But, at the same time, they provide a rich environment for criminal activity, ranging from vandalism to stolen identity to theft of classified government information. Also,

⁹ Hacking is an approach by which a computer system or computer network is attacked and accessed, and the cyber vulnerability thereby exposed is exploited by the hackers, most often for the theft of sensitive information (Mali, 2010: 60).

individuals may store sensitive information on their laptops, computers, tablets and smartphones. The internet is an open world where there are groups dedicating their time to gaining access to sensitive information. These groups are known as hackers; they use the vulnerabilities of the systems or networks to attack computer systems (Mali, 2010: 60).

Computer security, also known as cybersecurity or IT security, is the protection of information systems from theft or damage to computer equipment, the software programmes and information stored in databases. Cybersecurity is also used to protect IT systems from being disrupted or interrupted. This implies physical access to computer equipment and devices must also be controlled and protected from any harmful activity emanating from hackers accessing a network. This includes the infection of IT systems by the spreading of malware, whether intentional, accidental, or due to operators/users being tricked into diverging from cybersecurity operating procedures. In the field of CCTV digital systems' increasing reliance on computer systems, the internet and wireless networks in their operations and the growth of 'smart' technologies linked to CCTV, cybersecurity has become important for the storage and protection of the integrity of recorded video images (Schatz, Bashroush & Wall, 2017: 53-54).

3.8.1 The mechanism of crime reduction

The mechanisms under which CCTV aims to reduce crime are based upon the following assumptions:

- **Deterrence:** The potential offender becomes aware of the presence of CCTV, assesses the risks of offending in this location to outweigh the benefits and chooses either not to offend or to offend elsewhere.
- **Efficient deployment:** CCTV cameras allow those monitoring the scene to determine whether police assistance is required. This ensures that police resources are called upon only when necessary.

3.8.2 CCTV systems as a security concept

CCTV is a valuable management and security tool. The installation of a CCTV system as part of a series of security recommendations generally intended to prevent or detect crime. CCTV can be very effective in maintaining security. Video evidence can help with security enquiries or investigations and assist in securing criminal convictions. The visual recording of incidents, for evidential or investigative purposes, has many benefits and with a competitive customer driven market is no longer cost prohibitive. CCTV systems will vary in size and complexity depending on the following context/situations:

- (i) **By Potential Offenders:** The threat of potential surveillance (whether the cameras are being monitored may be irrelevant) acts to produce self-discipline in which individuals police their own behaviour. In prison, the cells are arranged around a central watchtower from which a supervisor could constantly survey them. Prisoners could never be sure whether they were being watched, so began to police their own behaviour. Foucault (1991: 90) laid down the principle that power should be visible and unverifiable. With reference to visible: the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon. As to unverifiable: the inmate must never know whether he is being looked at any moment, but he must be sure that he may always be so'. Similarly, the CCTV camera may produce self-discipline through fear of surveillance, whether real or imagined.

3.8.3 Cyber threats to control rooms and CCTV surveillance operations

There are two primary aspects that need to be considered in securing the integrity of the control room and client site from possible attack. One aspect is the integrity of the controllers that are employed and the second is the integrity of the network against possible cyber and hacking attacks. Contract Surveillance Services (CSS) is an independent control room offering the monitoring of CCTV, fire and alarm systems. It offers a direct-to-client service or a third-party control room for other security companies that do not have their own control room. The company has a continuous

programme of technology adaption enabling it to connect. to sites anywhere in South Africa. CSS has found that, having its control room outside of the main business centres, removes controllers physically from the probability of intimidation by criminal syndicates. Operating in an out-of-the-way city reduces the possibility of external intimidation and collusion. Many control rooms connect to sites through the public internet and use home Domain Name Systems (DNS) protocols (Mali, 2010: 32).

A simple internet search will reveal many ways to hack networks. Closed networks or Virtual Private Networks (VPNs) offer higher levels of security for connecting remote sites with users and their devices. Site specific usernames and passwords are equally important, used in conjunction with private network security features. Routers and switches, designed for VPN applications, also come with built-in firewalls and, with a reasonable router or switch, reasonable levels of security can be achieved. In addition to network security, passwords and access levels to control room computer workstations needs to be strictly controlled so that operators have limited access to system files. This will also reduce the possibility of a cyberattack or collusion with hacker intruders (Mali, 2010: 42).

An identified threat is any vulnerable point in the network or the operation system and in the software in use, and is considered a risk, due to its potential to be used in a cyberattack. Computer operating systems and software in use will determine whether there is a risk to the computer system or to the information stored on the computer or computer network being used for CCTV surveillance operations. Also, a factor that affects and increases the level of risk is the user/operator of the system. The threat of an “insider” giving approval to the attacker to hack the computer without the management of the company finding out, remains high. Such insider facilitated access to sensitive information is often based on bribery, corruption or intimidation, i.e. the operator (insider employee) may be blackmailed to provide access to the information by cybercriminals who are thereby enabled to circumvent company cybersecurity measures. If the operating network system does not have a malware detector, such as antivirus software and/or anti-malware software, this will also increase the risk of

being attacked because the computer does not have software that cyber controls the incoming online traffic (Georgia Tech Information Security Center [GTISC] and Georgia Tech Research Institute [GTRI], 2015: np for a more detailed exposition of cyberthreats).

3.8.4 Deliberate Denial of Services (DDoS)

The researcher emphasises the importance of a Deliberate Denial of Service (DDoS) and jamming attacks carried out on CCTV surveillance systems. A Distributed Denial of Service (DDoS) attack involves multiple DoS agents configured to send attack traffic to a single victim computer. In most cases, uninterrupted and untampered operation is critically important for CCTV surveillance systems because they are used to monitoring and recording crimes or other important activities. DDoS is a deliberate act that significantly degrades the quality and/or availability of services offered by a computer system by consuming its bandwidth and/or processing time. CCTV operates from network computer connection. The interruption of computer may affect the digital recording of events which could be used by law enforcement agencies. As a result, legitimate users are unable to have full quality access to a web service or services. Producing a DDoS attack on a CCTV surveillance system, even for one minute, could make them miss a significant event, such as an extremely quick bank robbery or crimes with more dire consequences. That is why, while a DDoS attack on a home router could be an insignificant irritation, the DDoS attacks on CCTV surveillance systems have a serious impact and must be considered when designing, evaluating and testing a new CCTV system (Neumann, 2000: 136).

3.8.5 Some preventative cybersecurity measures

There are several basic preventative measures that can increase the security of the hardware, firmware and network communication of CCTV surveillance systems. For instance:

- factory reset button;
- strengthening an organisation's overall cyber-resilience;
- improving online access controls;
- applying 'strong' firewalls to block unwanted incoming or outgoing cyber traffic on an internet connection;
- implementing Intrusion Detection Systems (IDS) (Maat, 2009: 61). It also prevents them from interrupting CCTV operations or damaging a server (Chitauri, 2015: 23);
- using 'private addressing. This involves not using an Internet Service Provider, such as Google, for email addresses. This is a way to protect publicly routable IP addresses. Many home-based broadband routers rely on private addressing to protect systems in the home or for small business networks (Bowen, 2009: 67).

3.8.6 Risk planning for cyber protection

All organisations, especially government agencies, prefer to keep their information private. For that they must have a good risk management plan in place and a strong security system to prevent any cyberattack or leak of sensitive information. Having an insider providing access to information databases to cybercriminals is more dangerous than experiencing a cyberattack since, if strong cybersecurity measures are in place, a hacking attack can be timeously detected, and the network and online operations can be secured by a company's IT department by means of firewalls. But an insider already has access to company databases by passing all the security checkpoints. To secure an organisation from an insider, the following security checks should be implemented (Neumann, 2000: 136).

- not allowing any employees to use a removable disc, external hard drive, CD-RW or DVD. This will protect the organisation from many security issues, threats and risks, such as malware (e.g. viruses, spam, spyware and Trojans) and combat the insider threat (Neumann, 2000: 136).
- Make use of high security with a password (frequently changed) and security questions. A second security authorisation token on login into the system can also be used. This will provide protection from compromised passwords and security questions (Neumann, 2000: 136).
- in the sphere of information security, more than one or two methods can be used for checking if the attempt to log in is by a trusted employee or not. First step is a user ID and password, and when the password has upper letters and lower letters, numbers, and more than eight characters, it will be more complicated for an attacker to hack the system. Second step is an authorisation token that changes the security code every 30 seconds. This will protect the agency from outsiders or an attacker trying to access information on the internet, monitoring the log in locations and the time of intrusion attempt. This monitoring will help the IT department to understand if the employee is logging into the system outside of the facility and/or out of working hours (Gerber, 2000: 12-17).
- Other measures for securing a system are making use of biometrics, such as a fingerprint system, iris eye scan or voice recognition system, all of which will help to prevent an outsider from accessing systems (Mali, 2010: 34).
- Educating employees to be more aware of cyberattacks and what they should do to avoid them. This includes implementing proper operating procedures, frequent changing of passwords, and proper authentication when logging on, among others. Education and awareness campaigns within a company have

proven to be more effective than any other countermeasures for protecting information (Maat, 2009: 45)

- Since many attacks destroy data or programs, making copies (backups) of digital information is essential to recover from an attack. Backups need to be done for any critical information and need to be stored some distance from the systems they track so no common disaster (e.g. fire, flood, and earthquake) affecting both locations is likely. Optical-disk storage is preferable for backups because it cannot be as easily damaged as magnetic media. A backup can be an entire duplicate computer system when it is important to maintain continuous operation (Akuta, Ong'oa & Jones, 2011: 130).
- Encryption hides data in a form that cannot easily be read. A character-string “key” to decode it can be provided if necessary (Chitauro, 2015: np). Any attempts to modify encrypted data will result in rendering it undecipherable so it is possible to tell if encrypted messages or programmes have been modified (or repeated if a time is included in the message). Strong and virtually unbreakable methods of encryption have been developed recently with ‘public-key cryptography’ and software that is available for free downloads from several Web sites. Encryption methods can also be used for “authentication” or to provide digital ‘signatures’ on documents to prove who wrote them and when. Encryption has been touted as a solution to many security problems but is overrated. If an attacker gains system-administrator privileges, he/she may be able to get encryption keys or disable encryption methods without the company or organisation’s knowledge (Akuta, Ong'oa & Jones, 2011: 133).

3.9 LAWS AND POLICIES FOR CYBERSECURITY

This section will cover the laws and the policies for cybersecurity. The most recent update on cybersecurity was the 2013 executive order by President Barack Obama of the United States of America about the importance of the cyber threat to critical infrastructure and how its continuing growth represents a serious national security

threat. It also expounded on cybersecurity information sharing with the policy mentioning that the private sector security should increase its ability to defend itself against cyber threats (Obama, 2013: Section 1; Sec. 4a). According to the US National Institute of Standards and Technology (NIST), each organisation needs a good risk management plan to protect its valuable assets in accordance with the NIST standards on securing information systems and data assets. Furthermore, organisations should apply access controls to these assets to secure them properly and to ensure that these access controls fully protect these assets (Obama, 2013: Section 1; Sec. 4a).

At present the current legal framework relating to cybercrime in South Africa is a hybrid of different pieces of legislation and the common law. Offences relating to cybercrime are primarily under the Electronic Communication and Transactions Act 25 of 2002) (Electronic Communication and Transactions Act (ECTA), 2002: Chapter XII). The ECT Act seeks to provide for the Department of Communications to appoint cyber inspectors. The cyber inspectors may monitor Internet websites in the public domain and investigate whether cryptography service providers and authentication service providers comply with the relevant provisions. The inspectors are granted powers of search and seizure, subject to obtaining a warrant. Inspectors can also assist the police or other investigative bodies, on request. Chapter XIII of the ECT Act seeks to make the first statutory provisions on cybercrime in South African jurisprudence. The Act seeks to introduce statutory criminal offences relating to the following:

- unauthorised access to data (e.g. so-called “hacking” and trading in passwords used to commit an offence);
- interception with data (e.g. tapping into data flows or denial of service attacks);
- interference with data (e.g. viruses and denial of service attacks);

- computer related extortion, fraud and forgery (e.g. where someone gains financially by undertaking to cease or desist from doing something using a computer) (ECTA, 2002: Chapter XIII).

Any person aiding or abetting another in the performance of any of these crimes will be guilty as an accessory. The ECT Act prescribes the penalties for those convicted of offences which render a person liable to a fine or imprisonment for periods not exceeding 12 months in certain circumstances or five years in certain circumstances (ECTA, 2002: Chapter XIII).

There are cybersecurity laws that prohibit all the cyberattacks mentioned above, but the laws do little to prevent them in practical terms. The United States and many other countries have laws prohibiting eavesdropping on communications and damage to computers, which covers most of the attacks mentioned. But most attackers do not concern themselves about getting caught since it is hard to track them down and legislation dealing with cybercrime and cybersecurity are hard to apply. Laws can, however, be effective against repeat offenders within a given legal jurisdiction, such as spies selling secrets.

According to the National Initiative for Cybersecurity Education (NICE) (of the US National Institute for Standards and Technology (NIST)), cybersecurity is divided into seven categories, namely:

- security provision;
- operation;
- maintenance;
- protection and defence;
- investigation;
- collection of analyses; and
- providing support (technical, updating and equipment).

In terms of cybersecurity provision, there are organisations that deal with people-sensitive information. They need to be well organised, especially in the context of information security management, and must make sure that whoever handles these duties knows explicitly what their jobs entail (National Initiative for Cybersecurity Education, 2011: 45).

3.10 CYBERSECURITY, CYBERCRIME, INFORMATION SECURITY AND PRIVACY ISSUES RELATING TO THE USE OF CCTV SURVEILLANCE SYSTEMS

The right to privacy includes all those things that are a part of us, such as our body home, thoughts, feelings, secrets and identity. The right to privacy enables us to choose which parts in this domain can be accessed by others, and control the extent, manner and timing of the use of those parts we choose to disclose. Different countries across the globe have defined their privacy requirements, by articulating the conditions for the protection of personal data and preventing harm to an individual whose data is at stake. CCTV is a valuable management and security tool. The installation of a CCTV system as part of a series of security recommendations generally intended to prevent or detect crime. CCTV can be very effective in maintaining security. Video evidence can help with security enquiries or investigations and assist in securing criminal convictions. The visual recording of incidents, for evidential or investigative purposes, has many benefits and with a competitive customer driven market is no longer cost prohibitive. CCTV systems will vary in size and complexity depending on their purpose and the defined security operational requirements. However, the basic purpose of any system will be to observe a scene and the activities that occur within it, namely:

- covert: the camera is concealed;
- discreet: the presence of the camera will be known to some people, but its appearance will not automatically suggest its purpose; and

- overt: the appearance of the camera will be designed to clearly indicate its function and maximize the deterrent effect.

For crime prevention overt CCTV systems are usually more suitable whereas discreet or covert systems are more appropriate for crime detection and prosecution.

3.10.1 Privacy issues vs CCTV surveillance systems

According to the claims of some sociologists (Whitaker, 1999: 136; Lyon, 1994a: 190, 2001: 150), privacy has little theoretical or practical utility in the 21st century. Electronic surveillance has been challenged as an unwarranted invasion of privacy and conceptualised as a component of a new social control strategy involving the diffusion of the surveillance panopticon ranging from prisons to public spaces worldwide (Lyon, 2011: 89). Generally, most of the concerns about CCTV surveillance systems are related to privacy issues for obvious reasons. The privacy impact of CCTV surveillance systems is especially important in the light of revelations about global surveillance programs (the Snowden case¹⁰ and subsequent revelations of blanket surveillance of the internet of individuals), and video surveillance scandals.

However, besides privacy issues, an insecure or compromised CCTV surveillance system can raise a myriad of other non-privacy related issues. For example, breaches have been shown to endanger the security and safety of a prison, pose theft risks to institutions operating with money, such as banks and casinos, emotionally affect other persons (especially children), or interfere with police and law-enforcement crime prevention activities. At the same time, as more and more embedded devices are being analysed at a large scale for security vulnerabilities (Welsh & Farrington, 2008: 34) it

¹⁰ It is important to note here that Lyon and other surveillance scholars have discussed many aspects of mass surveillance over the past couple of decades predating Snowden. However, according to Lyon, the Snowden revelations have provided “clear evidence” of mass surveillance happening, bringing concerns about mass surveillance to the public eye in ways never seen before. David Lyon’s *Surveillance After Snowden*, compellingly demonstrates the relevance of the former NSA contractor, Edward Snowden’s revelations about the global mass surveillance implemented by the National Security Agency (NSA) in the United States and throughout the world.

is no surprise that CCTV surveillance systems have recently gained a dramatic increase in attention from security researchers.

Those and similar studies led to more than a handful of vulnerabilities being exposed with a large-scale impact in real life for more detail on security threats, vulnerabilities and attacks on CCTV systems). It has been argued here that the kinds of surveillance highlighted by the Snowden revelations are on one hand information-intensive, often relating to the internet and on the other, 'national security-oriented. The concept of 'security' also requires problematising in this context, which is yet another task for the multi-disciplinary research that today is patently urgent. As with surveillance or privacy, defining security is difficult especially under present conditions, where 'national' security has been elevated to a top priority by many governments. It is a highly contested concept, often erroneously supposed to be in conflict with claims to a right to privacy or to civil liberties (Zedner, 2009: 43). Much more nuanced understandings of security are required if the term is to retain any connection with the desires, aspirations and indeed well-being of everyday citizens.

3.10.2 The data protection legal framework in South Africa

Prior to the promulgation of the POPI Act, South African law did not have an omnibus of data privacy legislation. Currently, within South African legislation there are predominantly three statutes that contain data protection provisions (albeit limited) that are worth mentioning, namely: The Promotion of Access to Information Act (PAIA); The Electronic Communications and Transactions Act (ECTA); and the National Credit Act (NCA). PAIA is essentially a law that has been enacted to give effect to an individual's constitutional right of access to any information held by the State or any another person and that is required for the exercise or protection of any rights. This Act, to a limited extent, addresses the active control principles as well as other data protection principles by:

- individuals' access to records containing personal information about themselves in the public and private sector;
- requiring public and private bodies to take reasonable steps to establish adequate internal measures which provide for the correction of personal information (if such measures do not exist) until legislation providing for such correction comes into effect; and
- prohibiting the disclosure of a record if it would involve the unreasonable disclosure of personal information relating to a third party (ECTA, 2002)

The aims and objectives of the Protection of Personal Information Act (POPI) are, in brief, to promote the protection of personal information processed by public and private bodies; introduce conditions to establish minimum requirements for the processing of personal information; provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; provide for the issuing of codes of conduct; provide for the rights of persons regarding unsolicited electronic communications and automated decision making; regulate the flow of personal information across the borders of South Africa; and to provide for any other matters connected with any of the points above (Bygrave, 2014: 42).

Chapter 2, Section 14 (Bill of Rights) of the Constitution of the Republic of South Africa (1996) provides that all have the right to privacy that includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. In other words, the government has an obligation to ensure the fulfilment of that specific right as enshrined in the South African Constitution of 1996. The POPI Act 4 of 2013 part I contains Schedule 1. This is a set of eight general data protection principles which lie at the very root of the data protection legislation. This schedule imposes a duty on every data controller to comply with the data protection principles in relation to all personal data in respect of which he or she is in control of and for

which they are responsible in terms of its information security. In April 2014 the some of the provisions of the POPI Act relating to the information regulator and the Act's regulations came into effect. Once the remainder of the provisions of the Act become operational, parties that process personal information will be required to conform to the provisions of the Act within one year of the commencement such provisions. To date the President of South Africa has not yet announced the commencement of the balance of the provisions of the Act. Therefore, the bulk of the provisions discussed in this study will only come into effect on the publishing of the enactment date by the President, in the South African Government Gazette.

This is the most comprehensive Act in the South African legal framework that recognises electronic transactions. The current legal framework in South Africa provides specifically for the protection of personal information or personal data. There is need to establish a balance between the protection of personal data to safeguard an individual's right to privacy and, at the same time, ensure that regulation does not interfere with the right of various data users who use personal data for legitimate purposes. An additional significance is the criminal law principle of legality which provides that conduct cannot be deemed to be illegal unless there is an existing law that prohibits such conduct (Bygrave, 2014: 49). Historically, privacy has often been equated with a right to dignity. However, the common law has developed to give recognition to the independent right to privacy. The *locus classicus* for support for this view is *O' Keffe v Argus Printing and Publishing Co Ltd* where the Plaintiff complained that her photograph and name had been used for advertising purposes without her consent.

3.10.3 What are data protection principles?

Data protection principles are also known as information privacy principles. They include: what data may be collected about individuals; who should be notified of any collected data; under what conditions collected data must be stored; the right of individuals to access and call for correction of stored data; and limits to the use and disclosure of stored data. Some other concepts included in data protection legislation

are: allowance for anonymous participation, trans-border data flow control and the handling of specifically sensitive information, such as health information. There have been several international attempts to define an international data protection standard (Bygrave, 2014: 60).

3.10.4 How do data protection principles relate to cybercrime?

Cyber criminals often use devices to gain unauthorised access to data or to commit cybercrimes. These devices may consist of hardware devices or attachments and software programs. Most software programs can be downloaded from the internet. Some of these software programs can be installed through electronic mail to the victim's computer. Valuable information, such as credit card numbers and personal passwords, may be obtained in this manner (Bygrave, 2014: 40).

POPI Act uses the term "personal information" instead of "personal data", "responsible party" instead of the term "data controller" and "operator" instead of the term "data processor". However, these terms bear the same meaning as ascribed above. The international instruments that will be discussed herein refer to data privacy "principles" which are to be applied when processing personal data; however, the *POPI Act* instead refers to "conditions for lawful processing". Again, data privacy "principles" and "conditions" refer essentially to the same concept.

In the context of data privacy, Roos correctly states that where the privacy of a person has been infringed by the processing of personal information (by unlawfully processing true and correct data about an individual or by processing false and misleading data about an individual) the aggrieved party can rely on the principles of the law of delict to exercise his or her remedies.

Such remedies will be limited to the following:

- (a) an interdict to prevent the wrongful processing of personal data or further processing of personal data; and / or
- (b) a claim based on the *actio iniuriarum* for *solatium* for non-patrimonial loss for the injury caused to the Plaintiff's personality as a result of the wrongful intentional processing of personal data; or
- (c) a claim for compensation under the *actio legis Aquiliae* for patrimonial loss (*damnum iniuria*) sustained due to the wrongful, negligent processing of personal data (Neethling, Potgieter & Knobel, 2006: 34).

3.10.5 International instruments for data privacy and protection

As already mentioned, in 1973 Sweden was the first country in the world to enact data privacy legislation. However, by the 1980s data protection had become an international issue due to the emergence of a global market and the increase ease with which personal information could be transmitted outside the borders of the country of origin which lead to the increase in the exchange of personal information across national boundaries, known as "trans-border data flows" . International data protection instruments that emerged post the 1980s, generally have two primary goals:

- i) the setting of standards at an international level for the protection of personal data; and
- ii) providing for the free flow of information across national boundaries (where there are adequate controls).

Bygrave (2014) raises four general features which are characteristic of most successful international instruments dealing with data privacy:

- i) privacy law is largely statutory;
- ii) data privacy legislation normally establishes independent regulatory bodies, often referred to as Data Protection Authorities (DPAs) to oversee its implementation;
- iii) data privacy laws often take the form of 'framework' laws; and
- iv) DPAs often play a lead role in how data privacy law is understood and applied, even where their views are only advisory (Bygrave, 2014: 60-61).

The most important international attempts for data privacy protection were the following three vital instruments, that have had a profound effect on data privacy laws across the world relating to the trans-border flows of data, namely: the Organisation of Economic Co-operation and Development (OECD) Guidelines on Data Protection; the Council of Europe (CoE) Convention on Data Protection; and the European Union (EU) Directive related to data protection.

The 2013 revision to the 1981 version of the *OECD Guidelines* was required due to changing technologies, markets, user behaviour and the greater importance of digital identities over the past forty years. The *OECD Guidelines* also contains a set of basic principles that apply to the processing of personal data where member countries and non-member countries are encouraged to implement the provisions contained in *OECD Guidelines*. However, the 1981 version of the *OECD Guidelines* did not contain requirements as to how these principles are to be enforced by member nations. The revised *OECD Guidelines* explicitly make provision for the establishment of DPAs. There are eight core principles contained in the revised *OECD Guidelines*. They include the limitation principle, quality principle, specification principle, use limitation principle, security guard's principle, openness principle, individual principle and the accountability principle. Additionally, the revised *OECD Guidelines* contains three principles relating to trans-border data flows,

namely, that:

- i) the data controller remains accountable for personal data despite the location of the data;
- ii) trans-border data flows should not be restricted where the other country substantially observes the *OECD Guidelines* or sufficient safeguards exist to ensure a level of protection consistent with the *OECD Guidelines*; and
- iii) restrictions to TBDFs should be proportionate to the risk considering the sensitivity of the data, the purpose and context of processing.

Non-Member states are also invited to adhere to the *OECD Guidelines* and to collaborate with member countries in the implementation of the eight principles across borders. In 1980, the Organisation for Economic Co-operation and Development (OECD) issued its privacy guidelines which are applicable to video surveillance. The main aim of the guidelines (updated in 2013) was to protect privacy and promote free flow of information. To obtain these aims, the OECD guidelines set out five principles for member countries that subsequently became the basis for national laws around the world:

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.
- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and

the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller” (OECD, 2013: 14-15).

3.10.6 The General Data Protection Regulation of the European Union

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for by unifying the regulation within the EU.

3.10.7 CCTV surveillance and value adding to public spaces

What values do public spaces produce for society and citizens? CCTV video surveillance has both positive and negative effects. CCTV encourages broad participation and interaction in public spaces, for instance, by increasing citizens' sense of community safety. With the help of CCTV, both public and private spaces can be made more secure and serve more social functions such as:

- spaces of shared and individualised economic activities; tourism; cultural activities; begging; and social integration (Lyon, 2011: 36).

Research has shown that shared spaces do or, at least, can contribute to a sense of community (Skjæveland & Grayling, 1999: 34). Conversely, research has also shown that exclusionary spatial practices contribute to disintegration, social exclusion, hate and intolerance in private spaces (Madanipour, 1998; Flint, 2004: 50). The American Civil Liberties Union (ACLU) has outlined many concerns about video surveillance. ACLU maintains that those with access to the data have routinely misused data collected through Closed-Circuit Television (CCTV) cameras (Lyon, 2006: 37). In the United Kingdom, video surveillance privacy falls under the Data Protection Act of 1998. Most countries follow the Organisation of Economic Co-operation and Development (OECD) guidelines for privacy protection of personal data including video data. In South Africa, the POPI Act 4 of 2013 regulates the usage of video data. Experts agree that video surveillance undermines our right to anonymity. CCTV Video surveillance, augmented with biometric technology (e.g. facial recognition), needs to follow certain principles of protection, namely:

- i) Principle 1: Fair and lawful processing. This principle requires that personal data must be processed fairly and lawfully and must not be processed unless at least one of the conditions in Schedule 2 of the POPI Act is met.
- ii) Principle 2: Obtaining and further processing of data for specified and lawful purposes is acceptable.
- iii) Principle 3: Requires that personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which it is acquired.
- iv) Principle 4: Retention policy. Video and other surveillance data to be stored and kept by users for a minimum of 30 and a maximum of 90 days.

In other words, user-specific user-interaction privacy principles relating to retention policies require built-in privacy protection capabilities (software), i.e. broad-based cybersecurity measures, that require, if there is any invasion of privacy of innocent

individuals, at the very least to obtain consent to use video data collected, for instance, as evidentiary purposes in court.

3.10.8 Criticising surveillance and surveillance critique: Why privacy and humanism are necessary but insufficient

Surveillance's present notoriety makes this an opportunity and urgent moment for such a debate. It has been argued that without Snowden, we would not have had such a public opportunity to influence what 'surveillance' means and entails (Drum, 2014: np; Lyon, 2015: 19). This is especially the case in the United States yet the Snowden affair demonstrates the status of telecommunications surveillance, at least, as an object of international concern. Whatever the morality and legality of his actions, it is clear enough that the leaks have rendered the future of state surveillance a little less certain, a little more open for negotiation. Nevertheless, surveillance is equipped with its own kind of rationality, one which works to close such windows of opportunity. These consistently insist on surveillance's autonomy that is, its ability and right to internally justify its own scope, validity and efficiency. When the NSA implores the public that the sensible thing to do is simply trust the security experts and let the unknown lie undisturbed (Lizza, 2013: 23; Ackerman, 2014: 12), they are working towards a situation where surveillance justifies itself according to its self-created mechanisms of proof. This extends to surveillance systems' claim to their strategic necessity. Public Senate committee hearings are used to broadcast that the (Western) world has become more dangerous than ever before, requiring ever more expansive forms of surveillance (U.S. Senate Select Committee on Intelligence, 2014: 63). The Snowden leaks help attract proper scrutiny on exactly these schemas of justification, persuasion and validation. In cases, such as social media participation, many of us have determined the surrendering of personal information to be, by and large, beneficial to our interests. After all, within the present state of affairs, giving up some degree of privacy can provide greater individual autonomy and scope of action (Lyon, 2015: 62). The loss of privacy is thus outweighed, in some contexts, by the fear of being isolated by the irrelevance of our secrets (Lyon, 2015: 31). This is not to say that we have knowingly and happily jettisoned privacy; more often, privacy is slipping through our fingers unwillingly and unwittingly. Increasingly, the

choice to 'opt out' of privacy intrusive services becomes a non-option, the equivalent of social erasure (Lyon, 2015: 36). One major reason that privacy-based criticism ends up fighting an uphill battle is that surveillance can typically fall back to the felt sense of security and its moral legitimacy), and in doing so, depict privacy as a disposable luxury.

During the early 2000s, two events occurred that were to shape the direction of surveillance decisively, although the potential connections between them were not made public until 2010. One was the attacks on the US on 11 September 2001 ('9/11'), the London bombings on 7 July 2005 ('7/7'), and the Madrid train attack, the aftermath of which hugely boosted security-related surveillance at least in the global north. Interestingly, the activities of the quickly formed Department of Homeland Security took some cues from 'Customer Relationship Management' in their quest for 'Total Information Awareness' (Lyon, 2003: 92f). The other was the definitive appearance of social media, symbolised by the invention of Facebook in 2004, that quickly established itself as a mainstream dimension of the internet, simultaneously facilitating new levels of consumer surveillance (not to mention social surveillance, now based on self-expressed preferences and tastes (Marwick, 2012: 60; Trottier, 2012: 80). By President Obama's inauguration in 2009 the US Department of Homeland Security (DHS) had developed a Social Networking Monitoring Centre to check for 'items of interest' (Lynch, 2010: 45). In a sense, then, the Snowden disclosures may be functioning as a wake-up call to publics still unaware that the day of mass surveillance of ordinary citizens had already dawned. If it was not already clear, after 9/11 the 'national security' rationale for intensified surveillance (Ball & Webster, 2003: 78) became prominent and with it the use of data analytics (now generally referred to as 'Big Data') (Lyon, 2015: 23).

The Total Information Awareness programme was dependent on a very large-scale database using "new algorithms for mining, combining and refining data" that included bank machine use, credit card trails, internet cookies, medical files anything, indeed, that might produce interesting correlations that might indicate meaningful relationships between records. These, the Snowden files show, are among just the methods used by the NSA in its surveillance both domestic and foreign (Lyon, 2015: 24).

3.11 CONCLUDING REMARKS

The increasing reliance on surveillance measures and technology security policies is based on an insufficient and incomplete knowledge and consideration of the social and economic cost of surveillance. The researcher predicts an increasing demand for surveillance solutions (stand-alone and integrated) rapid growth for commercial, residential, private and public places. There seem to be a number of potential benefits associated with CCTV. For the police, the potential benefit of CCTV in reducing crime by deterring offenders from committing an illegal activity may be much lower on its list of priorities than the apprehension of suspects who were caught on camera committing a crime (Norris & McCahill, 2006:45). The use of a camera image to aid in the identification and apprehension of a suspect, as well as to help secure a conviction in criminal court, is a common justification that is used by the criminal justice system alike in many jurisdictions currently experimenting with increased use of video surveillance in public places. The growth of CCTV seems largely dissociated from its capacity to fight crime, while it remains hard to prove that it is in line with a global population surveillance project. The diffusion process of CCTV development rather result from the combination of several factors: political parties' intention to announce safety concerns, headline grabbing by local authorities, central government wishing to strengthen public private partnerships at the local level (such as in Great Britain), growth of the security market, business interests, etc. CCTV can be analysed as a socio technical device, able to aggregate different types of protagonists carrying various specific interests. As an actor-network, CCTV turns out to be able to enlist protagonists by different mechanisms, beyond the circle of its initial supporters. Indeed, CCTV users can take the object on board and progressively acquire its multiple uses that then become justifications for its use, fuelling the buy- in process in a specific place. One stone remains unturned in this general overview of the international CCTV literature: is the diffusion of CCTV systems the expression of a new penology? This issue, raised in particular by Surveillance Studies, seems important, as contemporary cities, marked by a growing social heterogeneity, make up a background conducive to fear of strangers (Lyon,2011;45). However, only systematic comparison between observed CCTV uses and the adjudications made following case selection would allow the examination of two theses:

the extension of State surveillance capacities and the emergence of a new form of social control (shaped by local authorities) focused on the management of specific targets and behaviours. Such a comparison would gradually lead to totally new conclusions about a blind spot in the literature: the effective capacity of CCTV to normalize behaviour.

CHAPTER 4

RESEARCH FINDINGS: DATA ANALYSIS AND INTERPRETATION

4.1 INTRODUCTION

This chapter describes and discusses the findings of the study that was conducted in selected areas of Johannesburg and Tshwane in Gauteng Province. The primary aim of the research was to evaluate the use of CCTV surveillance systems for crime prevention and control from selected areas from Johannesburg and Tshwane. The aim was achieved by identifying what information to seek from participants/ respondents. The researcher tried to achieve this aim by utilising data elicited from a review of current literature, manual searches of CCTV evaluation study bibliographies. As the research study progressed, the researcher conducted manual searches of the references section of each study for potential inclusion.

The central or primary research question in this study was: *What is the contribution that CCTV surveillance systems can make towards crime prevention and control?* As a consequence, the interview questions and questionnaire were structured with a number of linked questions to expand on the above focus.

Face-to-face interviews were conducted with CCTV operators, and members of CPFs and residents in residential areas based on two sets of similar but slightly different interview question schedules and a survey questionnaire randomly applied to persons in streets. These two research instruments (schedules of interview questions and survey questionnaire) were first 'pre-tested' and then approved and certified by the supervisor before being implemented in the field. The questionnaire was revised in order to evaluate the respondents' perceptions of its purposes and capabilities, and any public concern in respect of CCTV implementation.

The interviews to CCTV operators focused on exploring several issues including the adequacy of training; how suspicious behaviours were identified; what monitoring

strategies were adopted; the quality of working relationships with external agencies; and the evidentiary value of CCTV surveillance systems.

While questions posed to members of residential CPFs/residents in those areas concentrated more on the following aspects:

- When were CCTV surveillance cameras installed in your neighbourhood/residential area (month/year date)?
- If 'public space' (streets/entrance to neighbourhood) (as opposed to on private/business/commercial property) has been indicated above what was the motivation/reason provided for its (CCTV Camera Surveillance System) installation in such public areas?
- If installed in 'public space' (streets/entrance to neighbourhood) who was responsible for deciding on its installation use of CCTV System as Evidence in Court.

The above primary framework components for the two sets of interview questions assisted in finding the state of current evaluation and implementation and other factors related to formulation of a secure crime prevention framework CCTV surveillance systems.

The researcher made both primary and secondary findings regarding the research questions.

4.1.1 Interview and survey questionnaires

Two sets of schedules of interview questions and one survey questionnaire were utilised in this research study, namely,

- i) Interview Schedule of Questions: Private Security Control Rooms: CCTV

Surveillance Operations (Annexure G);

- ii) Interview Schedule of Questions: CPFs & Residential Areas: CCTV Surveillance Operations (Annexure H); and
- iii) Street Survey Questionnaire (Annexure I).

The Interview Schedule of Questions questionnaires were set out (with subsidiary/clarifying questions for each topic/theme) as follows:

Section A:

- biographical information;
- highest educational/training qualification(s);
- experience related to the research focus; and
- occupational/work position/job description of interviewees.

Section B:

- area or location of the CCTV surveillance operation;
- what operational processes are followed in the control room for CCTV surveillance operations;
- what happens when a suspicious activity is picked up on CCTV cameras?

Additional questions for selected CPF area members/residents interview questionnaire:

- how is the CCTV installed in your area currently funded?
- what do you think are the crime reduction/prevention values/benefits of the installed CCTV surveillance cameras in your area?

Accordingly, Section A set out to measure the socio-demographic variables of the participants which included gender, age category, level of education and work experience.

Section B measured the level of CCTV surveillance camera awareness with reference to CCTV installation, ownership and decision makers regarding the recommendation of CCTV cameras as a security control measure.

4.2 DATA ANALYSIS AND DISCUSSION: SCHEDULE OF INTERVIEW QUESTIONS

4.2.1 Schedule of Interview Questions: Private security control rooms: CCTV surveillance operations (Annexure G)

Sixty participants were interviewed for this schedule of interview questions.

As a preliminary research procedure, the researcher sent out ten letters to different private security companies requesting permission to do the research at their company and interview selected members of staff, particularly in the control rooms. (see: Annexure D: Letter requesting permission to do research at their respective sites). This is in accordance with the principles of ethical consideration as discussed in Chapter Two of the study. Permission was received from six companies and names withheld for the sake of confidentiality. Computer laptop was used predominately during the observational period with minimal use of paper field notes (proving too cumbersome to complete within a limited working space). The primary audience for CCTV is a small number of relatively low-ranking workers within a security system (Smith, 2008: 12). They watch, with greater or lesser alertness, monitors which show flickering, grainy views, often of empty spaces. Entering data directly into an Excel spreadsheet was deemed an appropriate method for data collection in this particular setting. Benefits included the reduction in time spent transcribing handwritten field notes later and the ability to record data verbatim and accurately (i.e. speed of typing versus handwriting). The

manager and operators of the control room consented to the use of a laptop and expressed no reservation about the taking of notes during the observational period.

Four types of data were recorded during the observational period and these categories are very much related to Norris and Armstrong's (1999: 52) study of 592 hours of observation. The quantitative observational period included shift data – number of operators per shift, types of people entering the control room and length of monitoring; targeted incident data – how and why the surveillance was initiated and by whom; characteristic data – the age, sex and appearance of individuals from targeted incidents; and deployment data – whether deployment was necessitated and the outcome of deployment.

This study has enabled the researcher to partially fill a gap in the literature, by giving a voice to those closest to CCTV; a first-person account from 'those who know best'. This research focus led to the construction of several specific field questions. These were, namely:

- What goes on inside a CCTV control room? (By this is meant the job structure, length of shifts, pay, forms of management and interaction between co-workers etc.)
- How does the system work – i.e. who is targeted and why?
- Are the cameras effectively and rigorously monitored at all times?
- How are the operators trained and do their social backgrounds and personal prejudices influence who is monitored?
- How do CCTV operators interpret and make sense of a series of random images?

- Are CCTV cameras on the malls /residential areas, that is, to make the areas *appear* a safe place for the public to encourage potential customers/residents there?
- What do the operators themselves think of the cameras?

The principal research instrument for data collection was through systematic, investigative observation, where the ‘observer-as-participant’ technique was adopted (Gold, 1969: 36). This method is generally employed in short ethnographic studies, as it allows for relatively brief spells of formalised, overt observation, rather than prolonged periods of informal, covert observation or regular group participation (Clarke, 1997: 141).

In addition, data through the general conversations held with the operatives was amassed. Indeed, many of these wide-ranging discussions were turned into an informal style of interviewing. For most of the day, the cameras are left on an ‘automatic’ setting. Despite the fact that they are not being manually controlled, each camera still records everything that comes across its path in a time-lapse format.

Section A: Biographical and demographic information

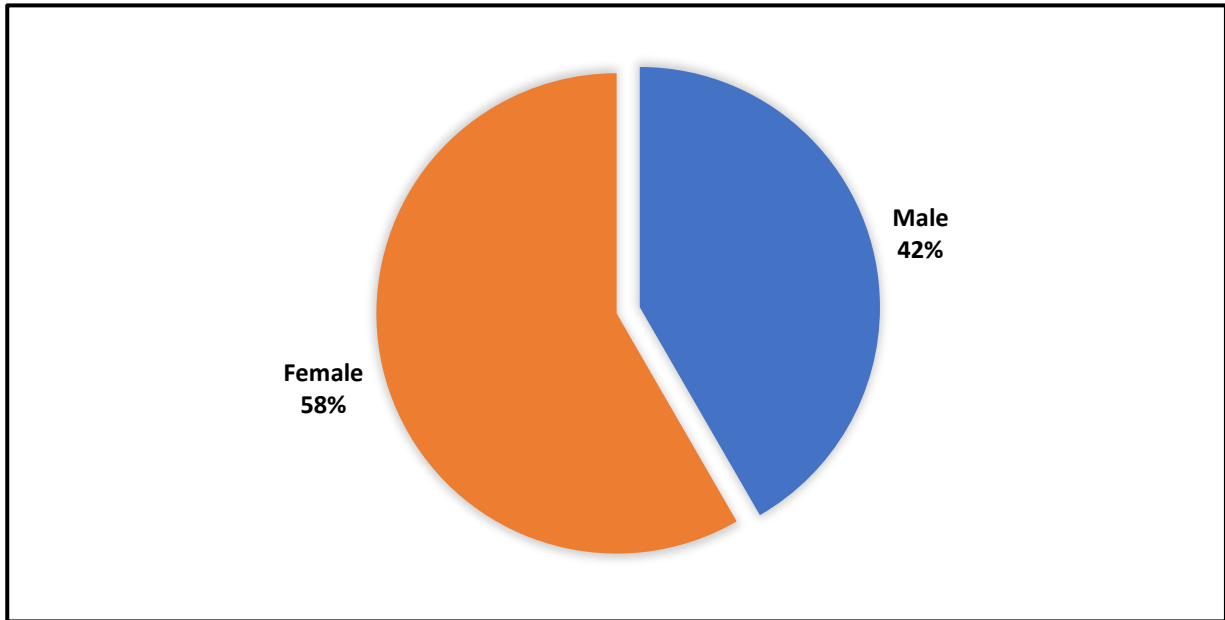
The important biographical and demographic information reflected in this study relates to gender, age, educational level and years of experience. A total of 60 respondents were revealed by the demographic data.

Gender composition of CCTV operators

Table 1.1: Gender composition of CCTV operators (n=60)

Gender	(X)
Male	25
Female	35

Figure 1.1: Gender composition of CCTV operators (n=60)



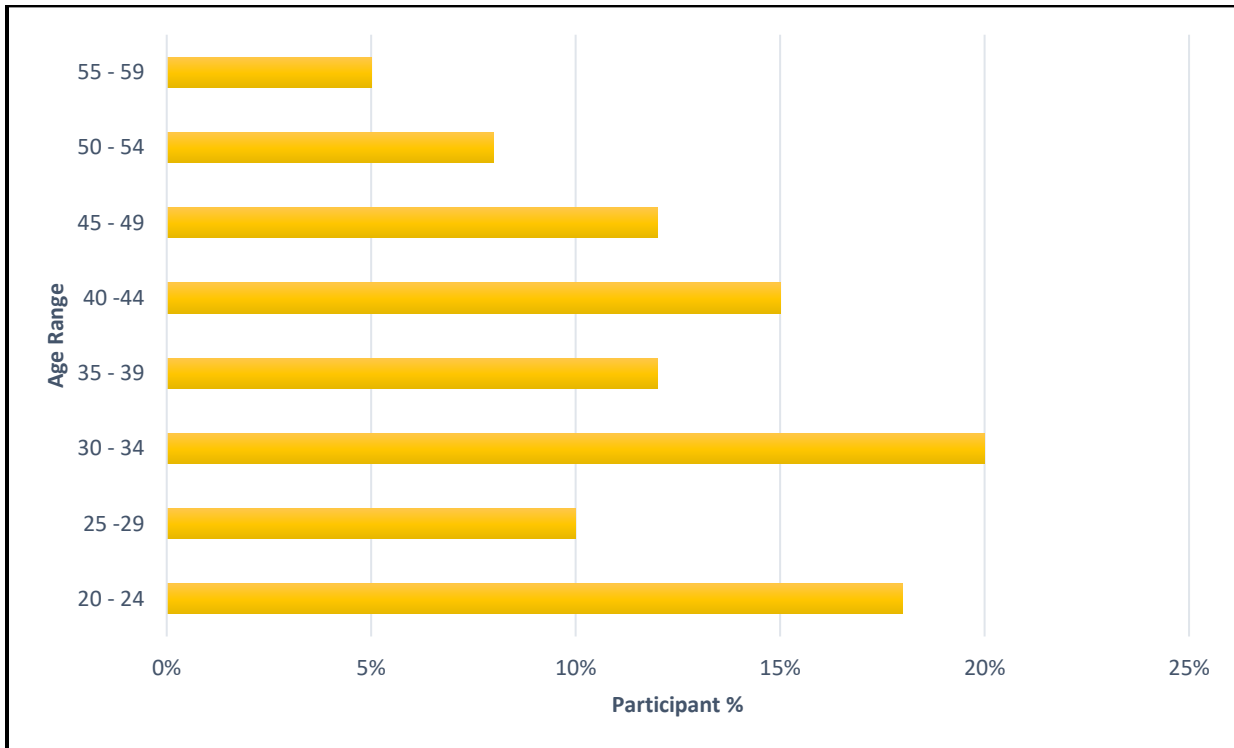
The gender demographics of the CCTV operators interviewed comprised 58 percent females (35) and 42 percent males (25). The preponderance of females in the sample may just be indicative that most CCTV monitor operatives in control rooms are in fact females, having proved to be more effective in monitoring operations having better concentration levels than their male counterparts (Donald, 2015: np).

Age Analysis of CCTV operators

Table 1.2: Age categories of CCTV operators

Age category	(X)	Age	(X)
20-24 years old	11	26-29	6
30-34	12	35-39	7
40-44	9	45-49	7
50-54	5	55-59	3

Figure 1.2: Age categories of CCTV operators



The above age grouping helps to understand the age group associated with the use of CCTV operations. The largest proportion of respondents is in the age category of 30-34 years (12) – an indication of years of experience. This is closely followed by those aged 20-24 years old (11) with lower numbers for the other age categories. This also implies that the industry requires energetic staff with experience. There are only a few aged above 50 years that represent a wide knowledge base about the theme being studied. Also, there are few below 20 years indicative of their lack of required experience.

The next section will look at the demographic summary relating to highest educational level of respondents.

Highest educational qualification

Table 1.3: Highest educational qualification (NQF levels) (n=60)

Highest educational qualification	(X)
Standard 8/Grade 10	12
Standard 9/Grade 11	10
Standard 10/Grade 12	8
Certificate Level NQF 3-4	9
Certificate Level NQF 5	6
1-year Diploma	7
3-year Diploma	8

[Note: The categories of: BA degree; BTech; Advanced Diploma; Hons/Postgraduate Diploma; Masters; and Doctoral – all had nil returns.]

Fifty percent of the respondents' highest qualification was in the combined high school categories, namely, Standards 8-9-10/Grades 10-11-12 (30). (Standard 8/Grade 10 = 12; Standard 9/Grade 11 = 10; and Standard 10/Grade 12 = 8. Total = 30)). Next highest had a certificate (Higher Education Qualification Framework (HEQF) level 3-4) = 9; followed by a three-year diploma (8); a one-year diploma (7) and a certificate (NQF level 5) (6). The post-matric educational levels represented by these qualifications had a total of 30 making up the balance of 50 percent. None of the postgraduate categories had any representatives. Their respective roles and levels of responsibility (seniority) were governed by their educational qualification levels. It can also be concluded that the highest number per category having only a Standard 8/Grade 10 level of schooling points to the need for on-the-job training by the employer companies.

The following section indicates the total number of years of work experience in the private security industry of interviewees.

Years of work experience in the private security industry

Table 1.4: Years of experience working in the private security industry sector (n=60)

Years of work experience in PSI	(X)
Less than 1 year	20
1 year	12
2 years	7
3 years	13
4 years	1
5 years	3
6-9 years	4

[Note the categories of: ‘10 years’; ‘11-15 years’; and ‘more than 15 years’ – all had nil returns].

Table 4.4 presents the years of experience per CCTV controller who were interviewed. The largest number (20/33%) as displayed in the table had less than a year in the job. The next highest category was ‘three years of experience’ (13/22%); followed by one year of experience (12/20%); and lesser numbers for ‘two years of experience (7/11.7%).

The following section refers to what position (job) and for how long that position been occupied by the interviewee at the company where they work.

Table 1.5: Occupational position in the company

Position	(X)
Site Manager	3
Supervisor	5
Team leader	15
Member of response team	13
Control Room Operator	11
CCTV Surveillance Operator	13

Figure 1.3: Work position in the company

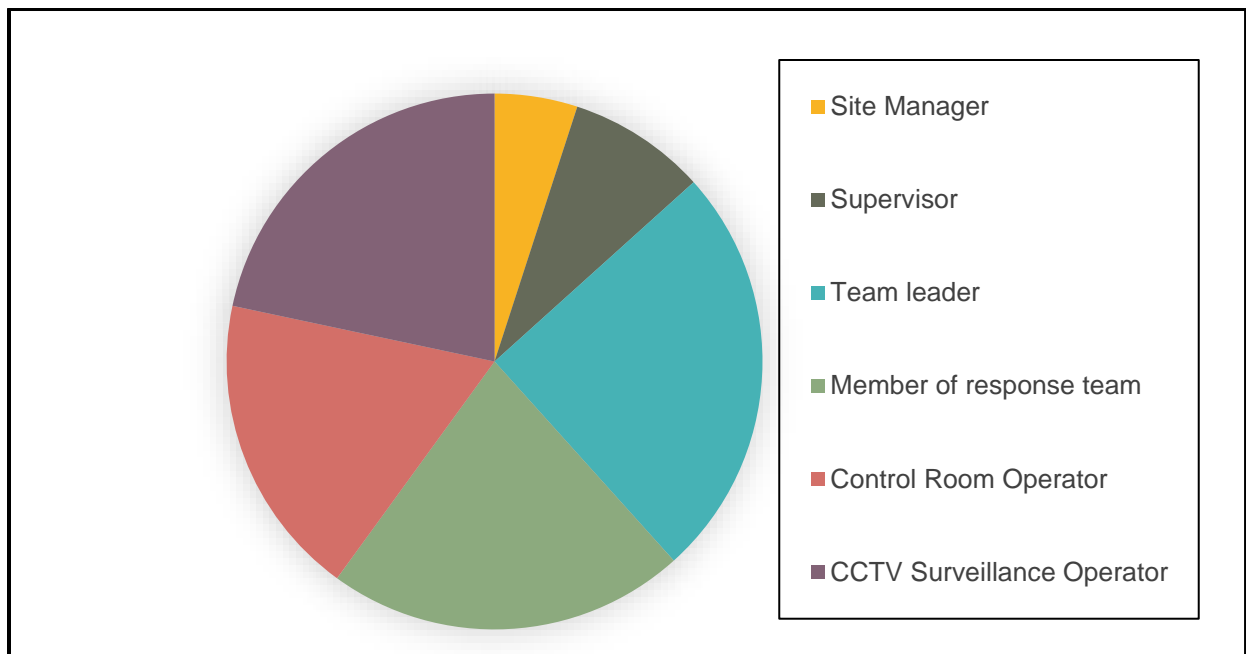


Table 4.5 displays, the hierarchy of occupational position in the company where they currently worked of CCTV operator interviewed. The highest number reflects that of CCTV operators which means they are the majority dealing with the monitoring of CCTV surveillance. Figure 4.3 indicates that 22 percent of participants are in the CCTV surveillance operators' category with the same number being members of a response team. In other words, 44 percent fall under junior management.

How many years of work experience in current position?

Table 1.6: Years of experience in current post

Years of experience in current post	(X)
Less than 1 year	25
1 year	7
2 years	14
3 years	3
4 years	10
5 years	1

[Note: For the following categories there was a nil return: 6-9 years; 10 years; 11-15 years; more than 15 years.]

According to the table above, 42 percent of the participants had less than one year's experience in their current job position.

Section B: CCTV surveillance operations

In this section of the interview questions set out to determine various aspects of CCTV surveillance operations. In addition, the interviews set out to obtain information on the following aspects: For each incident, the following information was recorded by the observer: date of incident, start and end time of incident, total surveillance time in minutes, camera or cameras used, camera operator, location, description of incident (i.e. assault, intoxicated in public), description of individual/s if applicable (i.e. male, approximate age), police deployment and whether arrest/s were made. Each incident was double checked against the control room's logbook to ensure:

- i) time of surveillance was correct;
- ii) whether the incident resulted in an arrest; and
- iii) whether footage was requested by police, etc.

At all times, an operator was present in the control room with a second operator working during 'busier periods', such as Friday and Saturday nights, as well as events that attracted higher than usual crowd numbers in areas under surveillance. A CCTV system is not a physical barrier. It does not limit access to certain areas, make an object harder to steal or a person more difficult to assault and rob. This does not mean it is not an example of situational crime prevention. It is highly situational, and as will be shown, does have some crime prevention capacity in the right situations. Although CCTV has many functions, the primary preventative utility is to trigger a perceptual mechanism in a potential offender. It seeks to change offender perception so the offender believes if he commits a crime, he will be caught. In other words, CCTV aims to increase the perceived risk of capture, a factor which, assuming the offender is behaving in a rational (or limited rational) manner, will de-motivate the potential offender. For this crime prevention process to succeed, two elements must exist:

- (i) The offender must be aware of the cameras' presence; and
- (ii) The offender must believe the cameras present enough risk of capture to negate the rewards of the intended crime.

The researcher felt that the pre-interview informal discussions held with a potential interviewee were very beneficial, particularly from the perspective of 'breaking the ice' and helping the interviewees to relax (Creswell, 2013: 45). The recording of the interview, rather than taking notes, also allowed the researcher to pay more attention to the mannerisms and body movements of the interviewee and the researcher neither observed nor received any concerns from any interviewee about the interview being recorded (taken into consideration the element of concentration by the interviewer). A variety of themes were identified from the responses to the interview questions and in the informal discussions both before and after the interviews. These themes are outlined hereunder:

- significant consultation with a wide range of stakeholders takes place in advance of the installation of any system;
- there was widespread community concerns about criminality and social disorder in their areas.

To the question of where CCTV surveillance systems (cameras) were installed the following was indicated in the responses:

Table 1.7: Sites where CCTV cameras are installed

CCTV installed site	(X)
On public streets	11
Residential neighbourhood	11
Central Business District (CBD)	9
Shopping centre/mall	7
Gated neighbourhood	6
(Private) Security estate	5
Business premises	5
Factory/industrial site	3
Along highways	3

The highest number of cameras installed are in residential areas as demonstrated above in the table. The reason for installation sites identification being for the researcher to understand precisely whether there is interaction between CCTV operators and the various installed surveillance systems sites.

The above table and graph show that public streets and residential areas have the largest proportion of installations (18%), followed by CBDs (15%). This suggests that CCTVs are installed where the highest criminal presence or number of crime incidents occur.

Description of CCTV camera installations at sites

Below is a description of the specific site where the CCTV cameras have been installed at each of the sites above.

Shopping centre/mall

Table 1.8: Shopping centre/mall

Shopping centre/mall	(X)
Inside mall along walkways/passages	19
Underground parking/parkade	18
In open-air shopping centre car park	13
At entrances to shopping centre	7
Inside shops	3

All areas in which CCTVs are installed are indicated in Table 4.7, with (in order of priority) the top three sites for CCTV camera installations being: i) Inside malls along walkways/passages; ii) Underground parking/parkades; and iii) In open-air shopping centre car parks.

Residential neighbourhoods

Table 1.9: Residential neighbourhoods

Residential neighbourhood	(X)
At entrance access roads	27
Along residential streets	18
At cross roads/corners of streets inside residential area	12
On masts on private property of selected residents' properties	3

The above table indicates places where CCTVs are installed in residential areas with 45 percent indicating “at entrance to access roads”; followed by 30 percent “along residential streets”.

Central Business Districts (CBDs)

Table 1.10: Central Business Districts

Central Business District (CBD)	(X)
On street corner mast	39
Along pedestrian walkways	11
Mounted on selected buildings	7
Along pedestrian walkways	11
Inside buildings	3

Most cameras installed in CBDs are to be found mounted on street corner masts (streetlight poles) (65%). (The names of CBDs are withheld for security reasons).

Table 1.11: Gated neighbourhoods

Gated neighbourhood	(X)
At boom gate access-controlled entrance	21
At entrance access roads	12
Along residential streets	14
At cross roads/corners of streets inside security estate	7
On masts on private property of selected residents’ properties	6

As the table above points out, CCTV installations are mounted at boom gate entrances to gated neighbourhoods (35%); followed by along residential roads (23%) in the vicinity and at the entrance to access roads to the neighbourhood (20%). In car parks, there may be little resistance to the installation of CCTV cameras. In part, this is

because the public space is utilised for one rather inconsequential purpose – the parking of vehicles. It is also the case that a car park is a well-defined and clearly marked physical space, meaning that individuals know that it is a car park and can choose to park their vehicle there or not (providing there are other alternatives). These points stand in sharp contrast with how individuals come into contact with CCTV in other public settings.

Private security estates

Table 1.12: Private security estate

Private security estate	(X)
At boom gate access-controlled entrance	25
At entrance access roads	13
Along security estate roads	11
Along perimeter walls (at intervals)	6
On masts on private property of selected residents' properties	5

As the table above shows, the largest number of CCTV installations at private security estates are mounted at boom gate entrances (42%); followed by entrance access roads (22%); and along security estate streets/roads (18%).

Table 1.13: Business premises

Business premises	(X)
Over vehicle parking area	29
At access-controlled entrance	13
Along perimeter fencing/wall	7
Mounted on business premises' building	6
Inside business premises	5

At business premises, most of the CCTV installations are found at the vehicle parking areas (48%); followed by 22 percent at the access-controlled entrances.

Factory/industrial site

Table 1.14: Factory/industrial site

Factory/industrial site	(X)
Over vehicle parking area	34
At access-controlled entrance	14
Along perimeter fencing/wall	6
Mounted on factory building	3
Inside factory building	3

Similarly, to business premises, at factory/industrial sites, 57 percent indicated that the CCTV cameras are installed in the site's parking areas followed by 23 percent at the access-controlled entrances.

4.2.2 Operational processes followed in control rooms for CCTV surveillance

In this section ten questions, reflecting differing opinions on the use of CCTV, were posed to the participants for the purpose of ascertaining their general views on the subject. Each participant was asked to indicate their level of understanding and awareness with each statement, by providing answers about their views on CCTV, which display some of the general attitudes towards this measure. Here the researcher focussed on their knowledge of the technology and the meanings that they ascribed to it. The researcher consequently looked at selected aspects of the interviews, namely: at how the informants link CCTV to crime. In this regard the researcher discussed their perception of CCTV as a measure against crime and their assessments regarding the assumed aims of public CCTV surveillance.

As David Lyon (1994) has pointed out, the sociological response to the general issue of surveillance has been dominated by images of the Panopticon (Lyon, 1994: 61). These interviews focused on exploring several issues including the adequacy of training; how suspicious behaviours were identified; and what monitoring strategies were adopted; the quality of working relationships with external agencies, and the evidentiary value of CCTV.

An issue raised by Norris & Armstrong (1999: 28) in relation to the disciplinary potential of public CCTV systems concerns the problem of classification. As Poster (1990: 34) pointed out, the disciplinary power of the panopticon is only complete when one-way total surveillance is combined with a detailed “dossier that reflects the history of his deviation from the norm” (1990: 91). As Norris and Armstrong point out, the street population monitored by open street CCTV surveillance systems are unknown to the observer, which means that those watching the screens are unable to systematically identify and classify people in public space.

To the question: *What operational processes are followed in the control room for CCTV surveillance?* – interviewees provided various descriptions of what operational processes are followed by control room operatives when operating CCTV surveillance systems. For instance, below are various descriptions of what operational processes are followed by control room operatives when operating CCTV surveillance systems:

A control room is manned 24 hours a day, 365 days a year. For most of the day, the cameras are left on an ‘automatic’ setting. This means that they follow a pre-programmed, computerised time-pattern schedule by rotating round full circle approximately every 2 to 3 minutes. Even though they are not being manually controlled, each camera still records everything that comes across its path in a time-lapse format. Each day this footage is stored on a special videotape, allowing anyone with a legitimate complaint the chance to review a tape from the day of a particular incident (Interviewee AD, 2018). However, this can be a lengthy process: “It usually takes us about 3 to 5 hours to do, and it has to be done on the central monitor... which

means the operator [while this process is going on] can only monitor the little, split screens to watch the campus” (Interviewee, A6, 2018).

Perhaps more importantly, and echoing findings by McCahill and Norris (2002 :171), when tapes are being reviewed, none of the cameras actually record. The process of requesting CCTV footage follows a strict chain of evidence and can only be accessed by relevant authorities, usually the police. The tapes are kept, by law, for a maximum of 31 days after which time they must be wiped clean. This process is a computerised, automatic setting which enables the operator to monitor a single camera (the image from which appears in real-time enlarged on the central screen), and to systematically ‘ignore’ footage from the other cameras showing on the monitors in the control room. However, this ‘prioritising’ process does have its drawbacks as one operator pointed out.

“While monitoring CCTV cameras is one of the primary roles for staff in the security control room, they also spend a significant amount of time retrieving footage when it is requested by internal and external parties, including SAPS” (Interviewee H2, 2018).

These responses to the above question complement what was found by Norris and Armstrong (1999: 45) that the level of operator integration within other agencies of control – such as the police – private security officers patrolling on the ground are a crucial determinant factor behind quick and successful deployment. Furthermore, the research took as its starting point the general view put forward by McCahill and Norris, (2002: 40) that the relationship between surveillance and society is that of exchange.

Another example of the social processes underpinning CCTV operations can be seen in McCahill and Norris’s (2002: 67) research, which revealed how management’s use of cameras to monitor and control employees was undermined and resisted by security staff and lower level workers due to their shared class identity. CCTV operators demonstrated how fire prevention, property management, co-ordinating the activities of

the workers and car park administration, as opposed to explicit social control, sit higher on day-to-day managerial operational agendas. According to McCahill & Norris, (2002 :44), CCTV systems have diverse operating procedures, staffing policies and levels of technological sophistication. McCahill and Norris (2002: 67) further describe, for example, how handling alarms, parking barriers and door entry systems, along with health and safety concerns, form the basis of an operator's day rather than monitoring and targeting certain social groups with the cameras. Indeed, McCahill and Norris's (2002) state that the usage of CCTV in this way was "rare" (McCahill & Norris, 2002: 67). CCTV operators are also intensely exposed to the emotional control of the actual camera images they watch, frequently being overcome by resultant negative feelings of boredom, frustration, stress, guilt, sadness and anxiety (Smith, 2008:12).

Nearly all of informants assumed that CCTV has been applied mainly for crime reduction. CCTV operators discussed the process of contacting police when an incident appeared to warrant police attention or deployment. Operators expressed the relativity of time when police respond to incidents, especially knowing they may be attending to other incidents, short of staff, or an officer is unable to answer the telephone/view the monitor due to a more pressing (crime) situation. In addition, operators knew to also prioritise incidents in relation to the workload of police, yet would store footage for future use if requested or necessitated.

4.2.3 Response to suspicious activities observed

To the question: *What happens when suspicious activity is picked up on the CCTV cameras?* – descriptions of what happens when suspicious activity is picked up on the CCTV cameras and observed in the control rooms were provided, namely:

"CCTV surveillance systems direct security personnel to situations which may lead off their translation into crime. CCTV monitors are monitored by CCTV operators who reports instantly suspicious criminal activity in the areas covered video surveillance. CCTV deters potential offenders who perceive an elevated risk of apprehension. CCTV may be perceived as reducing the time

available to commit crime, preventing those crimes requiring extended time and effort” (Interviewee, A4, 2018).

“Reaction/patrol officers are summoned to attend to the scene. This reaction activity is done with the collaborative effect with the control room. If the suspicious activity constitutes crime, more resources are mobilised, e.g. the SAPS and supervisor on duty on the specific day” (Interviewee A5, 2018).

In this regard, in these conditions, policing becomes increasingly proactive rather than reactive. In his survey of town centre managers Reeve (1996: 75) found that a third of respondents had “new powers to ensure that inappropriate activities and uses do not occur”.

“The camera network is actively monitored from a security control room, which enables the deployment of SAPS and response security personnel when incidents are detected” (Interviewee A6, 2018).

Furthermore, the kind of activity/incident on which a response team is sent out is described below:

“Response team is summoned to investigate the matter; they do this in collaboration with CCTV Controller. The most common signals we receive are burglary, panic, electric fence activation and power failures. We also monitor various other equipment such as CCTV and various guard monitoring systems. Our vehicles are all equipped with live satellite tracking which helps us with control and logistics. They are also dedicated to their areas allowing for quicker response times” (Interviewee A6, 2018).

To the question of whether their company co-operates with the SAPS in responding to observed crime incidents, all respondents answered in the affirmative (100%). In

describing the manner in which they co-operate with the police, one interviewee described in detail how this is done:

“Intelligence sharing [is] very common between the SAPS and private security staff. One of the functions of CCTV surveillance systems is [as] an instrument used as ex-post investigative tool used by police [video footage as evidence in court]. There was also evidence of the police supporting offender information to mobilise the security staff in the active monitoring of the offenders” (Interviewee, A7, 2018).

Another participant mentioned that:

“In our office board we have contact numbers for the SAPS and other emergency departments. For instance, for police we call 10111 and for the Fire brigade we contact 998/999 and for Life Line¹¹ we contact 086 132 2322” (Interviewee A7, 2018).

Now that some CCTV systems have audio links, the operators can actually ‘speak’ in real time to the watched. In the absence of such, a patrol officer is summoned to the scene of the suspicious (or crime) activity being observed.

At its best, CCTV was said to be a cost-effective tool which could help speed up investigations and encourage offenders to plead guilty, saving police and court time. This is similar to findings by Levesley and Martin (2005) regarding police attitudes to CCTV usage. CCTV was also seen as an aid in locating a wide range of incidents that might require police intervention. This related not only to criminal conduct but also to public safety issues. CCTV surveillance cameras have been used to locate lost children, missing persons and to initiate ambulance responses for people that had collapsed (fallen down) in public places. In addition to assisting in the deployment of officers to incident scenes, CCTV is also valued by CCTV operators for assisting in

¹¹ AN NGO providing counselling, particularly for people who phone in and reveal indicate suicidal tendencies.

the tracking and location of offenders, and for providing an independent witness once an offender is located. The major perceived advantage of footage is that it encourages suspects to plead guilty, thereby reducing the administrative workload of police and saving time spent in prosecuting offences.

In this regard, Bowcott, (2008:np) reported that “only 3% of street robberies in London were solved using CCTV images” (Bowcott, 2008: np), although other studies report that the three percent statistic in fact applied to all crime (Edwards (2009:np), commenting on the same report, stated that: “up to 80 per cent of CCTV footage seized by police is of such poor quality that it is almost worthless for detecting crimes” (Edwards, 2009: np).

One of the major purposes of CCTV surveillance systems is to provide appropriate evidence to arrest and convict offenders. Police in all locations visited spoke highly of the value of video evidence and viewed this as one of the most tangible benefits CCTV offered to policing. Communications between police and control room operators are vital to any actively monitored system. The common practice is for there to be some form of direct telephone link between control room operators and local police stations or police officers out on patrol, allowing operators to inform police of incidents and vice versa. In addition, operators commonly have a two-way radio tuned into the police frequency in the control room, to enable them to focus on relevant incidents and provide video evidence that may later be required in prosecutions. In most locations where there is active monitoring, operators maintain telephone communications with Police Communications Centres or the police station during an incident. The advantage of a monitor located in police facilities is that police personnel can then direct police on the street.

Accordingly, CCTV is perceived to assist policing in a number of ways. These are:

- co-ordinating police responses to incidents;
- improving detection and clear up rates; and
- providing evidence for prosecution

To the question on how CCTV surveillance fits into overall crime prevention initiatives, most participants indicated that:

“Footage from CCTV surveillance system can be presented to court by the SAPS testifying in [a] court of law to seek conviction and suspects may also present in court seeking [a] verdict [in their favour], [In other words] it works in the other way” (Interviewee A8, 2018).

To the question of what value they thought CCTV surveillance operations can provide to crime prevention initiatives in local areas, most participants indicated the following:

“In places where CCTV is installed, research shows there is a crime reduction” (Interviewee A9, 2018).

The literature study in Chapter 3 revealed the importance of CCTV in crime prevention. In addition, the effect of CCTV on the public, including: evidence of effects of CCTV systems on feelings of safety in public; evidence of the effects of CCTV on alleviating fear of victimisation is also given.

When asked how CCTV surveillance systems can best assist in solving crime, again the majority indicated that the significant reduction of crime was the primary motive for its installation.

“One suburb saw a 90% drop in crime since the addition of the cameras. This fall in crime is attributed to camera installation and its impact either as a deterrent” (Interviewee R, 2018).

To the question of whether any CCTV footage from the CCTV surveillance operations in the control room where they were working resulted in the solving of a crime (i.e. led to the arrest of a perpetrator and/or a successful prosecution of the suspect), all respondents answered this question in the affirmative (100%) and indicated that at least one of their cases in the previous three years had been used as evidence in court leading to a conviction. A major example of such successful use being the Bozwana murder case:

“The High Court in Pretoria has admitted CCTV video footage as evidence, showing slain North West businessman, Wandile Bozwana, before [and as] he was assassinated” (Interviewee Q, 2018).¹²

Overall, CCTV operators were of the opinion that CCTV surveillance systems add great value to crime prevention and positively add to overall reduction in crimes in the areas surveilled.

Two final questions regarding how the utilisation of CCTV surveillance can be improved for more effective crime prevention, the general consensus was:

“The use of human beings as CCTV monitors must be discouraged, fatigue affects concentrating, rather opt for automation” [i.e. addition of analytics software] (Interviewee 2, 2018).

¹² In the Pretoria High Court, a senior police forensic analyst detailed the techniques used in analysing close-circuit television (CCTV) footage to map out the movements of four men accused of the murder of North West businessman, Wandile Bozwana and his business partner and lover, Mpho Baloji.

In this regard, available literature on CCTV monitoring operations points to the fact that the use of humans in the process of operating CCTV is not the best recommended procedure due to fatigue during the long hours of work (Norris & Farrington, 1999: 12). This factor might lead to the risk of offenders/perpetrators of crimes going unnoticed.

Even though it is regarded as very effective since:

“CCTV surveillance offers multiple eyes [cameras] at the same time unlike a security guard stationed at a specific point [and] instructed not to desert a post” [i.e. being static] (Interviewee SI, 2018).

To the question: *Has any CCTV footage from CCTV surveillance operations in this Control Room been used to solve (leading to arrest of perpetrator/successful prosecution) a crime?* And follow up questions requesting more information on the response to the primary question in this section, namely: i) if yes, provide some examples/cases of such?; ii) how often (number) in the last (indicate selected time period with an ‘X’) has that occurred (indicate number of cases); iii) list (in order of priority by number of incidents) for what crimes (no more than ten crimes to be listed)? iv) in the listed cases above were any of the perpetrators arrested? To these questions the following data was provided:

Table 1.15: Number of cases used within time period

Period of time*	“X”	(Estimated) Number of cases
Previous six months	6	4
12 months	4	2
Two years	1	2
Three years	3	1
Four years	1	0

[*Note: the category in the questionnaire: ‘five years’ had a nil return.]

As shown in Table 4.15, CCTV evaluations on crime statistics showed mixed results in their effectiveness in reporting crime. For the previous six (6) months, 4 cases were reported as narrated by participants. However, participants argued that an increase in police recording consequent on CCTV installation was desirable since it was evidence that CCTV surveillance is important for crime prevention and control. Table 4.15 displays the frequencies of cases reported within a certain time period under CCTV surveillance system observations. As indicated in the table, for the previous six months, four cases were reported followed by two cases for the preceding 12 months and two years' periods respectively.

Only three types of cases (crimes committed) that were used were listed as follows (in order of priority by number):

Table 1.16: Crimes in order of priority of cases used

1. Murder
2. Vehicle hijacking
3. Theft

In all the cases listed, the participants indicated suspects were arrested. The CCTV footage provided as evidence led to both successful arrests of perpetrator(s) of the crime(s) and successful conviction(s) assisted by the video evidence provided by CCTV systems. Most of the convictions occurred within six months of the arrest(s) and were most successful in murder cases. As one participant put it (in a murder case):

“In the case of Zwelethu Mthethwa, he was convicted last year for murder evidence of his action retrieved from CCTV footage, the judge described it a ‘Silent Witness’” (Interviewee A12, 2018).

The key finding from this part of the study was what was termed the 'boredom factor'. The aim of the daily routine is to prevent trouble and to resolve disturbances, wherever they occur. The boredom factor arises principally from the monotonous viewing of hours of routinised, uneventful televisual images. The general concord surrounding the CCTV cameras, was that they were a useful tool in the fight against crime: "They [the cameras] certainly make life a little bit easier... I mean it's much easier to follow someone with the cameras than it is to follow them on foot, because most of the time they don't even know that they're being followed" (Interviewee A7, 2018). Findings call into question the effectiveness of the control room detecting incidents with operators spending less than one-fifth of their time actively searching for and monitoring incidents and most incidents (55%) being initiated by police communication.

In conclusion, the objectives to employ and use video-surveillance are shaped different expectations and practices of the actors involved. The researcher observed that the control room is connected to its environment by several links – communication and information devices. The researcher noted the following:

- radio or telephone link to the security patrol in the mall and to facility staff in the centre (technical and cleaning service);
- cell phone 'always carried': all shops have an emergency number to inform security in case something happens;
- emergency linkage to parking ticket dispenser and car park entry/exit;
- elevator emergency alarm fire alarm systems, connected to the fire station entry alarm systems; and
- direct telephone lines or radio linkages to maintenance service, activated in case of an alarm.

These multiple linkages make it clear that many sources of information impact the work of the observer in the control room which really is the 'nerve centre' of the shopping mall. It is the place where incoming information needs to be handled and managed and where, if necessary, decisions are made immediately. The CCTV-system represents one information source besides others. A contracted security company runs both systems observed. The staff are divided into specialised operators and guards. Two modes of internal work organisation are applied:

- a strict division between video operator and guard; and
- a more flexible mode where everyone on staff performs video work and patrolling according to internal arrangements and changing demands.

4.2.4 Schedule of Interview Questions: CPFs and residential areas: CCTV surveillance operations (Annexure H)

In the study by Ditton (2000: 692-695), respondents were presented with several CCTV-related statements such as: 'CCTV might stop the innocent from being wrongly accused'; and 'CCTV won't reduce crime; it will drive it elsewhere'. Overall, respondents showed mixed responses towards these. Few studies have measured respondents' actual knowledge of how CCTV works, and the link between people's level of knowledge and support for CCTV. One study observed that, "public acceptance is based on limited, and partly inaccurate knowledge of the functions and the capabilities of CCTV systems in public places" (Norris & Armstrong, 1999: 56).

This interview questionnaire was aimed at determining the knowledge and attitudes/opinions of residents with regard to CCTV surveillance camera operations in their CPF residential area. Forty residents or CPF committee members participated.

Section A: Biographical information

Gender

Table 1.17: Gender composition of CPFs and individuals in residential areas (n=40)

Gender	(X)		(X)
Male	16	Female	24

Figure 1.4: Gender composition of CPF members and individuals in residential areas

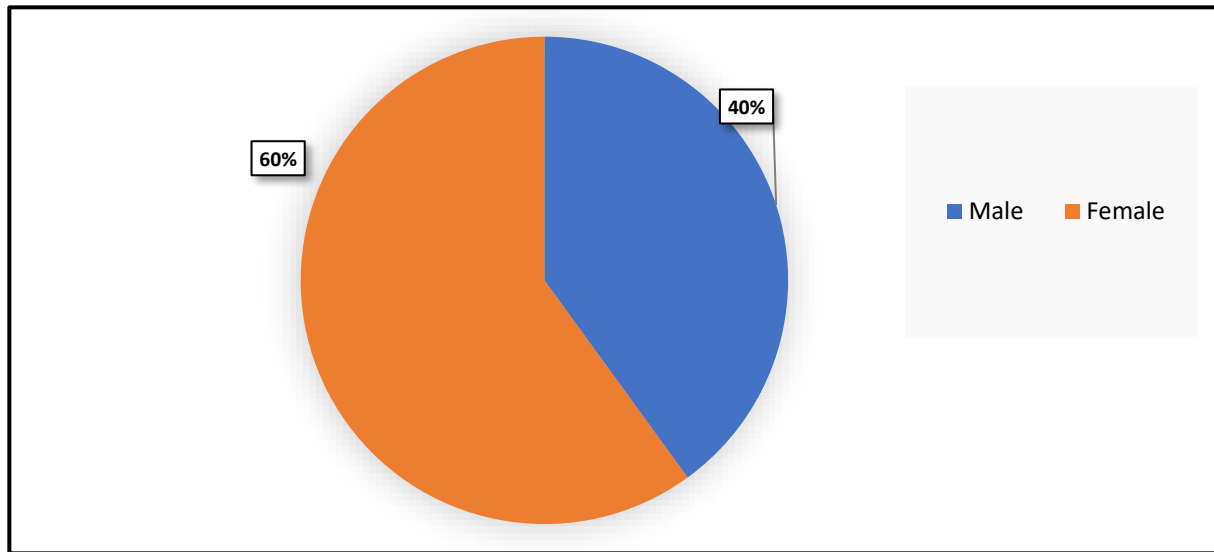


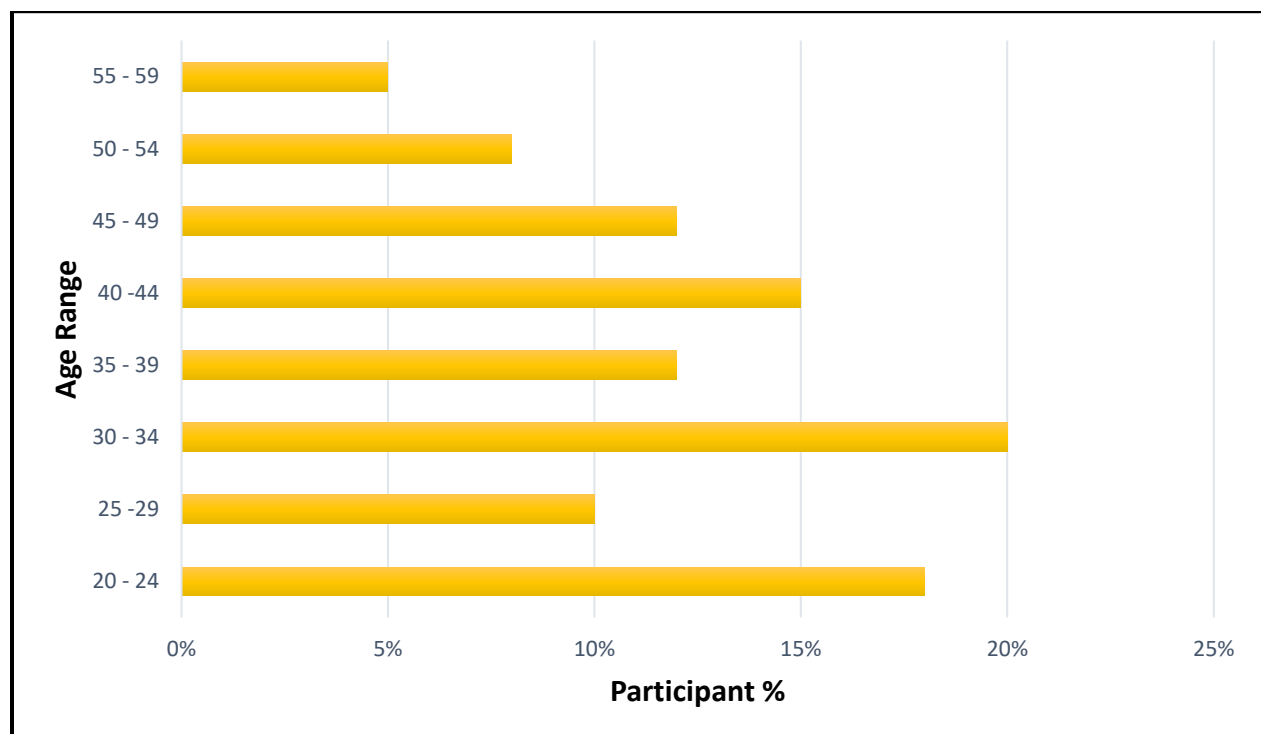
Figure 4.4 and Table 4.14 depict the gender composition of participants interviewed in residential areas with CPFs having CCTV surveillance systems in their areas. A total of 16 (40%) males and 24 (60%) females participated.

Age of participants

Table 1.18: Age categories of respondents

Age	(X)	Age	(X)	Age	(X)
20-24 years	8	26-29	5	30-34	12
35-39	7	40-44	4	45-49	2
50-54	2	55-59			

Figure 1.5: Age categories of CPF members and individuals in residential areas



The bar graph above displays the frequencies of age distribution of CPFs members and individual respondents. The age group that participated was mostly in the category: 30-34 years old (30%); followed by the category: 20-24 years old (20%).

Highest educational qualification of participant

Table 1.19: Highest educational qualification

Highest educational qualification	(X)
Standard 10/Grade 12	11
Certificate Level NQF 3-4	8
Certificate Level NQF 5	12
1-year Diploma	2
BA degree	1
BTech	1

The largest proportion of the participants, as indicated in the above table, had certificate (NQF level 12) followed by Grade 12 respectively.

Section B: CCTV surveillance operations (in CPF/residential areas)

To the question of where CCTV surveillance cameras were installed in their neighbourhood/residential area, the following sites were indicated:

Table 1.20: Where CCTV installed in neighbourhood/residential areas

CCTV installed site	n=40
Shopping centre/mall	7
Central Business District (CBD)	9
Business premises	5
Factory/industrial site	3
Residential neighbourhood entrance	2
Gated neighbourhood	4
(Private) Security estate	1

On private residential property	1
On public streets	5
Along highways	3

The above table and graph show that public streets and residential areas have the largest proportion of installations (18%), followed by CBDs (15%).

Figure 1.6: Where CCTV installed in neighbourhood/residential area

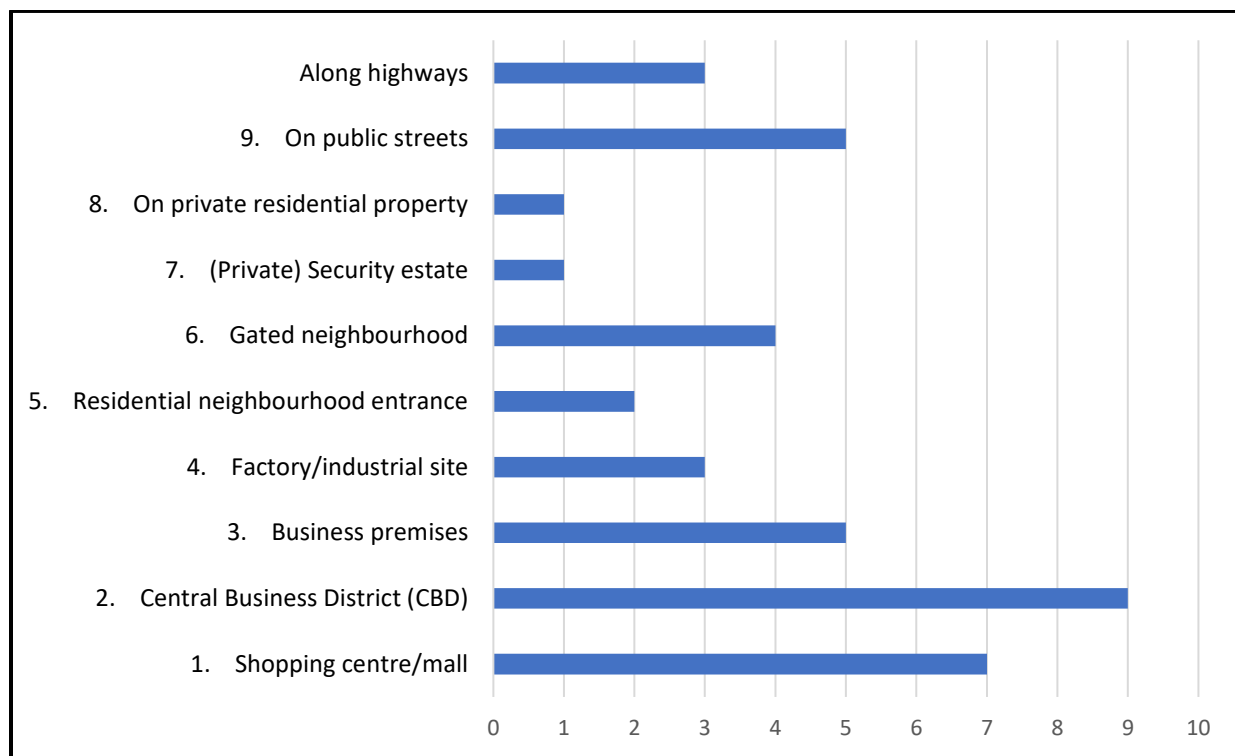


Table 4.17 and Figure 4.7 display the findings of the statistical analysis of areas with CCTV installations in CPF/residents interviewee areas with the highest being in local CBDs, (22.5%); followed by shopping centres/malls (17.5%). This suggests that such places are saturated by cameras. This is slightly different as indicated in the interviews with CCTV operators, which data indicated that: public streets and residential areas had the largest proportion of installations (18%); followed by CBDs (15%) (see Table 4.6 above).

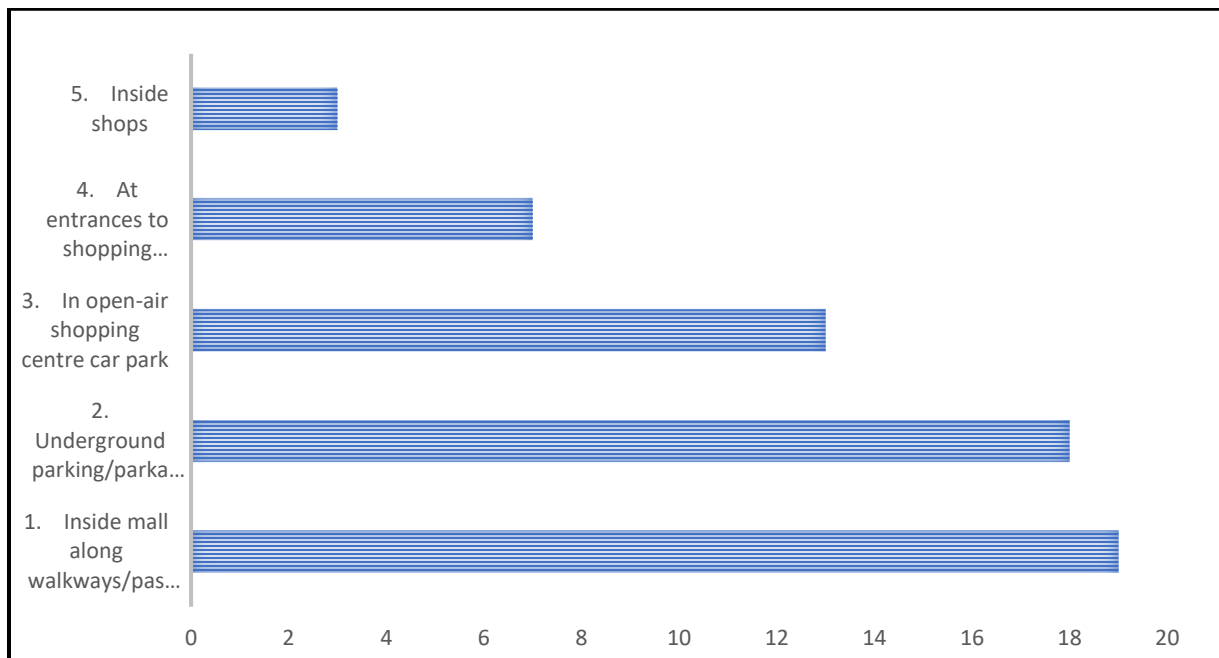
The information from Table 4.17 and Figure 4.7, was further expanded with site specific information (as presented below).

Shopping centre/mall

Table 1.21: Shopping centre/mall

Shopping centre/mall	(X)
Inside mall along walkways/passages	19
Underground parking/parkade	18
In open-air shopping centre car park	13
At entrances to shopping centre	7
Inside shops	3

Figure 1.7: Shopping centre/mall



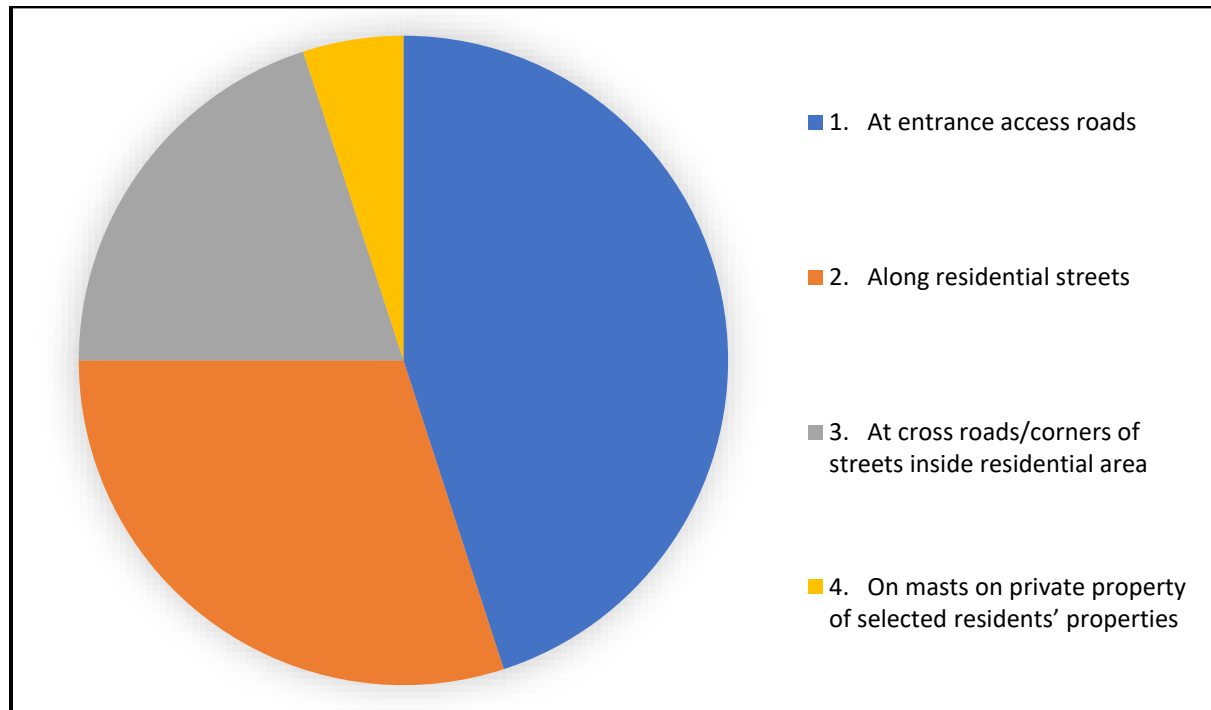
All areas in which CCTVs are installed, as indicated in Table 4.18 and Figure 4.7, with (in order of priority) the top three sites for CCTV camera installations being: i) inside malls along walkways/passages; ii) underground parking/parkades; and iii) in open-air shopping centre car parks.

Residential neighbourhoods

Table 1.22: Residential neighbourhoods

Residential neighbourhood	(X)
At entrance access roads	27
Along residential streets	18
At crossroads/corners of streets inside residential area	12
On masts on private property of selected residents' properties	3

Figure 1.8: Residential neighbourhood



The above diagram indicates places where CCTVs are installed in residential areas with 45 percent indicating “at entrance to access roads”; followed by 30 percent “along residential streets. It suggests that CCTV cameras are mounted at entrances to monitor all people entering respective places, for sake of footage.

Central Business Districts (CBDs)

Table 1.23: Central business districts

Central Business District (CBD)	(X)
On street corner mast	39
Along pedestrian walkways	11
Mounted on selected buildings	7
Along pedestrian walkways	11
Inside buildings	3

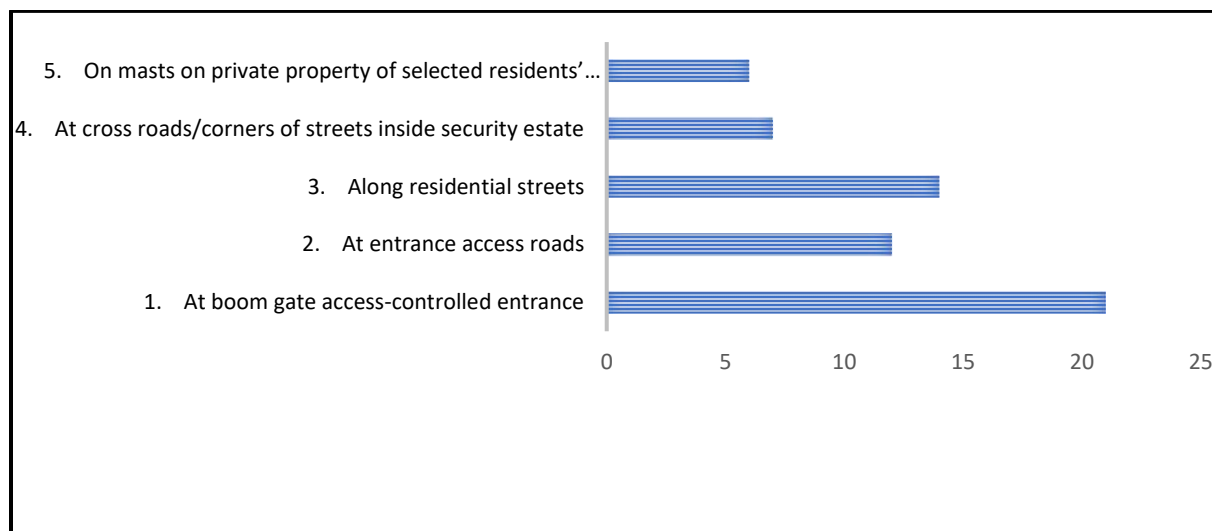
With respect to the central business districts research question, results also showed many cameras mounted on street corners than any other places as shown in Table 4.20 and effects of open-street CCTV, depending on location characteristics, on specific crime types. In particular, CCTV had significant reduction effects on assault, robbery, and burglary in residential areas, but it did not have significant reduction effects on auto theft and theft from auto in any location type. Location base rates of crime, however, were critical to the effectiveness of CCTV for assault, robbery, burglary, and theft from auto. For each of these crime types, CCTV effects were lessened as a location’s base rate of crime increased.

Gated neighbourhoods

Table 1.24: Gated neighbourhoods

Gated neighbourhood	(X)
At boom gate access-controlled entrance	21
At entrance access roads	12
Along residential streets	14
At crossroads/corners of streets inside security estate	7
On masts on private property of selected residents' properties	6

Figure 1.9: Gated Neighbourhoods



As the diagram above points out, CCTV installations are mounted at boom gate entrances to gated neighbourhoods (35%); followed by along residential roads (23%) in the vicinity; and at the entrance to access roads to the neighbourhood (20%). Offenders use these entrances when entering a neighbourhood when committing crime and therefore it is necessary that at gated neighbourhoods and boomgates, cameras should be mounted.

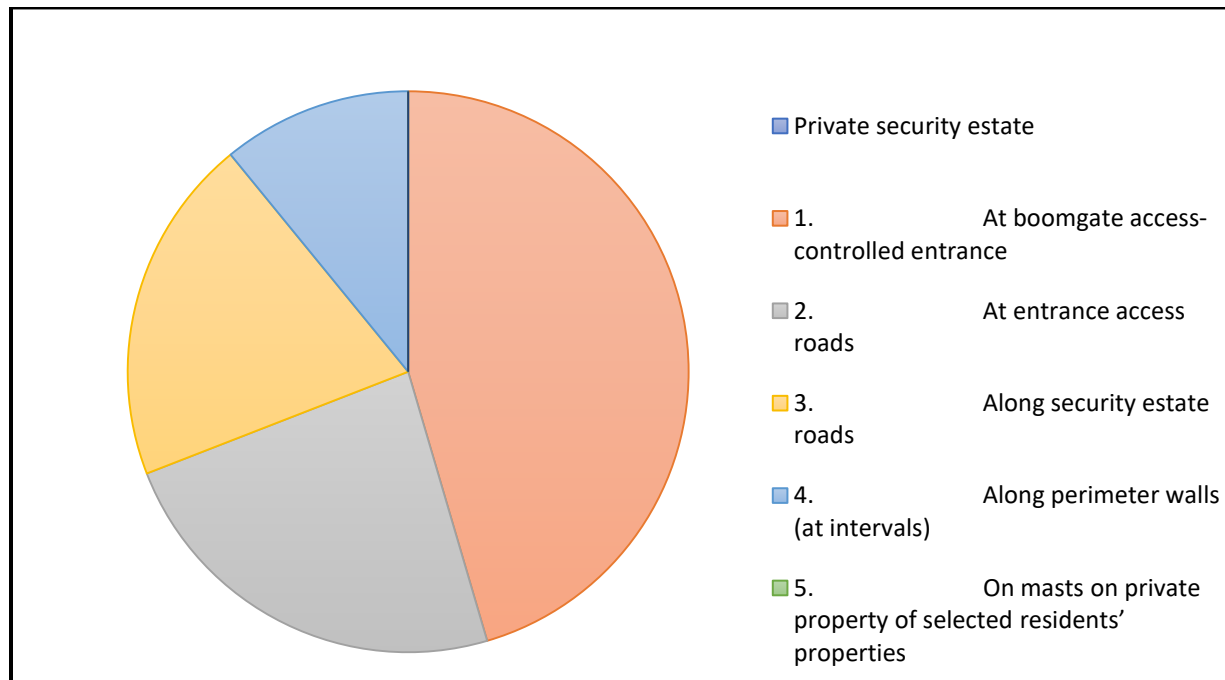
Private security estate

Table 1.25: Private security estate

Private security estate	(X)
At boom gate access-controlled entrance	25
At entrance access roads	13
Along security estate roads	11
Along perimeter walls (at intervals)	6
On masts on private property of selected residents' properties	5

Table 4.22 above and Figure 4.10 below illustrate the differences between various categories of CCTV installation at various places as indicated in the tables.

Figure 1.10: Private security estate



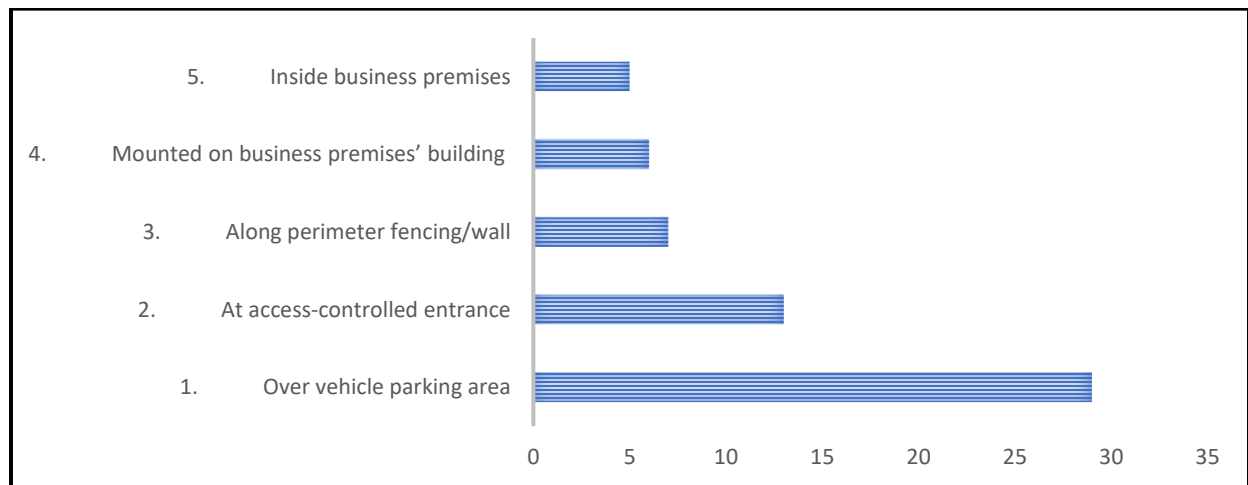
As the diagram above shows, the largest number of CCTV installations at private security estates are mounted at boom gate entrances (42%); followed by entrance access roads (22%); and along security estate streets/roads (18%).

Business premises

Table 1.26: Business premises

Business premises	(X)
Over vehicle parking area	29
At access-controlled entrance	13
Along perimeter fencing/wall	7
Mounted on business premises' building	6
Inside business premises	5

Figure 1.11: Business premises



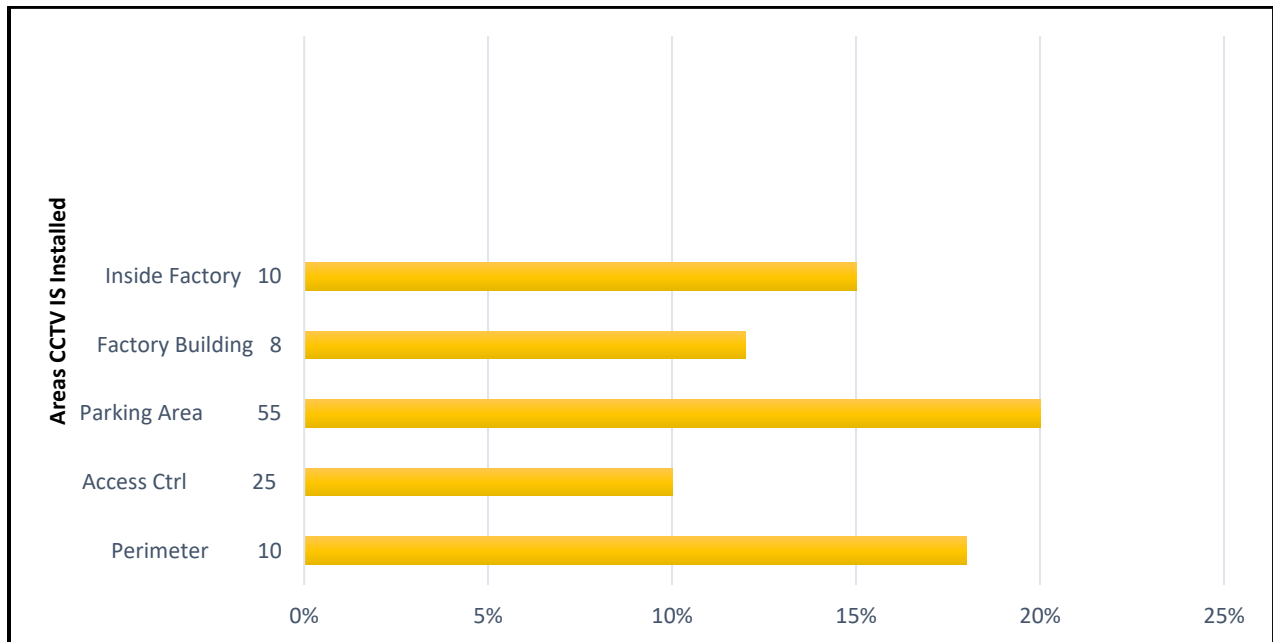
At business premises, most of the CCTV installations are found at the vehicle parking areas (48%); followed by 22 percent at the access-controlled entrances. The reason for installation at business premises is that, these areas are targeted by criminals and CCTV surveillance system is used as situation crime prevention strategy.

Factory/industrial site

Table 1.27: Factory/industrial site

Factory/industrial site	(X)
Over vehicle parking area	34
At access-controlled entrance	14
Along perimeter fencing/wall	6
Mounted on factory building	3
Inside factory building	3

Figure 1.12: Factory/industrial site



The bar graph above displays the percentages of CCTV installed at specific at a point in time. The reflection above shows the highest of CCTV is found at parking areas, followed by access control areas. This reflects that, these areas are prioritised because of the criminal activities at the spots. Similarly, to business premises, at

factory/industrial sites, 15 percent indicated that the CCTV cameras are installed in the site's parking areas followed by 23 percent at the access-controlled entrances.

Analysis

To the question: If "public space" (streets/entrance to neighbourhood) (as opposed to private/business/commercial property) has been indicated above what was the motivation/reason provided for its (CCTV Camera Surveillance System) installation in such public areas?

A selection of responses to this question are presented below:

"For crime prevention and control" (Interviewee D10, 2018).

"I conceptualise open-street CCTV as a regulatory project which is generated as an emotive response to socially constructed 'deviant populations' in the city" (Interviewee D11, 2018).

"The perception of cities as breeding grounds for deviance often deters investment, and the implementation of CCTV is used as revitalising tool to attract back investors into cities" (Interviewee D12, 2018).

"The motivation behind implementing the open-street CCTV schema is to deter vandalism occurring in the downtown core and apprehend offenders culpable of mischievous actions" (Interviewee D13, 2018).

"Cameras record live feeds continuously, and are often viewed by local police in order to apprehend or charge offenders" (Interviewee D14, 2018)

"Anti-crime police services have no comprehensive plan for dealing with [crime] displacement, and no public consultations were held before the issue went to city council to be ratified" (Interviewee D15, 2018).

The example of “anti-crime” or crime-prevention initiatives suggests that it is not simply metropolitan areas with large, visible, underclass populations who are turning to CCTV as a “silver bullet” to police perceptions of disorder, but that camera surveillance, as a form of governance, is diffusing into smaller, rural communities (Norris & Armstrong, 1999: 12):

“The scope of open-street CCTV in cities is growing, and there is little indication that this trend will reverse” (Interviewee D16, 2018).

“The objective of the CCTV project was to deter crime, vandalism, and rowdyism on Jeppe Street in downtown” (Interviewee D17, 2018).

“The initiative had the unanimous support of local companies which indicates that CCTV in Johannesburg and Pretoria was generated from both the level of police and the level of business” (Interviewee D18, 2018).

The above resonates and corroborates the theory behind using CCTV in crime fighting by police and private citizens as summarised by Armitage (2002: 34).

Although rarely addressed in the research literature, there is also the distinct possibility that if offenders are aware and cautious in the presence of cameras, they may be unaware of the extent of the cameras’ capabilities. As a result, they may curtail their criminal activity in a wider area than that covered by the camera system. In effect, this extends the value of the cameras beyond their area of operation; process criminologists call a *diffusion of benefits*.

Cameras can also be used to gather intelligence and to monitor the behaviour of known offenders in public places (such as shoplifters in public retail areas). Camera operators often come to know the faces of local offenders, and the cameras become a way to monitor their movements in a less intrusive manner than deploying

plainclothes police officers. For example, officers in one city were able to gather intelligence on the behaviour of individuals selling stolen goods. This intelligence was gathered remotely by CCTV cameras and enabled police to interdict in an organized and coordinated manner. Although intelligence gathering is a potential benefit of CCTV, the use of intelligence gathered from CCTV to control public order through surveillance is perceived by some to be a threat to civil liberties. CCTV can be used for general location management. The cameras can be used to look for lost children, to monitor traffic flow, public meetings, or demonstrations that may require additional police resources, or to determine if alarms have been activated unnecessarily thus removing the need for a police response. Brown (1995: 35) reports that some police commanders claim that assaults on police have reduced because the cameras allow them to determine the appropriate level of response to an incident, either by sending more officers to large fights, or by limiting the number of officers to a minor incident and avoid inflaming the situation. Camera footage can also help identify potential witnesses who might not otherwise come forward to police. CCTV camera evidence can be compelling, though issues of image quality are a factor if CCTV images are used for identification purposes. If the cameras record an incident, and police respond rapidly and make an arrest within view of the camera (and the offender does not leave the sight of the camera), the recording of the incident can help investigators gain a conviction, usually through a guilty plea. The potential to assist in police investigations may also drive offenders away from committing offences that take time, as they run a greater risk of capture.

In this section, a number of themes were revealed which are discussed below. However, the two major themes that emerged were the issues of support for CCTV installation in their area, and privacy.

The general argument is that the area will benefit from a positive economic impact when people feel safer. The findings are mixed but generally show there is some reduced level of fear of crime among people in CCTV areas, but only among people who were aware they were in an area under surveillance.

4.2.5 Support for CCTV

One of the principal aims of the study was to measure the level of support for the installation of CCTV cameras in residential areas amongst those individuals with no prior knowledge and experience of CCTV in their area.

The extent to which CCTV is perceived to be an invasion of privacy may influence the degree to which residents support such systems. Around 17 percent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy and this proportion varied between 12 percent and 23 percent across the nine target areas (see Interviewees A1, A2 & A3, 2018).

4.2.6 Issue of privacy

To the question: Do you have any concerns about issues of 'invasion of privacy' with the installation of CCTV cameras in your neighbourhood? – the following:

As in the case of support for CCTV, given that a low number of people that expressed the view that CCTV invades privacy, similar arguments apply to the comparison of these groups with other variables. Many participants understood there was an interest for extra security and surveillance systems crime prevention and control. However, find difficulties to continue sacrificing their privacy, human rights, and civil liberties.

Around 17 per cent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy, and this proportion varied between 12 per cent and 23 per cent across the nine target areas.

4.2.7 Analysis of the different survey samples

Analysis of the different survey samples showed an acceptable degree of similarity between the residential surveys on most socio-economic and demographic characteristics (CPFs communities). This similarity meant that the results from these could be meaningfully reported as a whole and levels of variation of the particular variable under consideration would be reported when necessary.

There are several possible explanations for the similarity, given that residential areas are not 'public space' in the same way as city centres. The areas in which the systems are installed tend to be highly localised. In most areas respondents have been consulted or informed about the proposed CCTV system prior to its installation. As was mentioned above, bids had to show evidence of this consultation process and to demonstrate support among residents. Of those supporting CCTV, 11 per cent felt that it was an invasion of privacy.

As in the case of support for CCTV, given that a low number of people expressed the view that CCTV invades privacy, similar arguments apply to the comparison of these groups with other variables. Both are discussed in more detail in later sections.

When was and where is CCTV surveillance systems installed in your area?

To the question of when the CCTV surveillance cameras were installed in the neighbourhood/residential area by month and/or year, most were unsure of exact dates and could not place a month or year date however very familiar with the presence of CCTV installation in their locality, As one participant put it: From the first question, which is asking the existence of CCTV cameras in various places, all the respondents noticed the presence of this system and they clearly indicates the places. It shows the CCTV system is not a new thing in Johannesburg/Tshwane. Then, 70 percent of respondents agreed the purposes of these cameras are for monitoring and security reasons, such as the following actions:

4.3 COMPARATIVE ANALYSIS

In this section, a number of themes were revealed which are discussed below. However, the two major themes that emerged were the issues of support for CCTV installation in their area, and privacy.

The general argument is that the area will benefit from a positive economic impact when people feel safer. The findings are mixed but generally show there is some

reduced level of fear of crime among people in CCTV areas, but only among people who were aware they were in an area under surveillance. One of the principal aims of the study was to measure the level of support for the installation of CCTV cameras in residential areas amongst those individuals with no prior knowledge and experience of CCTV in their area. The extent to which CCTV is perceived to be an invasion of privacy may influence the degree to which residents support such systems. Around 17 percent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy and this proportion varied between 12 percent and 23 percent across the nine target areas (see Interviewees A1, A2 & A3, 2018).

The question: Do you have any concerns about issues of 'invasion of privacy' with the installation of CCTV cameras in your neighbourhood? – the following:

As in the case of support for CCTV, given that a low number of people that expressed the view that CCTV invades privacy, similar arguments apply to the comparison of these groups with other variables.

Around 17 per cent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy, and this proportion varied between 12 per cent and 23 per cent across the nine target areas.

Analysis of the different survey samples showed an acceptable degree of similarity between the residential surveys on most socio-economic and demographic characteristics (CPFs communities). This similarity meant that the results from these could be meaningfully reported as a whole and levels of variation of the particular variable under consideration would be reported when necessary.

There are several possible explanations for the similarity, given that residential areas are not 'public space' in the same way as city centres. The areas in which the systems are installed tend to be highly localised. In most areas respondents have been

consulted or informed about the proposed CCTV system prior to its installation. As was mentioned above, bids had to show evidence of this consultation process and to demonstrate support among residents. Of those supporting CCTV, 11 per cent felt that it was an invasion of privacy.

4.3.1 Views about CCTV

Having described the characteristics and behaviour of the respondents, their views about CCTV are now assessed. They were asked several questions including whether cameras were already operating in the target area, their beliefs about the capabilities of CCTV cameras and systems, and their attitudes towards the installation of cameras.

When was and where is CCTV installed in your area?

To the question of when the CCTV surveillance cameras were installed in the neighbourhood/residential area by month and/or year, most were unsure of exact dates and could not place a month or year date. As one participant put it:

“Not sure, about two years ago” (Interviewee T2, 2018).

To the question: Were you in agreement with the decision to install? (CCTV cameras), the following:

To test all of the above questions the researcher relied on data from the interviews conducted with participants. The diverse array of views from the individuals interviewed in residential areas ran the gamut of views ranging from: those who not only feel safer in spaces where they know cameras are present, but who actively seek out such ‘safe’ spaces, to those who questioned the utility at all of CCTV surveillance systems.

Other participants advised that they actively sought out certain facilities because of the presence of cameras, meaning that they were not involved in the decisionmaking regarding the installation of CCTV in the first place.

What is seldom considered within the research literature is the possibility that CCTV may also lead to a sense of greater social inclusion for the citizen by affording them a measure of potential security (whether it be 'real' or 'perceived' security) and/or creating instances where the people who have been a victim of crime, may assert their right to access justice or be afforded equal treatment under the law.

To the question: *If yes, what were your primary reasons for wanting its installation?*

Support for the notion that public forms of CCTV provide an ontological security effect was not, however, universal across service providers or service users. Indeed, the majority of interviewees were positive about the possibility that public CCTV might prevent crime.

To the question: *If no, what were your reasons for not agreeing with installation?*

Privacy issues identified here: One of the most influential premises in Criminology is that crime rates decrease in correlation with an efficient control and crime prevention strategy. However, the implementation of an intensified surveillance as a generalized mechanism for controlling crime and deviance raises different conflicts in various fields of an individual's life and activities (Lyon, 2011:15). Such conflicts have been overlooked as long as security reasons are becoming more prevalent when balancing opposing interests (citizens' privacy or sex offenders reintegration versus community safety or the public interest) (Welsh & Farrington, 2009b:28). In this sense privacy continues to be at risk given that societies are preferably more inclined to choose security in the first place. One should ask before implementing a CCTV system about what kind of effects it will have on civil rights. CCTV has actually come to prominence at a time when privacy issues are at the forefront of public debate (Gill, 2006: 450). As Andrew von Hirsh has put it (2000): When CCTV is in operation there are collateral damages, for cameras recording people cannot discriminate between criminals and non-criminals (Gill: 61). That is to say, CCTV involves scrutinizing ordinary people's

comings and goings. Surveillance in public spaces may have a chilling effect on freedom of speech or assembly (Gill, 2006: 62).

To the question: *After installation of the CCTV system in your neighbourhood did you feel safer and more secure?*

Overall, the reported level of support for the installation of a new CCTV system was high, with almost 82 percent of participants either very happy (57.3%) or fairly happy (24.4%) with the prospect.

Below is a particularly revealing response to this question:

“CCTV is also good in detecting and prosecuting anyone carrying out crime. It can be effectively use in detecting crime if and only if the monitoring room is also at the same place. It is because, if anything wrong happen in the area under CCTV supervision, the personnel can immediately alert the person in charged in that area, so that crime can be stopped directly. In the case of prosecution, the recorded video of the CCTV can be used as evidence in court. Whoever is being caught with CCTV while doing crime, there are no other way out. Of course, the video must be tested for the originality beforehand” (Interviewee A12, 2018).

Overall there was a high level of support for the introduction of both new and additional cameras, with particularly high levels in Johannesburg CBD where approximately 94 per cent of all respondents indicated they would be happy to see cameras in the town centre. The extent to which respondents are informed about the capabilities of CCTV could impact upon their perceptions of how it works and whether it is likely to have an impact on crime and anti-social behaviour. Respondents were asked:

To the question: *To the best of your knowledge, did the installation of CCTV surveillance system lead to any direct successes against criminals?* The following information was provided by respondents.

The relatively vague response of 'making the respondent feel safer' was the most frequently given answer. In contrast, more specific answers describing how CCTV could work (e.g. to provide evidence, to provide surveillance and monitoring) were mentioned by no more than a fifth of the sample. Respondents in all areas supported the installation of CCTV, regardless of whether these were new or existing cameras systems. The most common reason given was that it would make respondents feel safer. Overall, respondents were clear about how they thought that CCTV would work.

4.3.2 Civil liberties

Having examined respondents' knowledge of CCTV, this question will consider their opinions of it. The first issue is the perceived threat to civil liberties. Unlike the introduction of CCTV cameras in obviously public spaces, such as shopping areas or car parks, their installation in residential areas raises a number of questions as to how they are viewed by local residents who live in the area as opposed to visiting it for short periods of time.

To the question: *Do you have any concerns about issues of 'invasion of privacy' with the installation of CCTV cameras in your neighbourhood?*

The extent to which CCTV is perceived to be an invasion of privacy may influence the degree to which residents support such systems. Around 17 per cent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy, and this proportion varied between 12 per cent and 23 per cent across the targeted areas. The belief that CCTV is an invasion of privacy is influenced by the socio-demographic characteristics of the respondent. Previous studies have found that younger men are more likely to feel that CCTV is an invasion of privacy (Ditton, 2000: 697). and this relationship holds for the current study.

Privacy is an often-mentioned topic in the literature related to any discussion of CCTV monitoring (Goold, 2007: 61-63; Lyon, 2002: 50; Schlosberg & Ozer, 2007: 23; Solove, 2011: 42). Solove (2011) writes that a common statement made when individuals

accept without question, some government or private entity gathering personal information is, “I’ve got nothing to hide” Solove, 2011: 21). The assumption by many is that you do not have to worry if you have done nothing wrong (Solove, 2011: 34). Privacy research conducted by Solove and supported by Goold (2007: 61-63), argues that privacy should be protected at all costs because the failure to protect personal information can “inhibit such lawful activities as free speech, free association, and other first amendment rights” (Solove, 2011: 4).

Respondents were also asked what they thought the installation of CCTV could potentially achieve. This was assessed by posing the following questions:

To the question: After installation did you notice a reduction in crime in your area? respondents were also asked three related questions, namely:

- What do you think are the crime reduction/prevention value/benefits of installed CCTV surveillance cameras? (If your opinion none indicate so as well);
- Can you think of any ways of improving the use and utilising of the installed CCTV surveillance cameras for crime reduction/prevention?

Respondents were positive that the CCTV system would address specific perceived problems i.e. criminal activity at their specific targeted areas. Approximately 80 per cent of the sample agreed that ‘with CCTV on the estate, the level of crime would get lower’. This perception was correlated with the scale comparing perceived capabilities of CCTV.

.

How best do you think can CCTV surveillance systems assist in solving crime?

Video footage is a form of real evidence – it is not the videotape itself that is evidence, but the images recorded on the tape. Video evidence must be authenticated in court (Palmer, 1998: 61), and authentication is usually provided either by the camera

operator or a system manager responsible for releasing the tape to the police as evidence. Some legal scholars have argued video images are potentially overly persuasive. Even where not directly tendered as evidence in court, it was argued video footage provided invaluable background information for prosecutors, allowing them to ask pertinent questions and assess the validity of various witnesses. Although there were occasionally problems with image clarity in videotape evidence, police generally believed CCTV footage was invaluable and that ‘a picture speaks a thousand words. Two related questions were posed to respondents.

To the question: *Were you in agreement with the decision to install?* – all respondents answered in the affirmative.

To the question: *What are your thoughts on CCTV as a tool for crime prevention and control?* – overall the participants tended to support the installation of cameras in their area, and in the case of seniors, almost unanimously so, while in approximately half of all cases of shelter residents. However, the researcher cannot be more specific, since several participants changed their minds during the interviews. Reasons for supporting cameras mirror many of those found in official discourse. Two assumptions prevail, the first of which is that CCTV surveillance effectively deters crime.

“Surveillance helps, let’s put it that way, it is a deterrent and it certainly helps. I don’t care what areas they are in: it helps” (Interviewee, A10, 2018).

“I don’t think it stops crime, I think it stirs them up and prevents accumulation of crimes in certain areas that are detrimental to the city’s growth and safety” (Interviewee A12, 2018).

To the question: *Which private security company manages/operates them?* – the following appeared to be the overall view on this question: Awareness of how and who does the monitoring of CCTV in their areas is equally low across all respondents.

Issues of uncertainty include who is responsible for monitoring, whether the cameras are recorded, and when the cameras are operational.

To the question on how CCTV surveillance fits into overall crime prevention initiatives, most participants indicated that:

Asking only for a general assessment of the efficiency of CCTV, the researcher tried to avoid preconditioning possible answers. However, many informants talked at their own initiative about issues, such as crime prevention and public safety. Twenty-seven of the respondents stated that crime prevention was an important aim of CCTV. All of them equated prevention with deterrence. Risk calculations, the consideration of costs and benefits and the assessment of a possible prevention or deterrence effect by CCTV are interdependent. Thirty-three interviewees mentioned the enhancement of feelings of safety as one of the aims of CCTV. Their assessments differed depending on, whether their own feelings of safety improved by CCTV or not. Many participants affirmed that their feelings of safety and security improved with the presence of cameras. The statements of these respondents indicated that the term 'feeling of safety' is used in subjective manner and a variety of ways. The mechanisms under which CCTV aims to reduce crime are based upon the following assumptions:

- Deterrence: The potential offender becomes aware of the presence of CCTV, assesses the risks of offending in this location to outweigh the benefits and chooses either not to offend or to offend elsewhere.
- Efficient deployment: CCTV cameras allow those monitoring the scene to determine whether police assistance is required. This ensures that police resources are called upon only when necessary.
- Presence of a 'capable guardian': The Routine Activity Theory (Cohen & Felson, 1979: 588-608) suggests that for a crime to be committed there must be a motivated offender, a suitable target and the absence of a capable guardian. Any

act that prevents the convergence of these elements will reduce the likelihood of a crime taking place. CCTV, as a capable guardian, may help to reduce crime.

- Detection: CCTV cameras capture images of offences taking place. In some cases, this may lead to punishment and the removal of the offenders' ability to offend (either due to incarceration, or increased monitoring and supervision). The latter mechanism is by far the most publicised, with few bank robbery cases, in which images of the offenders on CCTV aided their detection and subsequent arrest.

Regardless of the potential for a CCTV system to have a role in crime prevention, it can still contribute in a detection role. There are numerous examples of tapes aiding in an offender's conviction. Camera footage can also help identify witnesses who might not otherwise come forward to police. CCTV camera evidence be compelling, though issues of image quality are a factor if CCTV images are used rapidly and make an arrest within view of the camera (and the offender does not leave the sight of the camera), the recording of the incident can help investigators obtain a conviction, usually through a guilty plea. The potential to assist in police investigations may also drive offenders away from committing offences that take time, as they run a greater risk There are several possibilities which CCTV system can have an impact on car crime. The following factors are presented for consideration in this context:

- CCTV reduces car crime by making it more likely that present offenders will be caught, stopped, removed, punished and deterred.
- CCTV reduces car crime by deterring potential offenders who will not wish to risk apprehension and conviction by the evidence captured on videotape or observed by an operator on a screen on which their behaviour is shown.
- The presence of CCTV leads to increases in usage of car parks, because drivers feel less at risk of victimisation. Increased usage enhances natural surveillance,

which deters potential offenders, who feel they are at increased risk of apprehension in the course of criminal behaviour.

- CCTV allows for the effective deployment of security staff/police officers towards areas where suspicious behaviour is occurring. They then act as a visible presence deterring potential offenders. They may also apprehend actual offenders red handed and disable their criminal behaviour.
- The publicity given to CCTV and to its usage in catching offenders is received by potential offenders who avoid the increased risk they believe to be associated with committing car crimes in car parks. The perceived risks of offending exceed the perceived benefits and offending either ceases or is displaced by place or offence.
- CCTV and signs indicating that it is in operation symbolise efforts to take crime seriously and to reduce it. The potential offender perceives crime to be more difficult or risky and is deterred.
- Those car crimes which can be executed in a very short space of time will be less reduced than those which take more time, as the offender calculates the time taken for police or security officers to come or the probability that panning cameras will focus in on him/her.

To the question: *How best do you think can CCTV surveillance systems assist in solving crime?* The following themes emerged from the responses received from participants:

4.3.3 Information gathering

The responses from participants regarding the value of CCTV is replicated in the literature and articulated by Armitage et al (1999: 78), which has been described as follows:

- *'Caught in the act'*: perpetrators will be detected, and possibly removed or deterred.
- *'You have been framed'*: CCTV deters potential offenders who perceive an elevated risk of apprehension.
- *'Nosy parker'*: CCTV may lead more people to feel able to frequent the surveilled places. This will increase the extent of natural surveillance by newcomers, which may deter potential offenders.
- **Effective deployment**: CCTV directs security personnel to ambiguous situations, which may head off their translation into crime.
- **Publicity**: CCTV could symbolize efforts to take crime seriously, and the perception of those efforts may both energize law-abiding citizens and/or deter crime.
- **Time for crime**: CCTV may be perceived as reducing the time available to commit crime, preventing those crimes that require extended time and effort.
- **Memory jogging**: the presence of CCTV may induce people to take elementary security precautions, such as locking their car, by jogging their memory.
- **Anticipated shaming**: the presence of CCTV may induce people to take elementary security precautions, for fear that they will be shamed by being shown on CCTV.

- Appeal to the cautious: cautious people migrate to the areas with CCTV to shop, leave their cars, and so on. Their caution and security mindedness reduce the risk.
- Reporting changes: people report (and/or police record) fewer of the crimes that occur, either because they wish to show the desirable effects of CCTV or out of a belief that: 'the City Council is doing its best', and nothing should be done to discourage it.
- Cameras can also be used to gather intelligence and to monitor the behaviour of known offenders in public places (such as shoplifters in public retail areas). Camera operators often come to know the faces of local offenders, and the cameras become a way to monitor their movements in a less intrusive manner than deploying plainclothes police officers. For example, officers in one city were able to gather intelligence on the behaviour of individuals selling stolen goods. This intelligence was gathered remotely by CCTV cameras and enabled police to interdict in an organised and coordinated manner (Welsh et al, 2008: 37).

The findings reveal that the majority of people questioned thought that the most important reason to install these cameras was to make people feel safe and put catching people who commit a crime as the most important, regarded the deterrence factor as the most important and. thought that these cameras were installed to spy on people. This is consistent with public CCTV schemes that are frequently installed to reassure the public that crime is being prevented (McCahill & Norris, 2002: 23 & 56; Gill & Spriggs, 2005: 18 & 20); Ratcliffe, 2006: 45 & 65). In any situation monitored by the CCTV operators, which will potential result in the commission (trigger) of a crime, they will ask the nearest Mobile Patrol Vehicle (MPV) to rush to the identified place immediately. The CCTV operators are private security officers who have already been taught on how to operate the system by security colleges but with standard operating procedures (SOP) mainly for the system. From the literature consulted (above listed),

it is clear that CCTV surveillance systems by design can be an effective tool in overall crime prevention initiatives. However, the system cannot be a 'stand-alone' one but must be supported by other elements, such as police action. Furthermore, there must be rules and regulations, policies and guidelines to follow by the enforcers and also by the public.

To the question: If "public space" (streets/entrance to neighbourhood) (as opposed to private/business/commercial property) has been indicated above what was the motivation/reason provided for its (CCTV Camera Surveillance System) installation in such public areas? Public areas / residential areas, these are target areas for criminals to commit criminal activity/ social disorder. CCTV surveillance systems as alluded earlier is used as a situational crime prevention strategy (SCP). SCP seeks to influence the offender's decision or ability to commit crimes at particular places and times by way of particularly designed measures. Situational prevention comprises a range of measures that highlight the importance of targeting very specific forms of crime in certain circumstances (Clarke 1997: 78). This involves identifying, manipulating and controlling the situational or environmental factors associated with certain types of crime (. It is also based upon assumptions regarding the nature of offending and of offenders (Cornish & Clarke, 2003: 60). Underlying the situational approach are four key elements, including:

- increasing the effort involved in offending;
- increasing the risk associated with offending;
- reducing the rewards that come from committing a crime;
- reducing situational factors that influence the propensity of an individual to offend; and
- removing excuses for offending behaviour (Cornish & Clarke, 2003: 60).

4.3.4 Residents' attitudes towards CCTV

In this section of this chapter residents' attitudes towards CCTV and their beliefs about how CCTV works was described. It provides new insights into the views of those living in residential areas where CCTV is to be installed. The following aspects were found:

- Eighty-two per cent were happy or very happy with the installation of CCTV, which is similar to the level of support found in face-to-face interviews with CCTV Operators and CPFs members.
- Those who had been victimised and who felt unsafe were significantly more likely to support CCTV although absolute differences were very small.

Individuals appeared confused about the capabilities of CCTV. However, this did not deter them in their support for CCTV and their perceptions as to what they thought CCTV could do. Approximately 80 per cent of the sample agreed that with CCTV on the estate, the level of crime would get lower. Sixty-three per cent were positive CCTV would reduce the number of people hanging around; 80 per cent thought that crime would be minimised or reduced; 68 per cent believed people would report more incidents; 56 per cent that the police would respond more quickly as a result of the cameras being installed. In this section, a number of themes were revealed which are discussed below. However, the two major themes that emerged were the issues of support for CCTV installation in their area, and privacy. The general argument is that the area will benefit from a positive economic impact when people feel safer. The findings are mixed but generally show there is some reduced level of fear of crime among people in CCTV areas, but only among people who were aware they were in an area under surveillance. One of the principal aims of the study was to measure the level of support for the installation of CCTV cameras in residential areas amongst those individuals with no prior knowledge and experience of CCTV in their area. CCTV in other public settings such as city and town centres, public housing communities, and transportation facilities evokes more resistance on the basis of threats to privacy and other civil liberties, and is associated with a larger number of social harms,

including the reinforcement of the notion of a fortress society and the social exclusion of marginalised populations (Lyon, 2011:34). Indeed, it is often these settings that are at the center of the debate over how best to strike a balance between the potential crime reduction benefits and social costs associated with CCTV.

The extent to which CCTV is perceived to be an invasion of privacy may influence the degree to which residents support such systems. Around 17 percent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy and this proportion varied between 12 percent and 23 percent across the nine target areas (see Interviewees A1, A2 & A3, 2018).

To the question: Do you have any concerns about issues of 'invasion of privacy' with the installation of CCTV cameras in your neighbourhood? – the following:

As in the case of support for CCTV, given that a low number of people that expressed the view that CCTV invades privacy, similar arguments apply to the comparison of these groups with other variables.

Around 17 per cent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy, and this proportion varied between 12 per cent and 23 per cent across the nine target areas.

Analysis of the different survey samples showed an acceptable degree of similarity between the residential surveys on most socio-economic and demographic characteristics (CPFs communities). This similarity meant that the results from these could be meaningfully reported as a whole and levels of variation of the particular variable under consideration would be reported when necessary.

There are several possible explanations for the similarity, given that residential areas are not 'public space' in the same way as city centres. The areas in which the systems are installed tend to be highly localised. In most areas respondents have been

consulted or informed about the proposed CCTV system prior to its installation. As was mentioned above, bids had to show evidence of this consultation process and to demonstrate support among residents. Of those supporting CCTV, 11 per cent felt that it was an invasion of privacy.

One of the IT applications in policing has been CCTV. Police departments had started to use CCTV systems in the early 1990s (Armitage, 2002: 34). As surveillance technology, CCTV assist police in order to provide social control and maintain order, prevent and catch criminals (Goold, 2006: 17; Kruegle, 2007: 45). CCTV cameras have been commonly used in order to decrease crimes, such as theft, crimes against personnel and assets and terrorism (Kruegle, 2007: 45). Specifically, 9/11 terrorist attacks have forced governments to invest in surveillance technology in order to protect their citizens against such dreadful attacks. In order to prevent future similar attacks, law enforcement agencies have started to extensively use surveillance systems, especially CCTV, to monitor human activities at airports, seaports, borders, and crowded city streets (Goold, 2006: 5).

As the use of CCTV in South Africa grows, companies are faced with difficult choices in terms of what they can and cannot legally do with their cameras and the footage they take. When is your footage admissible in court, when will it be deemed illegal? A security policy is the essential basis on which an effective and comprehensive security program can be developed. The importance of this critical component of the overall security system, however, is often overlooked. A security policy is the primary way in which management's expectations for security are translated into specific and measurable goals and objectives. It is crucial to take a top down approach based on a well-stated policy in order to develop an effective security system. On the contrary, if there is not a security policy defining and communicating those decisions, then they will be made by the individuals designing, installing and maintaining security systems. This will result in a disparate and less than optimal security system being implemented.

4.4 DATA ANALYSIS AND DISCUSSION: STREET SURVEY QUESTIONNAIRE (ANNEXURE I)

The street survey questionnaire was designed in three sections, namely:

- personal information including, race, gender and profession;
- experience of CCTV surveillance systems; and
- questions related to operations of CCTV in their areas (or of where they were responding to the survey questions).

The survey questionnaire was used to help the researcher to collect additional information and public perceptions/opinions about CCTV in order to complete the study of evaluating the use of CCTV surveillance cameras for crime control and prevention.

The Street Survey Questionnaire was administered to 50 respondents stopped randomly with the request to voluntarily answer the survey questions in public streets in and around the Johannesburg Central CBD (that included Rivonia, Joubert, Alice, 5th Street, Pybus, Wolmarans, Melle, Biccard and Jeppe) and the Sandton CBD. In the Pretoria Central CBD (mainly in the Sammy Marks Square and Church Square bounded by Mandela Drive, Bosman, Bloed and Church Streets). These areas have had CCTV cameras installed on streetlight poles and selected high buildings for many years. A total of 50 participants were evenly split (25/25) between Johannesburg and Pretoria.

During the surveys, participants were informed about the process as much as possible to help them understand the survey focus, to give them a sense of control, and to allow them to make an informed decision to continue with participating in the survey. The results confirmed that survey participants experienced the use of CCTV operation in their daily lives.

To address the research questions in more detail, several areas related to crime prevention and control were identified for the survey. Note that some of the tables below have condensed categories. This was done to indicate that categories which were sparsely populated were combined to ensure that the analysis of the effect of these category properties related to perceptions of CCTV investigated in the overall analyses and led to unbiased results.

Gender

Table 1.28: Gender

Male	35
Female	15

Figure 1.13: Gender composition of respondents

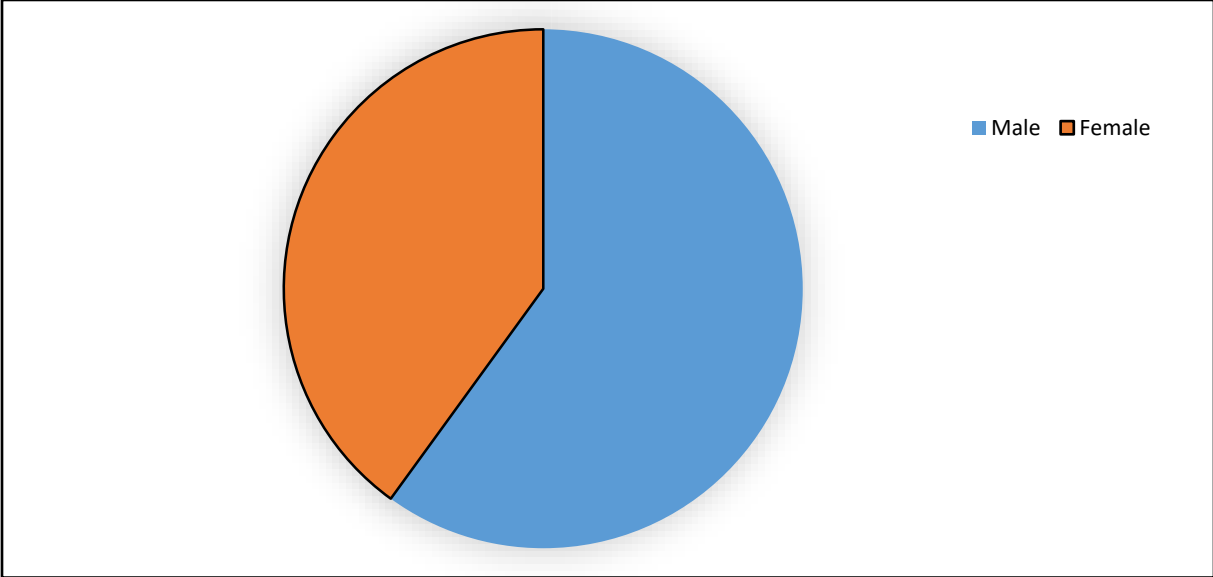
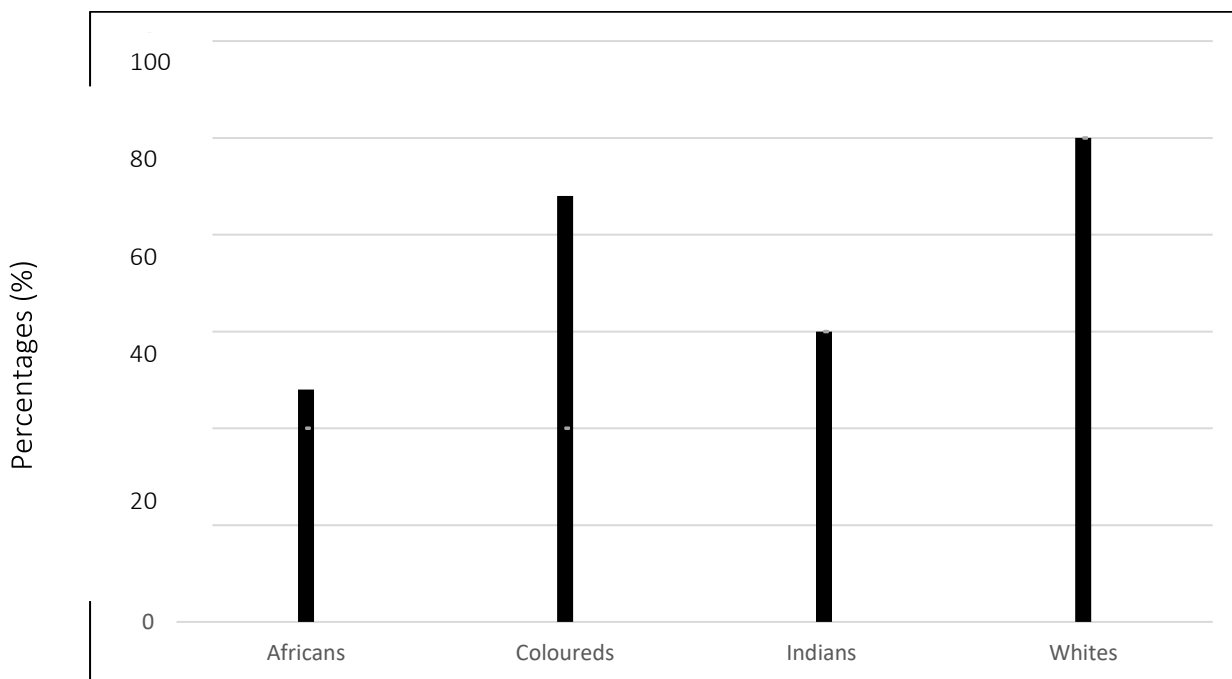


Table 1.20 and Figure 4.20 indicate that the majority of the sampled 50 respondents, sixty percent were male and 40 percent were female.

Table 1.29: Race composition of respondents

African	10
Whites	14
Coloured	12
Indian	14

Figure 1.14: Race composition of respondents



Comparisons of these racial groups' attitudes towards CCTV surveillance systems based on their ethnicity was not done.

To the question: *What value do you think CCTV surveillance operations can provide to crime prevention initiatives in local areas?* – the following data from the responses, namely: 51.6 percent thought they were very effective; 41.6 percent thought they were reasonably effective; 6.8% thought they were reasonably ineffective. This is displayed in the bar graph below:

Figure 1.15: Effectiveness of CCTV

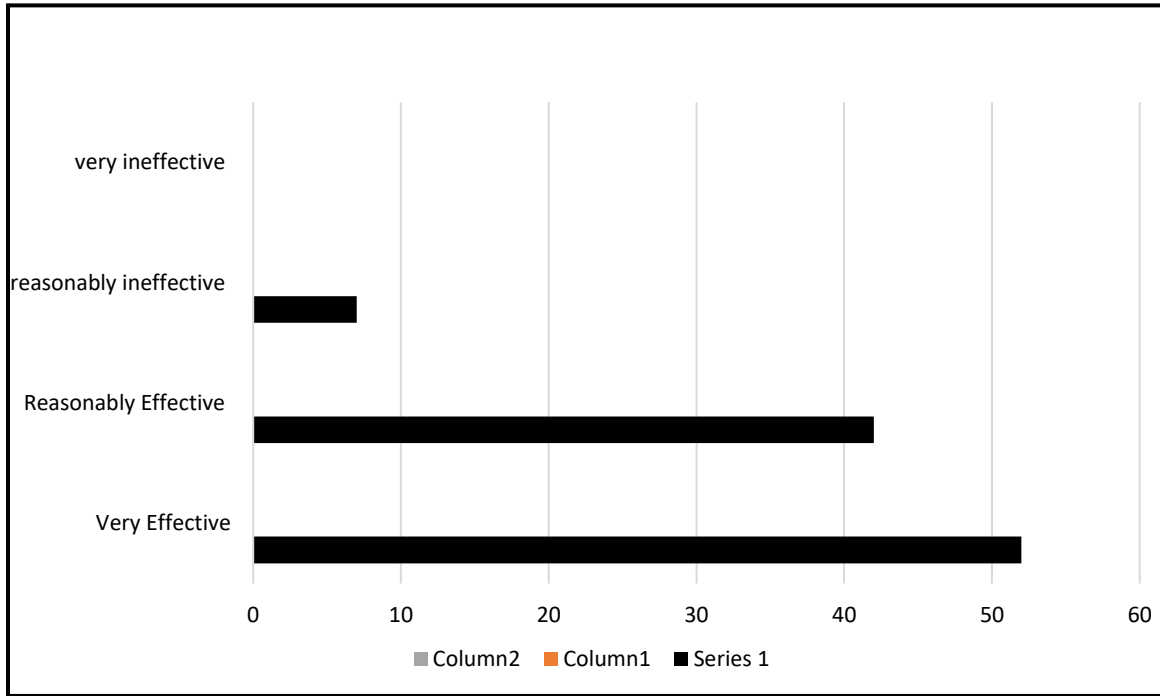
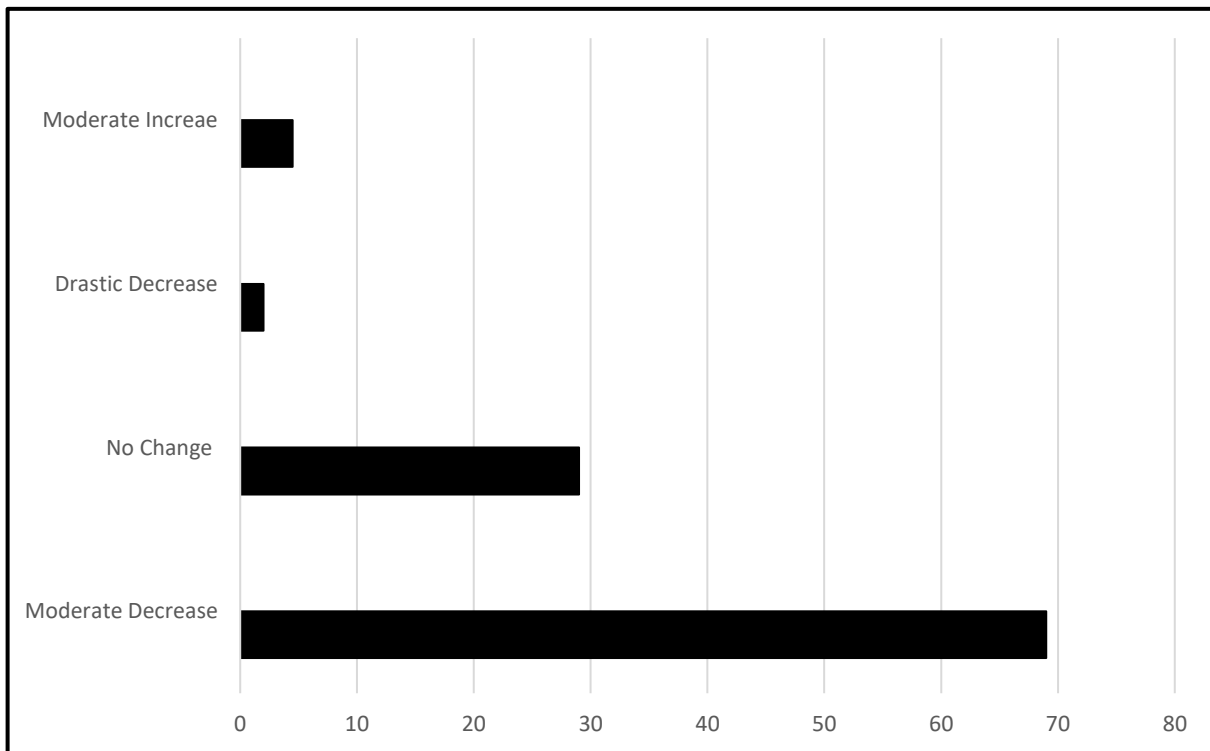


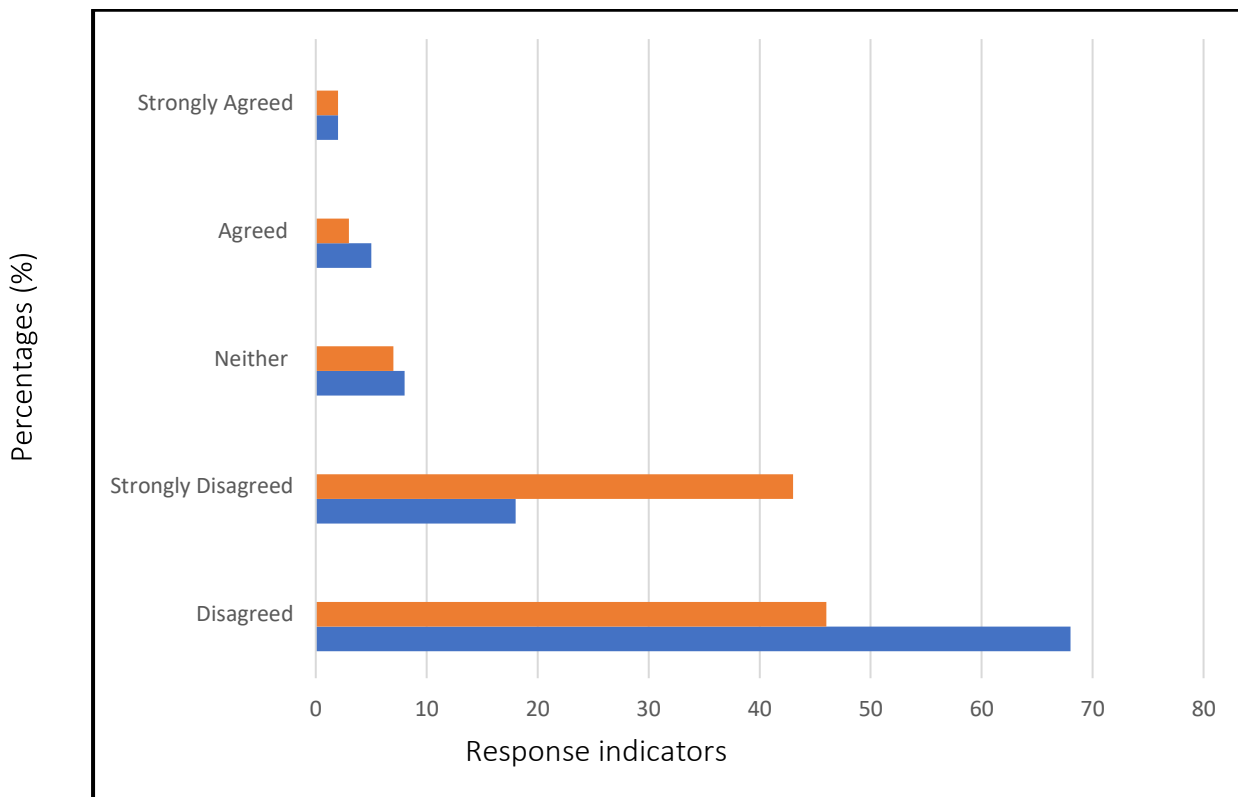
Figure 1.16: Impact on crime levels



Of the respondents, 68.9% thought there was a moderate decrease, 29.3% thought there was no change, 1.2% thought there was a drastic decrease and 0.6% thought there was a moderate increase.

To the question: *Do you have any concerns about issues of 'invasion of privacy' with the installation of CCTV cameras in your neighbourhoods?*

Figure 1.17: Privacy issues



Of the respondents, 67 percent disagreed; 18 percent strongly disagreed; eight percent neither agreed nor disagreed; five percent agreed; while almost two percent strongly agreed.

4.4.1 Analysis of street survey questionnaires

The extent to which CCTV is perceived to be an invasion of privacy may influence the degree to which residents support such systems. Around 17 per cent of all respondents either agreed or strongly agreed that the introduction of CCTV would be an invasion of people's privacy, and this proportion varied between 12 per cent and 23 per cent across the target areas. The belief that CCTV is an invasion of privacy is influenced by the socio-demographic characteristics of the respondent. Previous studies have found that younger men are more likely to feel that CCTV is an invasion of privacy (Ditton 2000: 710) and this relationship holds for the current study. There are several possible explanations for the similarity, given that residential areas are not 'public space' in the same way as city centres. As in the case of support for CCTV, given that there is a low number of people expressing the view that CCTV invades privacy, similar arguments apply to the comparison of these groups with other variables. Statistical differences can be found, though they do not correspond to large numbers of people in the sample. installed tend to be highly localised. In most areas respondents have been consulted or informed about the proposed CCTV system prior to its installation. As was mentioned above, bids had to show evidence of this consultation process and to demonstrate support among residents. Of those supporting CCTV, 11 per cent felt that it was an invasion of privacy. Respondents were generally of the opinion that their area was safe (70.97%), that crime has decreased over the past five years (67.74+13.13%) and that statistics were fairly to definitely in touch with public opinion

The respondents were asked whether they were aware of the CCTV installed in the area where they were being questioned.

Of the respondents, 82 percent stated that they knew the location of cameras; and ten percent did not know.

Asked if they would support further installations: eight percent stated that they would not support the installation of additional cameras.

4.4.2 Deductions

From the data of the street survey: in general, respondents believed CCTV surveillance systems had at least a slight crime deterrence effect. This was statistically significant with stronger support on the issues of:

- crimes against public administration;
- state and administration of justice;
- crimes impacting on freedom of movement (i.e. feelings of being safe but crimes that impact on walking around) than crimes against property.

Overall, results from the analysis suggest that the introduction of the cameras were associated with a reduction in all crime in the target areas surrounding CCTV installation sites. The most common reason given for the installation of CCTV in town centres is to combat what is loosely defined as “anti-social behaviour” (also known as “disorder offenses” or “petty” street crime).

This reduction was largely due to a decline in petty street crime offences, since the frequency of serious crimes around each camera location in the two CBDs was generally too low to detect a measurable impact on serious crime alone. A further cause of the low number of serious offences within the radius view of each camera was that most often serious crimes, such as murder, occur inside buildings or in areas not clearly viewed (videoed) by CCTV cameras (Leggett, 2004: 72).

Farrington (2009: 45) supports the idea that CCTV can be most effective at preventing certain types of crime at certain types of places (e.g. open car parks (not under cover). Crimes that occur in public on streets should therefore be subject to some deterrent effects of CCTV cameras in place.

Generally, most responses were similar in nature for the more specific questions. All the participants said that they thought that CCTV had had a positive impact on reducing crime in the CBD area (where the survey was conducted).

More than 50 percent of the respondents agreed on the usage of CCTV for crime prevention and control as one participant said: "*Crime prevention and control*" (Respondent T2, 2018).

To the question: "In the last two years have you been a victim of crime (personally experienced a crime situation) in this CBD/public street area?", all of the participants answered "yes". Even though fear of crime is a debatable concept in the criminal justice literature, there is no consensus about the definition and how to measure the construct. Studies on the link between crime and fear use unidimensional definitions of the concepts and generally do not differentiate between types of crime and kinds of fear (Norris & Armstrong, 1999: 12).

To the question: Knowing there is a CCTV surveillance system in this CBD/public street area, do you feel safer when coming into this CBD/city centre/public street area? The majority said "yes" they felt safer coming to the area during the daytime but "no" to at night (i.e. they seldom, if ever, came into the area at night). Those who said "yes" were asked whether CCTV had "come to your aid/assistance or was of any help". Many answered no and, when asked for a reason, one response was: "*Didn't come to my assistance... [it was] out of order*" (Respondent T3, 2018).

There is an extensive literature on fear of crime and the underlying theories of fear of crime can be grouped in three different camps Karakus et al (2010: 175): the victimization model, disorder model and community concern/social control model. According to the proponents of the victimisation model, fear of crime is caused by the actual crime rates in the community or individuals hearing about crime happening around them. Studies on disorder model argue that physical and spatial disorder and incivility in the neighborhood make people unsafe and they begin to think about being victim of crime. Individuals see the physical and structural decay in the neighborhood as the signals of crime and they become frightened. Related to the disorder model, community concern/social control model explains the fear of crime as a result of

deterioration in the social fabric of community. When social control tools are eroded and members of community start to have loose neighborhood relationship. However, there are some other feelings, such as anxiety, worry or concern about crime which are related to fear but the distinction between these feelings have not been resolved in the literature as yet (Gray, Jackson & Farrall, 2011: 67). Another important aspect of CCTV is that law enforcement officials are quickly deployed to the incident scene and investigations are conducted according to the data recorded by the system (Brown, 1995: 48-50). The theory behind using CCTV in crime fighting by the police is precisely summarised by Armitage (2002: 56). These are deterrence, efficient deployment, self-discipline, presence of a capable guardian, and detection. For the deterrence, if there is a camera in a place, a potential offender calculates the cost and benefit of committing a crime and decides not to commit or go to other suitable places. Secondly, CCTV system helps the police to deploy their human resources and other resources wisely by paying adequate attention on the right time to a spot when police assistance is needed. CCTV system also brings self-discipline not only to offenders, but also to victims. In the presence of CCTV cameras in place, victims become alert against crimes. Therefore, they try to reduce the risk of being a prey of a criminal by taking personal precautions against crimes. For the offenders, CCTV cameras give the sense of being watched all the time and they try to control their own behavior in order not to be caught in misbehavior. According to Routine Activity Theory presented by Cohen and Felson (1979: 588-608), there should be convergence in space and time of likely offenders, suitable targets, and the absence of capable guardians. CCTV cameras prevent the convergence of these three elements by providing a capable guardian all the time. Finally, CCTV cameras help the police to detect offenders by recording images of offences taking place. These records play important role in arresting, sentencing and incarcerating of the criminals. Thus, criminals are caught and cannot commit new crimes and the justice is served for the society. CCTV is also seen as a fear reduction strategy (Lee, 2007: 78) and offered as a capable guardian (Piza, 2014: 63). Nevertheless, the role of CCTV in reducing fear of crime is questionable (Smith, 2008: 12). Norris and Armstrong, (1999: 85) found that CCTV had a significant impact on reducing fear of crime in the boroughs of London. In addition,

some researchers did pre/post surveys to evaluate the level of fear of crime among public; they noted positive effect of CCTV on the reduction of fear of crime Phillips, (1999: 75). Furthermore, Brown (1995: 45) indicated that CCTV is an effective tool in reducing fear of crime among public in the case study of Birmingham, UK. On the other hand, Gill and Spriggs (2005) surveyed people to see the effect of CCTV on fear of crime. They found that even though there was a decrease in fear of crime in public when compared to before and after CCTV installation, this reduction could not be attributed to CCTV. Regarding our study, some scholars (Armitage, 2002: 90; Fletcher, 2011: 60) used RAT theory to explain the relationship between fear of crime and CCTV.

One of the reasons given for saying “not at nighttime” was:

“It’s Catch 22 situation given the challenges of load shedding [electricity blackouts by ESKOM], CCTV surveillance needs to be connected to a [constant] source of power to function” (Respondent T9, 2018).

However, when asked whether, in their experience, CCTV footage influence crime, one respondent said that in his personal experience it had as he Determine conviction or not based on footage evidence: *“opened a case after being mugged in CBD [at] Eloff Street, yes”* (Respondent K, 2018).

To the question: Who do you think funds the operations of this CBD/public street area CCTV surveillance system? The general response was along the lines of:

“Government agencies [such as the] SAPS and government authorities [town council/municipality]. In private sector it is funded by community associations” (Interviewee T20, 2018).

All respondents were in support of the extension of public CCTV camera installations to: i) Other CBDs in this metropolitan area and linked to a Central Control Room; ii)

the suburbs; and iii) the townships. The research about the benefit of CCTV systems in crime-fighting is incomplete, confusing, and inconsistent (Dempsey and Forst, 2012: 73). A group of researchers (Carli, 2009;70; Squires, 2003: 56; Phillips, 1999: 82) argue that CCTV systems are necessary tool for the police in decreasing crime rates, responding crimes in a timely manner and maintaining order and providing social control. On the contrary another group of researchers (Armitage, 2002: 64; Deisman, 2003: 51; Gill and Spriggs, (2005: 85) claim that there is no significant data proving the benefit of CCTV in crime fighting. According to Deisman (2003: 90), the effect of CCTV on crime is variable and unpredictable. The deterrence effects of CCTV also change according to type of a crime, location of a crime, and time of a crime. Similarly, Welsh and Farrington (2008: 15) did an extensive systematic review to assess the effects of closed-circuit television surveillance on crime. They concluded that CCTV has a modest but significant desirable effect on reducing crime in car parks, especially vehicle crimes and it is more effective in reducing crime in the U.K. than in other countries.

To the question whether they had any suggestions or recommendations for improving the current CCTV surveillance system in the CBD, one respondent answered:

“Most CCTV infrastructure is monitored by outsourced private security companies. This has created tension in the industry. These companies sometimes mistreat their employees, which later affect performance because they spend most their time resolving matters at CCMA”¹³ (Respondent WE34, 2018).

Another stated that:

“Certainly so, due to cost with the CCTV surveillance technology, some companies are still making use of analogue software with its limited capacities.

¹³ The Commission for Conciliation, Mediation and Arbitration (CCMA) is an independent dispute resolution body established in terms of the Labour Relations Act, 66 of 1995 (LRA).

Advise companies [that they] must migrate digital technology, it has better properties/features” (Respondent WQ7, 2018).

While the street survey responses were similar to some of the information obtained from the two sets of face-to-face interviews, some results were inconsistent with the findings of the qualitative research conducted in the period prior to the street surveys. Furthermore, the pragmatic use of these several sources of information for this research study by necessity triangulated the data, thereby building a coherent justification for the analytical framework (Creswell, 2003: 196). Besides, there is limited research about the role of CCTV in preventing ongoing criminal activity and arresting the suspects (Bekkers & Moody, 2011: 458-460). However, there is a majority support from public regarding deployment of CCTV cameras in the public places because CCTV increases safety feelings of citizens and decreases fear of crime and victimization. Even though there are some concerns about profiling and the breach of privacy (Lyon, 2011: 23), people generally support the use of security cameras in crime fighting. Armitage (2002: 70) reviews the studies about the evaluation of CCTV systems in the literature and concludes that there are several methodological problems in the studies due to several reasons. These are: inadequate pre and post CCTV time periods in which data are collected, no account taken of seasonal variations, no control areas for comparison, little discussion of displacement or diffusion of benefits, unspecified sample size, and lack of independent evaluation. Thus, there should be methodically sound empirical studies in the literature in order to know to what extent the surveillance plays role in crime prevention and crime reduction.

There are fears that CCTV surveillance may come increasingly to be seen as a method of controlling public order (Gill & Spriggs, 2005: 67). Such fears centre on the increasing sophistication of the technology coupled with the lack of a regulatory framework to monitor the collection, storage and use of information. Pattern recognition systems make it possible to match video images of a person's face with a computer database while communications and corroborative software facilitate both the sharing

and the centralisation of such data (Gill, 2006: 35). The coalescence of these technological threads enables the identification of an individual and the monitoring of that individual's activities on a scale only previously envisaged in the literature of science fiction. Both the police and many commercial organisations have an interest in pursuing the possibilities since potential applications range from the investigation of crime to sophisticated direct marketing techniques (Tilly, 1997: 45). Within the UK there is no law of privacy to prevent the abuse of CCTV surveillance and this in turn leads on to the second of the legal issues, namely: the legal regulation of CCTV (Pawson & Tilley, 1997: 45; Gill & Spriggs, 2005: 67; Gill & Turbin, 1998: 23, 1999: 32)

4.4.3 Street survey findings: Some conclusions

The extant literature raises a number of questions about the growth of CCTV computer enhanced surveillance technology. Referring to deployment decisions for first generation system. Groombridge and Murji (1994a & 1994b) argue for minimum technology use matched to a specific goal supported by the public. The main purpose for full color, night vision, tilt, zoom, pan, and videotaped systems must be crime detection (Groombridge & Murji, 1994a: 286). As computer enhanced surveillance is not always needed to meet the target goal, second generation applications will also not always be required and should not be installed simply because they are available. System selection and deployment should be steered by a rule of minimum technology needed to meet a specific application goal rather than installing the most technological capable system affordable. The deployment of every CCTV system increases the psychological sense of being constantly watched and applications should be cautious, not automatic. The above theory is supported the theory of situational crime prevention strategy as postulated by (Cohen & Clarke, 1994:36). The following aspects were found:

Eighty-two per cent were happy or very happy with the installation of CCTV, which is similar to the level of support found in face to face interviews with CCTV Operators and CPFs members.

Those who had been victimised and who felt unsafe were significantly more likely to support CCTV although absolute differences were very small. Individuals appeared confused about the capabilities of CCTV. However, this did not deter them in their support for CCTV and their perceptions as to what they thought CCTV could do. Approximately 80 per cent of the sample agreed that with CCTV on the estate, the level of crime would get lower. Sixty-three per cent were positive CCTV would reduce the number of people hanging around; 80 per cent thought that crime would be minimised or reduced; 68 per cent believed people would report more incidents; 56 per cent that the police would respond more quickly as a result of the cameras being installed.

4.5 SIGNIFICANCE OF FINDINGS

As the use of CCTV in South Africa grows, companies are faced with difficult choices in terms of what they can and cannot legally do with their cameras and the footage they take. When is your footage admissible in court, when will it be deemed illegal? A security policy is the essential basis on which an effective and comprehensive security program can be developed. The importance of this critical component of the overall security system, however, is often overlooked. A security policy is the primary way in which management's expectations for security are translated into specific and measurable goals and objectives. It is crucial to take a top down approach based on a well-stated policy in order to develop an effective security system. On the contrary, if there is not a security policy defining and communicating those decisions, then they will be made by the individuals designing, installing and maintaining security systems. This will result in a disparate and less than optimal security system being implemented.

The above results both support and build upon the lessons of evaluations by other researchers (Welsh & Farrington 2009: 45). CCTV is associated with significant reduction in crime. However, whereas Welsh and Farrington (2009: 47) found that car parks were the only settings where CCTV was associated with major effects in crime decrease, this qualitative review, however, found evidence of significant crime

decrease within other settings most notably residential areas, Business commerce and Railway lines. Certainly levels of support for CCTV are high, although it was not clear that respondents were fully informed about how it functioned. This finding mirrors that for residential areas. The postimplementation survey shed light on whether new CCTV provision will change these levels of support the findings of Caplan et al (2011: 258-263) and Ratcliffe et al (2009: 65) have significant implications for CCTV policy and practice. The varied effect of individual cameras within singular systems suggests cameras may have differed on certain factors that influence effectiveness. As well as any changes in perception, the post-implementation survey will be interesting for what it tells us about changes in behaviour in response to new CCTV provision. Of particular importance is the continued need for CCTV to be narrowly targeted on vehicle, robbery and property crimes and not to be deployed as a stand-alone crime prevention measure. This finding is aligned to CCTV effect may be related to specific place-based characteristics of target areas. Just as certain crimes are conducive to certain environments, specific crime prevention tactics (e.g. CCTV) may be more effective at certain places than others Eck (2002: 702). As CCTV surveillance continues to expand its reach in both public and private space and evolve with new technology, policy will benefit from high quality evaluations of outcomes and implementation. The results of the analysis also demonstrated evidence of significant crime reductions within other settings, particularly residential areas. CCTV schemes incorporating active monitoring generated larger effect sizes than did passive systems. Schemes deploying multiple interventions alongside CCTV generated larger effect sizes than did schemes deploying single or no other interventions alongside CCTV. CCTV is a type of situational crime prevention (SCP) strategy in which levels of formal surveillance are increased within a target area (Cornish & Clarke, 2003: 72; Welsh & Farrington, 2009: 717). SCP is focused on preventing crime by reducing the number of criminal opportunities and increasing the perceived risk of offending through modification of the physical environment (Clarke, 1995: 183). The situational prevention of crime is mainly rooted in the rational choice perspective, in which crime is considered to be “purposive behavior designed to meet the offender's commonplace needs” (Clarke, 1997: 9-10). As per the rational choice perspective, offenders consider several “choice structuring

properties”, which include the potential rewards and inherent risks involved in the commission of a particular crime. The primary aim of CCTV is considered to be the triggering of a perceptual mechanism that impacts an offender's choice structuring properties in a manner that persuades them to abstain from crime (Ratcliffe, (2006: 52). More recently, Alexandrie (2017: 216-219) reviewed seven randomised and natural experiments of CCTV, finding crime reductions of between 24 percent and 28 percent in public streets and urban subway stations, but no effect in parking facilities or suburban subway stations. The findings of Alexandrie (2017: 215) diverged somewhat from those of Welsh and Farrington (2009: 70). Smaller effect sizes associated with quasi-experiments, varying study settings (i.e., countries), and differing integration with police practices as contextual factors may explain this difference. Recent research findings show support for Alexandrie’s (2017: 220) argument that integration with police practices may determine the effects of CCTV (La Vigne et al, 2011: 29; Piza, 2012: 56; Caplan & Kennedy, 2010: 20). The small number of studies used by Alexandrie (2017: 200) however, represents a small proportion of the knowledge base on CCTV.

Lastly, the findings of this research study’s qualitative evaluation echo those of Welsh and Farrington (2009: 45) in terms of the 34 UK CCTV projects they reviewed, which demonstrated a statistically significant reduction of approximately ten percent in crime in the experimental areas compared to control areas.

4.6 CONCLUSIONS

There is anecdotal evidence of the value of CCTV in prosecuting offenders. According to Gill and Hemming (2006: 36) “offenders are not put off by the presence of cameras. The decision-making processes determining where and why cameras are to be installed and whether political pressure is a motivating factor should also be routinely examined. Finally, these findings remind us of just how closely public area CCTV surveillance has come to resemble Jeremy Bentham’s original idea of the Panopticon. Although in the wake of Foucault’s Discipline and Punish there has been a tendency for criminologists and sociologists to see surveillance technologies, such as CCTV in terms

of social control, it is important to remember that for Bentham one of the great virtues of his panoptic prison was that it exposed prison guards as well as prisoners to outside scrutiny.

Overall, it might be concluded that public area CCTV reduces crime in some circumstances. In light of the mixed results and potential social costs, future CCTV schemes should be carefully implemented in different settings and should employ high quality evaluation designs with long follow-up periods.

4.7 RECOMMENDATIONS

The following recommendations, based on the findings from this research study, the information gleaned from the literature review and from general observations made when visiting and examining the locations selected for the study, are made:

1. Firstly, the researcher recommends that other researchers build upon the state of the research presented in this study by seeking opportunities to maximise the rigour of CCTV methodology.
2. Careful consideration needs to be given as to what exactly constitutes the success of a CCTV surveillance system.
3. Appropriate data needs to be gathered and interpreted as an integral part of any determination of success or otherwise (evidence-based policy and service).
4. An appropriate evaluation mechanism needs to be drawn up to review and determine the impact and effectiveness of existing and future schemes.
5. The use of CCTV in an area should be highlighted and publicised so as to inform the public and act as a deterrent to criminal behaviour.

6. All existing CCTV systems should be immediately examined and assessed to determine if they are fit for purpose and effective in their primary objectives.
7. The use of CCTV surveillance is based on Rational Choice Theory. It is expected that offenders will be less likely to commit a crime if they know they are being watched and have a greater risk of being apprehended (La Vigne et al, 2011: 60).
8. Public safety agencies may invest in CCTV for several reasons, such as to assist in the detection and retroactive investigation of crime or promote increased use of public spaces (Gill & Spriggs, 2005; Ratcliffe, 2006).
9. In as much as the promise of public surveillance cameras as a crime prevention and control tool is a powerful motivator for those investing in the technology, it is important to view it in the context of a larger community policing framework. Surveillance cameras alone are not a silver bullet, but simply another crime control and investigative tool. That tool should be employed along with other policing strategies, such as community-oriented problem-solving strategies and intelligence-led policing.
10. Further, it is important for jurisdictions to understand that public surveillance technology is only as good as the way it is employed. If it is employed minimally or is not well-integrated into other policing functions, it is unlikely to yield a significant impact on crime.

4.8 FUTURE RESEARCH

This research study only covered the evaluation of Closed-Circuit-Television (CCTV) for crime control and prevention from selected areas. Further research can work on the technical configuration of the system and legislation aspect in context to have binding law to complete police investigation and private security operations. Additional to that, enhancement work can be done to work on the risk management and mitigation plan to improve the efficiency of CCTV system and the organisations involved. The

effectiveness of the implementation of CCTV depends on the study being done to make sure that the process will bring success in future. None of the organisations will invest in something that cannot be sure the rate of success. Even though the study is being done, the criminal nowadays also become smarter. When they know the area was under CCTV surveillance, especially if they can see the camera, they will try as best as they can to avoid their faces from being caught by the camera. Even some of the criminal was wearing a mask to make sure that they cannot be recognised from the images of Closed-Circuit-Television (CCTV).

LIST OF REFERENCES

- Australian Communications and Media Authority (ACMA). 2011. *An overview of international cyber-security awareness raising and educational initiatives*. Research report commissioned by the Australian Communications and Media Authority. Available at: <https://www.acma.gov.au/theACMA/an-overview-of-international-cyber-security-awareness-raising-and-educational-initiatives> (accessed on: 12 January 2018).
- Ackerman, S. 2014. Outgoing NSA chief Keith Alexander signals openness to surveillance reform. *The Guardian*, 27 February. Available at: <http://www.theguardian.com/world/2014/feb/27/nsa-chief-keith-alexander-surveillance-reform> (accessed on: 18 November 2018).
- Akuta, E. Ong'oa, I. & Jones, C. 2011. Combating cybercrime in sub-Saharan Africa: A discourse on law, policy and practice. *Journal of Peace, Gender and Development Studies*, 1(4): 129-137.
- Alexandrie, G. 2017. Surveillance cameras and crime: A review of randomized and natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 18: 210-222.
- Alford, F.C. 2000. What would it matter if everything Foucault said about prison were wrong? '*Discipline and punish*' after twenty years, *Theory and Society*, 29(1): 125-146.
- American Civil Liberties Union (ACLU). 2002. What's wrong with public video surveillance? Available at: <https://www.aclu.org/other/whats-wrong-public-video-surveillance> (accessed on: 30 January 2019).
- Anon. 2017. CCTV footage a 'silent witness' in Mthethwa murder trial. *ENCA*, 16 March. Available at: <https://www.enca.com/south-africa/cctv-footage-a-silent-witness-in-mthethwa-murder-trial> (accessed on: 10 November 2018).
- Armitage, R. 2002. *To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime*. NACRO Briefing Note. Nacro Crime and Social Policy Section, London.

- Armitage, R., Smyth, G. & Pease, K. 1999. Burnley CCTV evaluation. (Pp. 225-250). In K.A. Painter & N. Tilley (Eds). *Surveillance of public space: CCTV, street lighting and crime prevention*. Crime Prevention Studies 10. Monsey, NY: Criminal Justice Press.
- Babbie, E. & Mouton, J. 2001. *The practice of social research*. Cape Town: Oxford University Press.
- Baghel, R. & Mayr, A. 2007. Glimpses through the cage of fear: International students experience Durban (Pp. 228-234). In R. Pattman & S. Khan (Eds). *Undressing Durban*. Durban: Madiba Press.
- Barnard-Wills, D. 2013. Security, privacy and surveillance in European policy documents. *International Data Privacy Law*, 3(3): 170-180.
- Baškarada, S. 2014. Qualitative case study guidelines. *The Qualitative Report*, 19(40): 1-18. Available at: <http://nsuworks.nova.edu/tqr/vol19/iss40/3> (accessed on: 14 December 2018).
- Bekkers, V. & Moody, R. 2011. Visual events and electronic government: What do pictures mean in digital government for citizen relations? *Government Information Quarterly*, 28(4): 457-465.
- Big Brother Watch. 2018. *Face off: The lawless growth of facial recognition in UK policing*. May. London: Big Brother Watch. Available at: <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> (accessed on 14 December 2018).
- Boeijie, H. 2010. *Analysis in qualitative research*. London: Sage.
- Bogdan, R.C. & Biklen, S.K. 2006. *Qualitative research for education: An introduction to theory and methods*. (5th edition). Boston: Allyn & Bacon/Pearson International.
- Bowcott, O. 2008. CCTV boom has failed to slash crime, say police. *The Guardian*, 6 May. Available at: <https://www.theguardian.com/uk/2008/may/06/ukcrime1> (accessed on: 30 August 2019).
- Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2): 27-40.

- Bowers, K.J. & Johnson, S.D. 2016. Situational prevention. (Pp. 111-135). In D. Weisburd, D.P. Farrington & C. Gill (Eds). *What works in crime prevention and rehabilitation: Lessons from systematic reviews*. New York: Springer.
- Brantingham, P. & Brantingham, P. 2003. Anticipating the displacement of crime using the principles of environmental criminology. *Crime Prevention Studies*. (16)(3): 119-148.
- Brooks, D.J. & Corkill, J. 2014. Corporate security and the stratum of security management. (Pp. 216-234). In K. Walby & R. Lippert (Eds.). *Corporate security in the 21st Century: Theory and practice in international perspective*. New York: Palgrave MacMillan.
- Brown, B. 1995. *Closed circuit television in town centres: Three case studies*. Police Research Group. Crime Prevention and Detection Series Paper 68. London: Home Office. Available at: https://popcenter.asu.edu/sites/default/files/Responses/video_surveillance/PDFs/Brown_1995_Full.pdf (accessed on: 18 November 2018).
- Bygrave, L.A. 2014. *Data Privacy Law: An international perspective*. New York: Oxford University Press.
- Caplan, J.M. & Kennedy, L.W. 2010. *Risk Terrain Modeling Manual*. Newark, NJ: Rutgers Center on Public Security.
- Caplan, J.M., Kennedy, L.W. & Petrossian, G. 2011. Police-monitored CCTV cameras in Newark, NJ: A quasi-experimental test of crime deterrence. *Journal of Experimental Criminology*, 7(3): 255-274.
- Cavoukian, A. 2008 *Privacy and video surveillance in mass transit systems: A special investigation report*. Privacy Investigation Report MC07-68, 3 March. Toronto: Information and Privacy Commissioner of Ontario.
- Chitauro, G. 2015. Cyber laws vital for Zimbabwe. *TechnoMag*. Available at: <http://www.technomag.co.zw> (accessed on: 28 November 2018).
- Chivers, W.G.K. 2016. *Investigating the dynamics of surveillance and resistance in the information society*. Unpublished thesis. PhD (Social Sciences). Cardiff University, Cardiff, UK.

- Clarke, R.V. 1995. Situational crime prevention. (Pp. 173-188). In M. Tonry & D.P. Farrington (Eds). *Building a safer society: Strategic approaches to crime prevention. Crime and Justice: A Review of research*, Vol. 19. Chicago: University of Chicago Press.
- Clarke, R.V. (Ed.). 1997. *Situational crime prevention: Successful case studies*. (2nd edition). Monsey, NY: Criminal Justice Press.
- Clarke, R. & Eck, J. 2003. *Become a problem-solving crime analyst: In 55 small steps*. London: University College of London, Jill Dando Institute of Crime Science. Available at:
<https://popcenter.asu.edu/sites/default/files/library/reading/PDFs/55stepsUK.pdf> (accessed on: 18 November 2018).
- Cohen, L.E. & Felson, M. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44: 588-608.
- Collis, J. & Hussey, R. 2013. *Business research: A practical guide for undergraduate & postgraduate students*. New York: Palgrave MacMillan.
- Cook, T., Hill, M. & Hibbitt, S. 2016. *Blackstone's Crime Investigators' Handbook*. (2nd edition). Oxford: Oxford University Press.
- Cornish, D.B. & Clarke, R.V. 2003. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. (Pp. 111-124). In M. Smith & D.B. Cornish (Eds). *Theory for practice in situational crime prevention. Crime Prevention Studies*, Vol. 16. Monsey, NY: Criminal Justice Press.
- Council of Europe. 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 28 January. European Treaty Series No. 108. Council of Europe: Strasbourg. Available at:
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> (accessed on: 10 October 2018).
- Creswell, J.W. 2013. *Qualitative inquiry and research design: Choosing among five traditions*. Thousand Oaks, CA: Sage.
- Creswell, J.W. 2014. *Qualitative inquiry and research design: Choosing among five approaches*. (3rd edition). Thousand Oaks, CA: Sage.

- David, M. & Sutton, C.D. 2011. *Social research: An introduction*. (2nd edition). London: Sage.
- Davidson, C. 2000. Transcription: Imperatives for qualitative research. *International Journal of Qualitative Methods*. June, 8(2): 35-52.
- Davies, S. 1996. The case against: CCTV should not be introduced. *International Journal of Risk, Security and Crime Prevention*, 4(2): 149-167.
- Degu, G. & Yigzaw, T. 2006. *Research methodology: Lecture notes for health science students*. Ethiopia Public Health Training Initiative, (EPHTI). Carter Centre/USAID. Available at: www.zadoco.site_research-method-fm-carter-center.pdf (accessed on: 5 October 2018).
- Denscombe, M. 2002. *Ground rules for good research: A 10-point guide for social researchers*. Philadelphia, PA: Open University Press.
- Department of the Premier and Cabinet. 1999. *CCTV Guidelines*. Brisbane: Queensland Government, Department of the Premier and Cabinet. Available at: <http://www.communities.qld.gov.au/community/crimeprevention/publications/documents/pdf/cctvguidelines.pdf> (accessed on: 30 August 2019).
- Department of Justice, South Africa. 2018. Protection of Personal Information Act No 4 of 2013. *Government Gazette*, 581 (37067). 26 November. Cape Town: Government Printers. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (accessed on: 25 July 2018).
- Ditton, J. 1999. *The effect of closed-circuit television cameras on record crime rates and public concern about crime in Glasgow*. Edinburgh: The Scottish Government, The Scottish Office Central Research Unit, Crime and Criminal Justice Research Findings No. 30. Available at: <https://www2.gov.scot/Publications/1999/08/ef48bf19-08b4-4641-9119-dd22fb1d29be> (accessed on: 29 April 2018).
- Ditton, J. 2000. Crime and the city: public attitudes to CCTV in Glasgow. *British Journal of Criminology*, 40: 692-709.

- Donald, C. 2015. How long can operators concentrate for? *Hi-Tech Security Solutions*, March. Available at: <https://www.securitysa.com/8289a> (accessed on: August 2019).
- Drum, K. 2014. If you think the NSA debate has been valuable, you have Edward Snowden to thank. *MotherJones*, 2 January. Available at: <https://www.motherjones.com/kevin-drum/2014/01/if-you-think-nsa-debate-has-been-valuable-you-have-edward-snowden-thank/> (accessed on: 17 February 2019).
- Duncan, J. 2018a. *Stopping the spies: Constructing and resisting the surveillance state*. Johannesburg: Wits University Press.
- Duncan, J. 2018b. How CCTV surveillance poses a threat to privacy in SA. *The Conversation*, 4 June. Available at: <https://theconversation.com/how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa-97418> (accessed on: 20 October 2018).
- Eck, J. 2002. Preventing crime at places. (Pp. 241-294). In D.P. Farrington, D.L Mackenzie, L.W. Sherman & B. Welsh (Eds). *Evidence-based crime prevention*. London: Routledge.
- Edwards, R. 2009. Seven of ten murders solved by CCTV. *The Telegraph*, 1 January. Available at: <https://www.telegraph.co.uk/news/uknews/law-and-order/4060443/Seven-of-ten-murders-solved-by-CCTV.html> (accessed on: 30 August 2019).
- Eckblom, P. 2005. Designing products against crime. (Pp. 203-244). In N. Tilley (Ed.). *Handbook of crime prevention and community safety*. Cullompton, Devon, UK: Willan.
- Eckblom, P. 2011. *Crime prevention, security and community safety using the 5Is framework*. Basingstoke, England: Palgrave MacMillan.
- Ekhom, O. 2013. *National security: Intelligence and community partnership approach*: Abuja, Nigeria: Law Lords Publications.

- European Security Research Advisory Board (ESRAB). 2006. *Meeting the challenge: The European Security Research Agenda*. A report from the European Security Research Advisory Board. Luxembourg: Office for Official Publications of the European Communities. Available at: http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf (accessed on: 15 August 2018).
- Felson, M. 1987. Routine activities and crime prevention in the developing metropolis. *Criminology*, 25: 911-931.
- Felson, R.B. 1994. The subculture of violence and delinquency: Individual vs. school context effects. *Social Forces*, 73(1): 155-173.
- Felson, M. & Clarke, R.V. 1998. *Opportunity makes the thief*. Police Research Series, Paper 9: 1-36.
- Foucault, M. (translated from the French by Alan Sheridan). 1999. *Discipline and punish: The birth of the prison*. New York: Random House.
- Garland, D. 1990. *Punishment and modern society: A study in social theory*. Chicago: The University of Chicago Press.
- Garland, D. 1996. The limits of the sovereign state: Strategies of crime control in Contemporary Society. *British Journal of Criminology*, 36(4): 445-471.
- Georgia Tech Information Security Center (GTISC) & Georgia Tech Research Institute (GTRI). 2015. *Emerging cyber threats Report 2015*. Proceedings of the Georgia Tech Cyber Security Summit 2014. Available at: <https://www.cc.gatech.edu/sites/default/files/images/2015emergingcyberthreatsreport.pdf> (accessed on: 14 November 2018).
- Gerber, L. 2000. Denial of Service attacks rip the internet. *IEEE Computer*, April, 33(4): 12-17.
- Gerrard, G. & Thompson, R. 2011. Two million cameras in the UK. *CCTV Image*, Winter: 10-12. Available at: <https://www.securitynewsdesk.com/wp-content/uploads/2011/03/CCTV-Image-42-How-many-cameras-are-there-in-the-UK.pdf> (accessed on: 10 December 2018).
- Gilbert, J.M. 2004. *Criminal investigation*. (6th edition). Upper Saddle River, NJ: Pearson Education.

- Gill, C. 2016. Community interventions. (Pp. 77-109). In D. Weisburd, D.P. Farrington & C. Gill (Eds). *What works in crime prevention and rehabilitation: Lessons from systematic reviews*. New York: Springer.
- Gill, M. 2006. *The handbook of security*. New York: Palgrave Macmillan; 2006.
- Gill, M. & Spriggs, A. 2005. *Assessing the impact of CCTV*. Home Office Research Study 292. London: Home Office Research, Development and Statistics Directorate. Available at: <http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf> (accessed on: 24 February 2019).
- Gill, M. & Turbin, V. 1999. Evaluating 'realistic evaluation': Evidence from a study of CCTV. (Pp. 179-199). In: K. Painter, N. Tilley & Moran, J. (eds). *Crime Prevention Studies*, Monsey, New York: Criminal Justice Press.
- Gold, R. 1969. Roles in sociological field observation. (Pp. 68-75). In G. McCall & J. Simmons (Eds). *Issues in participant observation: A text and reader*. London: Addison Wesley
- Goold, B.J. 2004. *CCTV and policing: Public area surveillance and police practices in Britain*. Oxford: Oxford University Press.
- Goold, B.J. 2006. Open to all? Regulating open street CCTV and the case for 'symmetrical surveillance'. *Criminal Justice Ethics*, 25(1): 3-17.
- Goold, B.J. 2007. Privacy, identity and security. (Pp. 61-63) In B.J. Goold & L. Lazarus, *Security and Human Rights*. Oxford: Hart Publishing.
- Goold, B. 2009. Surveillance and the political value of privacy. *Amsterdam Law Forum*, 1(4): 3-6. Available at: <http://amsterdamlawforum.org/article/view/88/162> (accessed on: 30 September 2018).
- Gray, E., Jackson, J. & Farrall, S. 2011, Feelings and functions in the fear of crime: Applying a new approach to victimisation insecurity. *British Journal of Criminology*, 51(1): 75-94.
- Greenwald, G. 2014. *Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Picador.
- Groombridge, N. & Murji, K. 1994a. As easy as AB and CCTV. *Policing*, 10(4): 283-290.

- Groombridge, N. & Murji, K. 1994b. Obscured by cameras? CCTV and policing, *Criminal Justice Matters*, Fall. 17: 9.
- Haggerty, K.D. & Gazso, A. 2005. Seeing beyond the ruins: Surveillance as a response to terrorist threats. *Canadian Journal of Sociology*, 30(29): 169-187.
- Hustinx, P. 2010. Privacy by design: Delivering the promises. *Identity in the Information Society*, 3: 253-255.
- Jacobs, J. 1961. *The death and life of Great American Cities*. New York: Random House.
- Jermyn, D. 2004. This is about real people! Video technologies, actuality and affect in the television crime appeal. (Pp. 71-90). In S. Holmes & D. Jermyn (Eds). *Understanding reality television*. New York: Routledge.
- Karakus, O., McGarrell, E.F. & Basıbuyuk, O. 2010. Fear of crime among citizens of Turkey. *Journal of Criminal Justice*, 38(2): 174-184.
- Karim H.V. 2007. *Strategic security management: A risk assessment guide for decision makers*. Oxford: Elsevier.
- Kietzman, J. & Angel, I. 2010. Panopticon revisited. *Communications of the ACM*, 53 (6): 135-138.
- Kruegle, H. 2007. *CCTV surveillance: Analog and digital video practices and technology*. Boston: Elsevier Butterworth Heinemann.
- Kvale, S. 1996. *Interviews: An introduction to qualitative research interviewing*. Thousand Oaks, CA: Sage.
- Kumar, R. 2011. *Research methodology: A step-by-step guide for beginners*. (3rd edition). London: Sage.
- Laura, J.N. 2001. Law enforcement management administrative statistics. Paper delivered at the executive brief of the International Association of Chiefs of Police. Washington D.C.

- La Vigne, N., Lowry, S., Markman, J. & Dwyer, A. 2011. *Evaluating the use of public surveillance cameras for crime control and prevention*. Washington, DC: The Urban Institute. Available at: https://www.urban.org/sites/default/files/publication/27556/412403-evaluating-the-use-of-public-surveillance-cameras-for-crime-control-and-prevention_0.pdf (accessed on: 19 January 2019).
- Lee, M. 2007. *Inventing fear of crime: Criminology and the politics of fear*. Cullompton, Devon, UK: Willan.
- Leedy, P. & Ormrod, J. 2010. *Practical research: Planning and design*. New York: Pearson.
- Leggett, T. (Ed.). 2002. *Drugs and crime in South Africa: A study in three cities (Johannesburg, Cape Town and Durban)*. ISS Monograph Series No. 69, March. Pretoria: Institute for Security Studies.
- Levesley, T. & Martin, A. 2005. *Police attitudes to and use of CCTV*. Home Office Online Report series. London: Home Office.
- Lizza, R. 2013. State of deception. *New Yorker*, 16 December. Available at: <http://www.newyorker.com/magazine/2013/12/16/state-of-deception> (accessed on: 19 January 2019).
- Lyon, D. 1994. *The electronic eye: The rise of the surveillance society*. Cambridge: Polity Press
- Lyon, D. 2002. *Surveillance society: Monitoring everyday life*. Buckingham, England: Open University Press
- Lyon, D. 2002. *Surveillance and social sorting: Privacy, risk, and digital discrimination*. London, UK: Routledge.
- Lyon, D. (Ed.). 2003. *Surveillance as social sorting: Privacy, risk, and digital discrimination*. New York: Routledge
- Lyon, D. 2006. 9/11, synopticon and scopophilia: Watching and being watched. (Pp. 35-54). K. Haggerty & R. Ericson (eds). *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.
- Lyon, D. 2011. *Surveillance society: Monitoring everyday life*. Buckingham. Open University Press

- Lyon, D. 2015. *Surveillance after Snowden*. Cambridge: Polity Press.
- Maat, S. 2009. *Cybercrime: A comparative law analysis*. Unpublished dissertation. LL.M. University of South Africa, Pretoria.
- Madanipour, A. 1998. Social exclusion and space. (Pp. 186-194). In R.T. LeGates & F. Stout (Eds). *City Reader*. London/ New York: Routledge.
- Mali, P. 2010. Types of cyber crimes and cyber law in India. *Journal of Law*, 10(1): 32-60.
- Marwick, A. 2012. The public domain: Surveillance in everyday life. *Surveillance & Society*, 9(4): 378-393.
- Matchett, A.R. 2003. *CCTV for security professionals*. Amsterdam: Butterworth-Heinemann.
- May, T. 1997. *Social research: Issues, methods and process*. (2nd edition). Buckingham: Open University Press.
- Maxfield, M.G. & Babbie, E.R. 1995. *Research methods for criminal justice and criminology*. Belmont, CA: Wadsworth.
- Mazerolle, L., Hurley, D.C. & Chamlin, M. 2002. Social behavior in public space: An analysis of behavioral adaptations to CCTV. *Security Journal*, 15(3): 59-75.
- McCahill, M. & Norris, C. 2002. *CCTV systems in London: Their structures and practices*. Working Paper No.10, April. RTD-Project: On the threshold to urban panopticon? Analysing the employment of CCTV in European cities and assessing its social and political impacts. (September 2001-February 2004). 5th Framework Programme of the European Commission.
- Norris, C. & McCahill, M. 2006. CCTV: Beyond penal modernism? *British Journal of Criminology*, 46, 97–118.
- Minnaar, A. 2006. *The implementation and impact of crime prevention/crime control public (open street) Closed-Circuit Television (CCTV) surveillance in South African central business districts (CBDs)*. Paper presented to the Crime, Justice and Surveillance Conference. Hosted by the Centre for Criminological Research, University of Sheffield/Surveillance and Society. University of Sheffield, Sheffield, UK. 5-6 April.

- Minnaar, A. 2007. The implementation and impact of crime prevention/crime control open street Closed-Circuit Television surveillance in South African Central Business Districts. *Surveillance & Society Journal* (Special Issue on Surveillance and Criminal Justice). Part 1, 4 (3): 174-207.
- Minnaar, A. 2008. Closed-circuit television (CCTV) surveillance in central business districts (CBDs): Street surveys from four South African cities. Paper presented to the XVth World Congress of the International Society of Criminology: *Crime and criminology – Research and action*. Barcelona, Spain. 20-25 July.
- Minnaar, A. 2014. 'Crackers', cyberattacks and cybersecurity vulnerabilities: The difficulties in combating the 'new' cybercriminals. *Acta Criminologica: Southern African Journal of Criminology. Special Edition No 2/2014: Research and practice in Criminology and Criminal Justice*: 127-144
- Minnaar, W. 2018. Spokesperson Johannesburg Metropolitan Police Department (JMPD) 28 September 2018.
- Müller, C. & Boos, D. 2004. Zurich Main Railway Station: A typology of public CCTV systems. *Surveillance and Society*, 2(2/3): 161-176.
- [US] National Institute of Justice (NIJ). [Sa]. *Crime & Crime Prevention: Community Crime Prevention Strategies*. Washington DC: National Institute of Justice, Office of Justice Programs. Available at: <https://www.crimesolutions.gov/TopicDetails.aspx?ID=10> (accessed on: 18 January 2019).
- [US] National Initiative for Cybersecurity Education. National Institute for Standards and Technology (NIST). 2011. *Draft National Cybersecurity Workforce Framework, ver. 2.0*. Washington, DC: NIST National Initiative for Cybersecurity Education. Available at: <https://www.nist.gov/file/359261> (accessed on: 18 January 2019).
- Neethling, J., Potgieter, J.M. & Knobel, J.C. 2006. *Law of Delict*. Durban: Butterworths
- Neumann, P.G. 2000. Denial-of-Service attacks. *ACM Communications*, 43(4): 136.
- Newman, O, 1972. *Defensible Space: People and Design in the Violent City*. London: Architectural Press.

- Norris, C. & Armstrong, G. 1999. *The maximum surveillance society: The rise of CCTV*. Oxford: Berg
- Norris, C. 2012. The success of failure. Accounting for the global growth of CCTV. (Pp. 251-258). In K. Ball, K.D. Haggerty & D. Lyon (Eds). *Routledge handbook of surveillance studies*. London and New York: Routledge.
- Obama, B. 2013, February 12. *Executive Order: Improving critical infrastructure cybersecurity*. Available at: <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity> (accessed on: 15 March 2019).
- Obama, B. 2014. Obama's speech on N.S.A. phone surveillance [Transcript]. *New York Times*, 17 January. Available at: <http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html> (accessed on: 20 February 2019).
- Organisation for Economic Co-operation and Development (OECD). 2013. *The OECD Privacy Framework*. Paris: OECD Publishing.
- Palmer, A. 1998, *Principles of evidence*. Sydney: Cavendish.
- Pandey, P. & Pandey, M.M. 2015. *Research methodology: Tools and techniques*. Romania: Bridge Center.
- Parker, J.R. & Federl, P. 1997. *An approach to license plate recognition*. Available at: <https://prism.ucalgary.ca/bitstream/handle/1880/46439/1996-591-11.pdf> (accessed on: 19 January 2019).
- Patton, M.Q. 2002. *Qualitative evaluation and research methods*. (3rd edition). Thousand Oaks, CA: Sage.
- Pawson, R. & Tilley, N.1997. *The handbook of security*. London, UK: Sage.
- Piza, E.L. 2012. *Identifying the best context for CCTV camera deployment: An analysis of micro-level features*. Unpublished doctoral dissertation. PhD in Criminal Justice. Newark, NJ: Rutgers University.
- Piza, E.L. 2018a. The history, policy implications and knowledge gaps of the CCTV literature: Insights for the development of body-worn video camera research. International. *International Criminal Justice Review*: 1-21.

- Piza, E.L. 2018b. The crime prevention effect of CCTV in public places: A propensity score analysis. *Journal of Crime and Justice*, 41(1): 14-30.
- Piza, E.L. & O'Hara, B.A. 2014. Saturation foot-patrol in a high-violence area: A quasi-experimental evaluation. *Justice Quarterly*, 31(4): 693-718.
- Piza, E.L. & Sytsma, V.A. 2016. Exploring the defensive actions of drug sellers in open-air markets: A systematic social observation. *Journal of Research in Crime and Delinquency*, 53(1): 36-65.
- Phillips, C. 1999. A review of CCTV evaluations: Crime reduction effects and attitudes toward its use. *Crime Prevention Studies*, 10: 123-155.
- Poster, M. 1990: *The mode of information. Poststructuralism and social context*, Cambridge: Polity Press
- Ratcliffe, J.H. 2006. Video surveillance of public places. Problem-Oriented Guides for Police Response Guides, Series No. 4. Washington, DC: Office of Community Oriented Policing Services (COPS office), US Department of Justice.
- Ratcliffe, J.H. 2011. *Video surveillance of public places*. Problem-oriented guides for police response guides series. Washington: DC: Center for Problem-Oriented Policing.
- Ratcliffe, J.H., Taniguchi, T. & Taylor, R. B. 2009a. The crime reduction effects of public CCTV cameras: A multimethod spatial approach. *Justice Quarterly*, 26, 746-770
- Ratcliffe, J.H., Travis, T. & Taylor, R.B. 2009b. The crime reduction effects of public CCTV cameras: A multi-method spatial approach. *Justice Quarterly*, 26(4): 46-70.
- Rea, L.M. & Parker, R.A. 2005. *Designing and conducting survey research: A comprehensive guide*. (3rd edition). San Francisco, CA: Jossey-Bass.
- Reaves, B. 2015. *Local police departments, 2013: Equipment and technology*. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.
- Roos, A. 2007. Data protection: Explaining the international backdrop and evaluating the current South African position. *South African Law Journal*. 124 (2): 400-437.

- Sargent, G. 2014. Yes, we have Snowden to thank for NSA surveillance debate. *The Washington Post*, 2 January. Available at: <https://www.washingtonpost.com/blogs/plum-line/wp/2014/01/02/yes-we-have-snowden-to-thank-for-nsa-surveillance-debate/> (accessed on: 23 November 2018).
- Sherman, L.W. 1998. *Evidence-based policing*. Washington, DC: Police Foundation.
- Short, E. & Ditton, J. 1998. Seen and now heard: Talking to the targets of open street CCTV. *British Journal of Criminology*, 38(3): 404-428.
- Sibiya, M. 2018. Surveillance evolves as cameras get a brain. *Startup Africa*, December. Available at: <https://startupafrica.co.za/?p=6382> (accessed on: 18 December 2018).
- Smith, G.J.D. 2008. Rooms without doors? Researching 'closed settings' – getting in, getting out' (Pp. 12-23). In L. Hempel & O. Svenonius (Eds). *The New Surveillance*. London: Routledge-Cavendish.
- Solove, D.J. 2011. *Nothing to hide: The false tradeoff between privacy and security*. New Haven, CT: Yale University Press.
- South Africa. 2002. Electronic Communications and Transactions Act No 25 of 2002 [ECTA]. *Government Gazette*, 446 (23708). 2 August. Cape Town: Government Printer. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf (accessed on: 18 November 2018).
- South Africa. 2013. Protection of Personal Information Act No. 4 of 2013 [POPI]. Pretoria: Government Printer.
- South African Police Service. 1996. *The National Crime Prevention Strategy*. Available at: (accessed on: 15 August 2019).
- South African Police Service. 2010. *National Instruction: Surveillance 3/2010*. Pretoria: National Commissioner of the SAPS.
- Statistics South Africa (StatsSA). 2018a. *Statistical Release P0302: Mid-year population estimates 2018*. 23 July. Pretoria: Statistics South Africa. Available at: <http://www.statssa.gov.za/publications/P0302/P03022018.pdf> (accessed on: 15 November 2018).

- Statistics South Africa (StatsSA). 2018b. *Victims of Crime Survey 2016/17*. September.
- Stelfox, P. 2009. *Criminal investigation: An introduction to principles and practice*. Uffculme: Willan.
- Steven, P. 2010. *Crime prevention*. New Providence, NJ: Matthew Bender & Co.
- Strydom, H. 2011. Ethical aspects of research in the social sciences and human service professions. (Pp. 113-130). In: A.S. de Vos, H. Strydom, C.B. Fouche & C.S.L. Delpont. *Research at grass roots: For the social sciences and human services professions*. Pretoria: Van Schaik.
- Surette, R. 2005. The thinking eye. Pros and cons of second-generation CCTV surveillance systems. *Policing: An International Journal of Police Strategies & Management*, 28(1): 152-173.
- Swart, H. 2018. Joburg's new hi-tech surveillance cameras: A threat to minorities that could see the law targeting thousands of innocents. *Daily Maverick*, 28 September. Available at: <https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/> (accessed on: 14 December 2018).
- Taylor, E. 2010. Evaluating CCTV: Why the findings are inconsistent, inconclusive and ultimately irrelevant. *Crime Prevention and Community Safety*, 12(4): 209-232.
- Tilley, N. 1993. *Understanding car parks, crime and CCTV: Evaluation lessons from safer cities*. Crime Prevention Unit Series Paper No 42. London: UK Home Office Police Department. Available at: www.crimereduction.gov.uk/cctv2.htm (accessed on: 18 November 2018).
- Trottier, D. 2012. *Social media as surveillance: Rethinking visibility in a converging world*. Burlington, VT: Ashgate
- Ulaga, W. 2003. Capturing value creation in business relationships: A customer perspective. *Industrial Marketing Management*, 32 (8): 677-693.

- United Nations Office on Drugs and Crime (UNODC). 2010. *Handbook on the United Nations Crime Prevention Guidelines: Making them work*. Criminal Justice Handbook Series. Vienna: United Nations. Available at: <https://www.erich-marks.de/Biografie/Media/HandbookCrimePrevention.pdf> (accessed on: 20 August 2019).
- University of South Africa. 2007. *Unisa policy on research ethics*. September. Florida: University of South Africa.
- U.S. Senate Select Committee on Intelligence. 2014. *Annual open hearing on current and projected national security threats against the United States*. Washington DC: Select Committee on Intelligence of the United States Senate. Available at: <https://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-national-security-threats-against-united-states#> (accessed on: 23 January 2019).
- Van Rooyen, H.J.N. 2013. *Investigate corruption*. Pretoria: Henmar.
- Welman, J.C & Kruger, S.J. 2001. *Research methodology for the business and administrative sciences*. (2nd edition). Cape Town: Oxford University Press.
- Weisburd, D., Farrington, D.P. & Gill, C. (Eds). 2016. *What works in crime prevention and rehabilitation: Lessons from systematic reviews*. New York: Springer
- Welsh, B.C., Hollis, M., Farrington, D.P., Elffers, H. & Braga, A. 2011. Research design influence on study outcomes in crime and justice: A partial replication with public area surveillance. *Journal of Experimental Criminology*, 7 (2): 183-198.
- Welsh, B.C. & Farrington, D.P. 2008. *Closed-circuit television surveillance and crime prevention: A systematic review*. Stockholm: Swedish National Council for Crime Prevention. Available at: https://www.bra.se/download/18.cba82f7130f475a2f1800023747/1371914733666/2008_closed-circuit_television_surveillance.pdf (accessed on: ?).
- Welsh, B.C. & Farrington, D.P. 2007. Evidence-based crime prevention (Pp. 1-17). In B.C. Welsh. & D.P. Farrington (Eds). *Preventing crime*. New York: Springer.
- Welsh, B.C. & Farrington, D.P. 2008a Effect of closed-circuit television surveillance on crime. *Campbell Systematic Reviews*, 17: 1-73.

- Welsh, B.C. & Farrington, D.P. 2008b. Surveillance for crime prevention in public space: Results and policy choices in Britain and America. *Criminology & Public Policy*, 3(3): 497-526.
- Welsh, B.C. & Farrington, D.P. 2009a. Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, 26(4): 716-745.
- Whitaker, R. 1999. *The end of privacy: How total surveillance is becoming a reality*. New York: The New Press.
- World Population Review, 2019a. *Johannesburg population*. (2019-18-01). Available at: <http://worldpopulationreview.com/world-cities/johannesburg-population/> (accessed on: 18 January 2019).
- World Population Review, 2019b. *Pretoria [Tshwane] population*. (2019-18-01). Available at: <http://worldpopulationreview.com/world-cities/pretoria-population/> (accessed on: 18 January 2019).
- Yin, R.K. 1994. *Applications of case study research*, London: SAGE.
- Zedner, L. 2009. *Security: Key ideas in Criminology*. London: Routledge.
- Zorn, T. 2010. Designing and conducting semi-structured interviews for research. Available at: <http://home.utah.edu/~u0326119/Comm4170-01/resources/Interviewguidelines.pdf> (accessed on: 18 November 2018).

Annexure A: UNISA Research Ethics Approval Letter



UNISA CLAW ETHICS REVIEW COMMITTEE

Date 20171128

Reference: ST69 OF 2017
Applicant: S Moyo

Dear S Moyo

**Decision: ETHICS APPROVAL
FROM 28 NOVEMBER 2017 TO
27 NOVEMBER 2020**

Researcher: S Moyo

Supervisor: Prof. AdeV Minnaar

EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG

Qualification: MTech in Security Management

Thank you for the application for research ethics clearance by the Unisa CLAW Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **CLAW Ethics Review Committee** reviewed the **Low Risk application** on 28 November 2017 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on the Research Ethics Risk Assessment. The decision was ratified by the Committee.*

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on research Ethics.
2. Any adverse circumstances arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.



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

4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, No 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. No fieldwork activities may continue after the expiry date of 5 September 2020. Submission of the completed research ethics progress report will constitute application for renewal of Ethics Research Committee approval.

Note:

The reference number ST69 OF 2017 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely



PROF D Govender
Chair of CLAW ERC
E-mail: govend1@unisa.ac.za
Tel: (012) 429-9482



PROF OS SIBANDA
Acting Executive Dean : CLAW
E-mail: sibanos@unisa.ac.za
Tel: (012) 429-8374




Annexure B: Turnitin Similarity Index Report

Turnitin Originality Report

- Processed on: 08-Feb-2019 20: 44 SAST
- ID: 1075107065
- Word Count: 40 908
- Submitted: 1

EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG
By Sheperd Moyo



Similarity Index
28%

Similarity by Source

Internet Sources: 26%
Publications: 8%
Student Papers: N/A

Annexure C: Language Editor Confirmation Letter

Barbara Shaw
Editing/proofreading services
18 Balvicar Road, Blairgowrie, 2194
Tel: 011 888 4788 Cell: 072 1233 881
Email: bmsshaw@telkomsa.net
Full member of The Professional Editors' Group

TO WHOM IT MAY CONCERN

This letter serves to inform you that I have done language editing on the following dissertation:

Name: **S MOYO**

Student no.: **36945323**

Qualification: **MTech Security Management dissertation**

Title: **EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR
CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES
FROM JOHANNESBURG AND TSHWANE, GAUTENG**

No of pages: **136 (of text excluding List of References and Annexures)**



Barbara Shaw

28 February 2018

Annexure D: Request permission to do research letter [DRAFT]

[Company address]

FOR ATTENTION: Managing Director:

Dear Mr/Ms....

RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH FOR AN MTECH DISSERTATION

Mr **Sheperd Moyo**, (UNISA Student Number: 36945323), is currently a Masters student at the University of South Africa (UNISA), busy with his research studies for a Masters' degree (MTech in Security Management). The title of his research topic is: ***EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG***

Mr Moyo has obtained ethical clearance from the UNISA College of Law Research Ethics Review Committee (#ref: ST69/2017) to proceed with his fieldwork research (see attached letter dated: 28 November 2017).

Accordingly, we would like to request permission for him to undertake fieldwork research and conduct interviews with your organisations/company's personnel, particularly those working in your control room and involved in the CCTV surveillance operations therein.

DESCRIPTION OF THE RESEARCH PROJECT

The primary aim and purpose of this study is to evaluate the use of CCTV Surveillance for better crime control and prevention. At the broadest level, the aim of this review is to give a clear sense of what can reliably be believed to be true about the effects of CCTV surveillance systems on crime reduction/prevention based on the existing evidence, to link these findings to a wider set of questions and considerations at the level of policy, and to highlight outstanding issues and areas where further research is needed. Accordingly, the purpose of the research is an exploratory study that intends to explore what is happening on the ground in terms of the topic; to seek new insights; to ask questions and to assess the phenomena in a new light. It is hoped to add value to the existing body of knowledge, particularly since there is very little in-depth research information known about the phenomena in South Africa. On the other hand, the exploratory study aims to find out the causal relationships between variables. The present study to undertake several site case studies as part of the research and

methodological approach. Case studies to be selected to evaluate the use of CCTV surveillance systems for crime control and prevention in selected policing precincts in Johannesburg and Tshwane (Pretoria) in the Gauteng Province. It is hoped the resulting research findings will lead to the formulation of a Best Practices Model for the use of CCTV Surveillance Systems in local community crime prevention and reduction initiatives in assisting both communities and police in combatting crime. In addition, use of CCTV surveillance in private security control rooms to assist in rapid response to crimes in progress in surveilled areas.

INTERVIEWS

The one-on-one interviews will be based on a Schedule of Interview Questions (see attached). Broadly the Schedule of Interview Questions will revolve around the primary research questions, inter alia:

- Tell me about your experiences with public CCTV surveillance?
- What in your opinion has been the impact of CCTV surveillance systems installation in your area on crime prevention and control?
- What do you think has been the impact that CCTV has on crime in general?
- What is your opinion of the impact of public CCTV surveillance regarding the privacy rights of individuals?
- How do you think can CCTV video footage be used as a surveillance technique in crime prevention and control?
- In what way do you think CCTV video footage be admitted as evidence in court?
- In what way do you think CCTV surveillance systems can be integrated into overall crime prevention initiatives and Community Policing?

CONFIDENTIALITY OF COLLECTED RESEARCH INFORMATION

All the information that is received from the participants/respondents will be treated with the utmost confidentiality (i.e. respondents will remain anonymous and no reference will be made to their identity or to the organisation for which they work). Neither organisation nor names of individual respondents/participants will be used in the resulting research report (i.e. identities will remain unknown and protected).

Participation in the research interviews/survey questionnaire will also be on a voluntary basis (informed consent).

The final dissertation (research report) once accepted will be placed in the UNISA library and therefore in the public domain and can be accessed by interested parties.

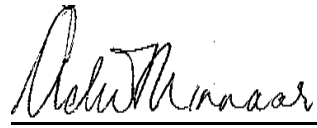
Attached for your information, is a detailed research proposal and a draft set of interview questions.

If any confirmation or other information is needed, Mr Moyo can be directly contacted at the following: **Tel:** 012 433 9477 / **Cell:** 082 316427 / **Email:** Emoyos2@unisa.ac.za.

Alternatively, Prof AdeV Minnaar, Mr Moyo's study supervisor, can also be directly contacted (see below for contact details).

Once permission is granted to Mr Moyo to commence his field research with members of your organisation/company, please inform him accordingly. Mr Moyo will then be in touch directly with you or a representative of your organisation/company for the scheduling of any interviews with the relevant persons at the organisation/company.

Regards

 (Prof)

AdeV Minnaar

Postgraduate Supervisor

Department of Criminology & Security Science

School of Criminal Justice, College of Law, University of South Africa

Email: aminnaar@unisa.ac.za Cell: 083 8949485 Tel: 012 433 9530

Annexure E: Participant Information Sheet

PARTICIPANT INFORMATION SHEET

Date:

UNISA College of Law ethics clearance reference number: ST69/2017

Dear Prospective Participant

RESEARCH PROJECT: *EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG*

My name is **Sheperd Moyo**, (UNISA Student Number: 36945323), and I am currently doing research in the Department of Criminology & Security Science, School of Criminal Justice, in the College of Law at the University of South Africa (UNISA), for a Masters' degree (MTech in Security Management).

My study supervisor is **Prof Anthony Minnaar** (Research Professor in Criminal Justice Studies in the Department of Criminology & Security Science at UNISA.)

We would like to invite you to participate in Mr Moyo's research study project titled: *Evaluating the use of CCTV surveillance systems for crime control and prevention: Selected case studies Johannesburg and Tshwane, Gauteng.*

THE PURPOSE OF THE STUDY

The primary aim and purpose of this study is to evaluate the use of CCTV Surveillance for better crime control and prevention. At the broadest level, the aim of this research study is to give a clear sense of what can reliably be believed to be true about the effects of CCTV surveillance systems on crime reduction/prevention based on the existing evidence, to link these findings to a wider set of questions and considerations at the level of policy, and to highlight outstanding issues and areas where further research is needed. Accordingly, the purpose of the research is an exploratory study that intends to explore what is happening on the ground in terms of the topic; to seek new insights; to ask questions and to assess the phenomena in a new light. It is hoped to add value to the existing body of knowledge, particularly since there is very little in-depth research information known about the phenomena in South Africa. On the other hand, the exploratory study aims to find out the causal relationships between variables. The present study to undertake several site case studies as part of the research and methodological approach. Three case studies to be selected to evaluate the use of CCTV surveillance systems for crime control and prevention in selected policing precincts in Johannesburg, Gauteng Province.

It is hoped the resulting research findings will lead to the formulation of a Best Practices Model for the use of CCTV Surveillance Systems in local community crime prevention and reduction initiatives in assisting both communities and police in combatting crime. In addition, the use of CCTV surveillance in private security control rooms to assist in rapid response to crimes in progress in surveilled areas.

WHY ARE YOU BEING INVITED TO PARTICIPATE?

You have been identified as a suitable participant given your work position/experience in your company related to either the management/supervision of CCTV surveillance systems or involved as an operator of these security systems in your company's control room/or as a first responder to CCTV surveillance alerts to a crime in progress.

Your company, upon my research permission request, has recommended/referred you to me and provided me with your contact information for that purpose.

In the course of my research study I intend to interview a minimum of thirty persons related to your work position as relating to CCTV surveillance systems operations at other companies in the selected research site areas.

WHAT IS THE NATURE OF YOUR PARTICIPATION IN THIS STUDY?

Your participation in this research study will be via a one-on-one semi-structured interview in order to gain valuable information from you as a participant. The interview will further serve to gain insight and in-depth detailed information from all participants' in terms of their respective fields of expertise. The interview should not last longer than +45 minutes and will be held at a time and venue according to the participant's convenience. The interview will be voice recorded (with the participant's permission) and notes will be written during the interview.

Broadly the Schedule of Interview Questions will revolve around the primary research questions, inter alia:

- Tell me about your experiences with public CCTV surveillance?
- What in your opinion has been the impact of CCTV surveillance systems installation in your area on crime prevention and control?
- What do you think has been the impact that CCTV has on crime in general?
- What is your opinion of the impact of public CCTV surveillance regarding the privacy rights of individuals?
- How do you think CCTV video footage can be used as a surveillance technique in crime prevention and control?
- In what way do you think CCTV video footage can be admitted as evidence in court?
- In what way do you think CCTV surveillance systems can be integrated into overall crime prevention initiatives and Community Policing?

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Your participation is completely voluntary, and you are under no obligation to consent to participation. You are also at liberty to withdraw from the study at any stage of the interview without giving a reason. Not agreeing to participate or withdrawal during the interview itself will have no negative repercussions (penalties or work sanctions) on you as an interviewee or employee of the company, since participation is voluntary.

If you do agree to take part, you will be given this information sheet to keep and be asked to sign a written consent form. Moreover, also providing permission to voice record your interview.

ANY NEGATIVE CONSEQUENCES IF YOU PARTICIPATE IN THIS RESEARCH PROJECT?

The researcher does not foresee any negative consequences to you personally in participating in this research study. In addition, all information (responses) provided by you to him during the interview will be regarded as confidential. The researcher will not disclose any respondents' names or contact details unless permission to do so is given by you.

WILL THE INFORMATION THAT YOU CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

The confidentiality of all information provided by you as a participant/interviewee of this study will be protected and kept confidential by the following steps taken by the researcher:

- All the identities of participants will not to be shared with any other persons with no exception.
- Anonymity of the participants to be maintained through the removal of any identifying characteristics.
- All interview information received by the researcher will be transcribed and viewed only by him.
- The information received from any respondent/interviewee will be electronically stored (password protected) by the researcher.
- The findings of the research will be documented in the form of an academic dissertation with all respondents only identified by a sequential number allocated to each.

Your name will not be recorded anywhere in the research report and no one, apart from the researcher, will know about your involvement in this research since all your responses (answers) to the interview questions will be given a code number and you will be referred to in this way in the data, the resulting dissertation or other research reporting methods, such as conference proceedings or journal articles or any publications, by this identifier number.

No one else besides myself as the primary researcher will have access to the research information/data collected in the interviews. (Your answers will be reviewed by people responsible for making sure that the research was done properly (i.e. members of the Research Ethics Review Committee and supervisor, Prof Minnaar).

HOW WILL THE RESEARCHER(s) PROTECT THE SECURITY OF DATA?

All documentation pertaining to this research study will be kept in a locked office or at researcher's home (residence adequately protected by means of security measures).

The electronic information will be stored on a password protected computer.

PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

No monetary payment, inducements, or incentives will be offered by the researcher for your participation in this study. Neither will any intimidatory actions be used by the researcher to force or entice you to participate.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the College of Law at the University of South Africa. A copy of the approval letter can be obtained from the researcher if you so wish.

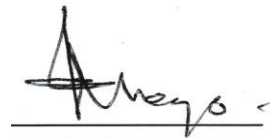
HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact **Mr Moyo** on cell: **082 316427**. The findings will also be accessible in the submitted final dissertation stored electronically in the University of South Africa's Library database of all UNISA dissertations and theses.

Should you require any further information or want to contact the researcher about any aspect of this study, please contact him on the above cellphone number, direct telephone office number: 012 433 9477 or email him at: emoyos2@unisa.ac.za.

Should you have concerns about the way in which the research has been conducted, you may contact Prof Minnaar, his supervisor at cell: 083 8949485 or via email at: aminnaar@unisa.ac.za. Contact the research ethics chairperson of the College of Law Research Ethics Review Committee, Prof D. Govender (email: Govend1@unisa.ac.za; Tel: 012 433 9582) if you have any ethical concerns.

Thank you for taking the time to read this information sheet and for participating in this study.



Mr Sheperd Moyo

Annexure F: Proforma Informed Consent Form

CONSENT TO PARTICIPATE IN THE RESEARCH STUDY:

EVALUATING THE USE OF CCTV SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: SELECTED CASE STUDIES FROM JOHANNESBURG AND TSHWANE, GAUTENG

I, _____, (participant's name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet covering letter.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the voice recording of the interview (delete if no consent to voice recording of interview) [strikethrough and initial by interviewee and researcher].

I have received a signed copy of the informed consent agreement.

Research respondent/Participant Name & Surname: (Please print)	
Participant's signature:	Date:
Researcher: Mr Sheperd Moyo UNISA Student No. 36945323	
Researcher's signature:	Date:

Annexure G: Schedule of Interview Questions: Private Security Control Rooms: CCTV Surveillance Operations

SCHEDULE OF INTERVIEW QUESTIONS

PRIVATE SECURITY CONTROL ROOMS: CCTV SURVEILLANCE OPERATIONS

RESEARCH PROJECT TITLE:

Evaluating the use of CCTV surveillance systems for crime control and prevention: Selected areas in Johannesburg and Tshwane, Gauteng

INSTRUCTIONS:

Please answer the following questions as honestly as possible. You do not need to identify yourself and, similarly, the researcher will uphold your anonymity in that there will be no possibility of any respondent being identified or linked in any way in the research findings by name or otherwise in the final research report (nor the company/organisation for which you work).

Where required, please indicate your answer with a cross (X) in the appropriate box or write a response in the space provided.

SECTION A: BIOGRAPHICAL INFORMATION

Question 1: Gender

Gender	(X)
Male	
Female	

Question 2: Age

Age	(X)	Age	(X)
20-24 years old		25-29	
30-34		35-39	
40-44		45-49	
50-54		55-59	
60+			

Question 3: Highest educational qualification

Highest educational qualification	(X)
Standard 8/Grade 10	
Standard 9/Grade 11	
Standard 10/Grade 12	
Certificate Level NQF 3-4	
Certificate Level NQF 5	
1-year Diploma	
3-year Diploma	
BA degree	
BTech	

Advanced Diploma	
Hons/Postgraduate Diploma	
Masters	
Doctoral	
Other (specify):	

Question 4: Have you undergone any other specialised training/shortcourse(s) applicable to work in the private security industry (list below).

--

Question 5: How many years of work experience do you have in the private security industry?

Years of work experience in PSI	(X)
Less than 1 year	
1 year	
2 years	
3 years	
4 years	
5 years	
6-9 years	
10 years	
11-15 years	
More than 15 years	

Question 6: How many years of work experience do you have in your current position?

Years of experience in current post	(X)
Less than 1 year	
1 year	
2 years	
3 years	
4 years	
5 years	
6-9 years	
10 years	
11-15 years	
More than 15 years	

Question 7: What is your current work position (within the domain of a control room CCTV surveillance operations)?

Position	(X)
Site Manager	
Supervisor	
Team leader	

Member of response team	
Control Room Operator	
CCTV Surveillance Operator	
Other (specify)	

SECTION B: CCTV SURVEILLANCE OPERATIONS

Question 8: The CCTV surveillance operations in this control room are currently installed at which sites (indicate all sites not just primary)?

CCTV installed site	(X)
1. Shopping centre/mall	
2. Residential neighbourhood	
3. Central Business District (CBD)	
4. Gated neighbourhood	
5. (Private) Security estate	
6. Business premises	
7. Factory/industrial site	
8. Along highways	
9. On public streets	
10. Other (specify)	

Question 9: If No 1 (shopping centre/mall) selected above describe CCTV installation at this site?

Shopping centre/mall	(X)
1. In open-air shopping centre car park	
2. Underground parking/parkade	
3. Inside mall along walkways/passages	
4. Inside shops	
5. At entrances to shopping centre	
6. Other (specify)	

Question 10: If No 2 (residential neighbourhood) selected above describe CCTV installation at this site?

Residential neighbourhood	(X)
1. At entrance access roads	
2. Along residential streets	
3. At crossroads/corners of streets inside residential area	
4. On masts on private property of selected residents' properties	
5. Other (specify)	

Question 11: If No 3 (Central Business District (CBD)) selected above describe CCTV installation at this site?

Central Business District (CBD)	(X)
1. On street corner masts	
2. Mounted on selected buildings	
3. Along pedestrian walkways	
4. Inside buildings	
5. Other (specify)	

Question 12: If No 4 (gated neighbourhood) selected above describe CCTV installation at this site?

Gated neighbourhood	(X)
1. At boomgate access-controlled entrance	
2. At entrance access roads	
3. Along residential streets	
4. At crossroads/corners of streets inside security estate	
5. On masts on private property of selected residents' properties	
6. Other (specify)	

Question 13: If No 5 (private security estate) selected above describe CCTV installation at this site?

Private security estate	(X)
1. At boomgate access-controlled entrance	
2. At entrance access roads	
3. Along security estate roads	
4. Along perimeter walls (at intervals)	
5. On masts on private property of selected residents' properties	
6. Other (specify)	

Question 14: If No 6 (business premises) selected above describe CCTV installation at this site?

Business premises	(X)
1. Along perimeter fencing/wall	
2. At access-controlled entrance	
3. Over vehicle parking area	
4. Mounted on business premises' building	
5. Inside business premises	
6. Other (specify)	

Question 15: If No 7 (factory/industrial site) selected above describe CCTV installation at this site?

Factory/industrial site	(X)
1. Along perimeter fencing/wall	
2. At access-controlled entrance	
3. Over vehicle parking area	
4. Mounted on factory building	
5. Inside factory building	
6. Other (specify)	

Question 16: What operational processes are followed in the Control Room for CCTV Surveillance (describe in detail)

Question 17: What happens when suspicious activity is picked up on the CCTV cameras (describe)?

Question 18: On what type of activity/incident is a response team sent out?

Question 19: Does your company co-operate with the SAPS in responding to incidents?

Yes		No	
-----	--	----	--

Question 20: If yes to above, describe in what way?

Question 21: If no to above, motivate why not?

Question 22: In your opinion, how does CCTV surveillance fit into overall crime prevention initiatives?

Question 23: What value do you think CCTV surveillance operations can provide to crime prevention initiatives in local areas?

--

Question 24: How best do you think can CCTV surveillance systems assist in solving crime?

--

Question 25: Has any CCTV footage from CCTV surveillance operations in this Control Room been used to solve (leading to arrest of perpetrator/successful prosecution) a crime?

Yes		No	
-----	--	----	--

Question 26: If yes, provide some examples/cases of such?

--

Question 27: If yes to Q25, how often (number) in the last (indicate selected time period with an 'X') has that occurred (indicate number of cases):

Period of time	'X'	(Estimated) Number of cases
Previous six months		
12 months		
Two years		
Three years		
Four years		
Five years		

Question 28: If yes to Q25, list (in order of priority by number of incidents) for what crimes (no more than ten crimes to be listed)?

1.	6.
2.	7.
3.	8.
4.	9.
5.	10.

Question 29: In the listed cases above were any of the perpetrators arrested?

Yes		No	
-----	--	----	--

Question 30: If yes, how many (in the time periods below) arrests were made?

Period of time	'X'	(Estimated) Number of cases
Six months		
12 months		
Two years		
Three years		
Four years		
Five years		

Question 31: In any of the above were there any successful prosecutions?

Yes		No	
-----	--	----	--

Question 32: If yes, how many successful prosecutions occurred (in the time periods below)

Period of time	'X'	(Estimated) Number of cases
Six months		
12 months		
Two years		
Three years		
Four years		
Five years		

Question 33: On what activity/action was success most dependent? (e.g. utilisation of CCTV footage of an incident (for identification purposes; evidentiary use in court); rapid response and arrest; further crime investigation)? (List in order of most valuable/successful activity)

1.	6.
2.	7.
3.	8.
4.	9.
5.	10.

Question 34: If yes to any of Qs 25-29 for what type of crimes has it assisted most successfully to either solve/successfully prosecute (list below types of crimes in order of priority by incidence numbers)?

1.	6.
2.	7.
3.	8.
4.	9.
5.	10.

Question 35: In your opinion does the utilisation of CCTV surveillance have any value/ impact/effect on crime prevention initiatives?

Yes		No	
-----	--	----	--

Question 36: If yes, describe in what way?

--

Question 37: If no, say why it is of no value/impact on crime prevention?

--

Question 38: In your opinion how can the utilisation of CCTV surveillance be improved for better/more effective crime prevention?

--

Question 39: Is there any additional relevant information you want to provide with reference to the utilisation and effectiveness of CCTV Surveillance in crime prevention?

--

**THANK YOU FOR YOUR TIME AND PATIENCE IN PARTICIPATING
IN THIS RESEARCH STUDY**

Annexure H: Schedule of Interview Questions: CPFs and Residential Areas:
CCTV Surveillance Operations

INTERVIEW SURVEY QUESTIONNAIRE

CPFs & RESIDENTIAL AREAS: CCTV SURVEILLANCE OPERATIONS

RESEARCH PROJECT TITLE:

*Evaluating the use of CCTV surveillance systems for crime control and prevention:
Selected areas in Johannesburg and Tshwane, Gauteng*

This interview survey questionnaire is aimed at determining your knowledge and attitudes/opinion about **CCTV surveillance camera operations in your CPF residential area.**

INSTRUCTIONS:

You are requested to answer each question and reflect your true reaction when doing so. Please answer the following questions as honestly as possible. You do not need to identify yourself and, similarly, the researcher will uphold your anonymity in that there will be no possibility of any respondent being identified or linked in any way in the research findings by name or otherwise in the final research report (nor the company/organisation for which you work).

Where required, please indicate your answer with a cross (X) in the appropriate box or write a response in the space provided.

Do not dwell too long on each question and please complete ALL questions.

NB: There are no wrong answers.

SECTION A: BIOGRAPHICAL INFORMATION

Question 1: Gender

Gender	(X)		(X)
Male		Female	

Question 2: Age

Age	(X)	Age	(X)	Age	(X)
20-24 years old		25-29		30-34	
35-39		40-44		45-49	
50-54		55-59		60+	

Question 3: Highest educational qualification

Highest educational qualification	(X)		(X)
Standard 8/Grade 10		BA degree	
Standard 9/Grade 11		BTech	
Standard 10/Grade 12		Advanced Diploma	
Certificate Level NQF 3-4		Hons/Postgraduate Diploma	
Certificate Level NQF 5		Masters	
1-year Diploma		Doctoral	
3-year Diploma		Other (specify):	

SECTION B: CCTV SURVEILLANCE OPERATIONS

Question 4: When were CCTV surveillance cameras installed in your neighbourhood/residential area (month/year date)

--

Question 5: Where in your neighbourhood/residential area have CCTV surveillance cameras been installed? (indicate all sites not just primary)?

CCTV installed site	(X)
1. Shopping centre/mall	
2. Central Business District (CBD)	
3. Business premises	
4. Factory/industrial site	
5. Residential neighbourhood entrance	
6. Gated neighbourhood	
7. (Private) Security estate	
8. On private residential property	
9. On public streets	
10. Along highways	
11. Other (specify)	

Question 6: If 'public space' (streets/entrance to neighbourhood) (as opposed to on private/business/commercial property) has been indicated above what was the motivation/reason provided for its (CCTV Camera Surveillance System) installation in such public areas?

--

Question 7: If installed in 'public space' (streets/entrance to neighbourhood) who was responsible for deciding on its installation?

--

Question 8: Were you in agreement with the decision to install?

Yes		No	
-----	--	----	--

Question 9: If yes, what were your primary reasons for wanting its installation?

--

Question 10: If no, what were your reasons for not agreeing with installation?

--

Question 11: Do you have any concerns about issues of 'invasion of privacy' with the installation of CCTV cameras in your neighbourhood?

Yes		No	
-----	--	----	--

Question 12: If yes, what are those concerns?

--

Question 13: If installed in 'public space' who funded its initial installation costs?

--

Question 14: How is it currently funded? (Residents private security company contract/Private Security Company/Not-for-Profit Co./Business Levy, or combination (indicate), etc.)

--

Question 15: Which private security company manages/operates them?

--

Question 16: If not a private security company, who/which organisation manages its operations?

--

Question 17: Do you know how many cameras have been installed in the 'public spaces' in your neighbourhood?

Question 18: Is the system operated 24/7?

Question 19: By whom?

Question 20: Who is the primary (first) responder to a CCTV activation/observation of criminal activity in your area?

Question 21: For how long are the video recordings (images kept/stored) before being deleted?

Question 22: After installation did you notice a reduction in crime in your area?

Question 23: If yes, for which crimes? (list in order of priority - only five)

1.
2.
3.
4.
5.

Question 24: What do you think are the crime reduction/prevention value/benefits of installed CCTV surveillance cameras? (If your opinion none indicate so as well).

Question 25: Can you think of any ways of improving the use and utilising of the installed CCTV surveillance cameras for crime reduction/prevention?

--

Question 26: After installation of the CCTV system in your neighbourhood did you feel safer and more secure?

Yes		No	
-----	--	----	--

Question 27: If no, why did/do you feel unsafe and insecure?

--

Question 28: To the best of your knowledge, did the installation of CCTV surveillance system lead to any direct successes against criminals?

--

Question 29: If yes, what crimes were detected with the assistance of the CCTV Surveillance System? (List in order of priority only five)

<ol style="list-style-type: none"> 1. 2. 3. 4. 5. 	
--	--

Question 30: If yes, what were those successes emanating from the detection of those crimes? (e.g. reduction in crime trends/statistics/arrests/prevention of crime/prosecution/convictions)

--

Question 31: Can you quantify any of those successes over the past:

No of years	No of successes		No of successes
12 months		One year	
Two years		Three years	
Four years		Five years	

Question 32: In your opinion how can the utilisation of CCTV surveillance camera systems be improved for better/more effective crime prevention?

Question 33: Is there any additional relevant information you want to provide with reference to the utilisation and effectiveness of CCTV Surveillance in crime prevention?

**THANK YOU FOR YOUR TIME AND PATIENCE IN PARTICIPATING
IN THIS RESEARCH STUDY**

Annexure I: Street Survey Questionnaire

QUESTIONNAIRE SURVEY SHEET

RESEARCH PROJECT TITLE:

*Evaluating the use of CCTV surveillance systems for crime control and prevention:
Selected areas in Johannesburg and Tshwane, Gauteng*

STREET SURVEY: CBD/OPEN STREET CCTV SURVEILLANCE SYSTEMS PUBLIC AWARENESS

Researcher's initials		<u>Questionnaire No.</u>		<u>Date</u>		<u>TIME</u>	
CBD (X)	PTA	JHB	Other:	Comments:			
Public street area (x)							

Bibliographic Info (Don't ask Qs 1 & 3 - fill in after interview)

1. Gender?	Male	Female	2. Age?	<20	20-29	30-39	40-49	50-59	60>
3. Race?	Black	Asian (Indian)	Coloured	White					
4. Are you a resident of or a visitor to this city?	Resident		Visitor		<i>If a visitor abort interview</i>				
5. South African/Non-South African (Foreigner)? [but still a resident of this city]	South African		Non-SA resident						
6. Do you live in or close to the CBD area or in the suburbs/ a township/out-of-town (rural)?	CBD		Suburbs		Township		Rural		
7. Do you know about or are aware that a CCTV surveillance system (security cameras) has been implemented (installed) in this CBD//public street area?	Yes		No		<i>If 'No' skip to A1</i>				
8. If yes (Q7), do you know when (year) it was installed in this CBD//public street area? [guess]									
8(a) Do you know how many cameras are currently installed in this CBD/city centre/public street area? [Try and get an estimate in numbers from respondent]							Yes	No	Num
9. Have you ever seen any of these cameras (i.e. identified them as cameras and where they are sited - do you know what the surveillance cameras look like)? [Get respondent to point one out]							Yes	No	
							Yes	No	

10. Are there any signs in this CBD/public street area indicating that CCTV cameras have been installed and/or the public is under camera surveillance?							
11. Do you know where the CCTV Operations Control Room for this CBD/public street area system is sited? <i>[If 'yes' ask for a building and/or street name where sited or point building out]</i>						Yes	No
<i>Building and/or street name:</i>							
12. What do you think was/is the main reason for the installation of CCTV surveillance in this CBD/public street area?							
13. In the last two years have you been a victim of crime (personally experienced a crime situation) in this CBD//public street area?						Yes	No
14. If yes, did the CCTV surveillance came to your aid/assistance or was of any help? <i>[reporting of; response to; use as digital evidence in court]</i>							
15. Do you think the CCTV surveillance system has had any impact on reducing crime in this CBD area?				Yes	No	<i>If 'No' go to Q16 but skip Q17</i>	
16. If no, could you please say why you think there has been no reduction in crime in this area?							
If yes, against which crimes do you think the CCTV surveillance system has had the most success? (number in order of priority)							
<i>Mugging</i>	<i>Pick-pocketing</i>	<i>Theft (stealing without a weapon)</i>	<i>Smash & grab at traffic lights</i>	<i>Street robberies (weapon used)</i>	<i>Armed robberies of business</i>		
<i>Rape/sexual assault</i>	<i>Vandalism</i>	<i>Theft out of vehicles</i>	<i>Theft of vehicles</i>	<i>Vehicle hijacking</i>	<i>Prostitution</i>		
<i>Assault GBH</i>	<i>Murder</i>	<i>Attempted murder</i>	<i>Other: (specify)</i>				
17. Knowing there is a CCTV surveillance system (cameras installed) in this CBD/public street area, do you feel safer when coming into this CBD/city centre/public street area?							
i) During the daytime?		Yes	No	ii) At night?		Yes	No
18. If no to either i) or ii) please give reasons for your feelings of being unsafe in this CBD/public street area							
19. Would you approve of the CCTV surveillance system in this CBD/public street area being expanded to:							
i) Other CBDs in this metropolitan area and linked to a Central Control Room?						Yes	No
ii) To the suburbs?		Yes	No	iii) To the townships?		Yes	No

iv) Other (specify):
20. Who do you think funds (pays for/comes off their budget) the operations of this CBD/public street area CCTV surveillance system? [Taxpayers is not the correct answer – probe for actual agency/dept.]
21. Who do you think operates the actual system? [Private co./ municipality/ police/combination of?]
22. Besides crime reduction can you think of any other uses for this CBD CCTV surveillance system?
23. What are your thoughts on CCTV as a tool for crime prevention and control?
24. Do you have any suggestions/recommendations for improving of the current CCTV surveillance system in this CBD?
25. Can you describe an experience you have had where the footage from CCTV influenced crime?
26. In your opinion, is there any part of CCTV process that can be improved upon?

Thank you for your time and co-operation in participating in this research survey