“CONSTRUCTING THE CRIMINAL: AN EXPLORATION OF POLICE PRACTITIONERS' UNDERSTANDINGS OF THE USE OF TELECOMMUNICATONS DATA IN CRIMINAL INVESTIGATIONS”.

Nicola Moffat

This dissertation is submitted in part-fulfilment for the degree of

Master of Science in Criminology and Criminal Justice

at the University of Glasgow

September 2012

Abstract

This dissertation examines telecommunications within criminal investigations in the hope that a comprehensive understanding of its use can be determined. Drawing on the findings of an empirical study of police practitioners as well as the key themes taken from a number of library based sources, this study attempts to investigate how telecommunications are shaping current and future policing investigations.

In efforts to directly address the distinct lack of any available literature or published research involving the use of telecommunications within a criminal investigation setting the study strives to gain a greater knowledge, at 'grass roots level', of the methodologies used, the practitioners involved and the challenges presented in the delivery of this investigative tactic.

Despite its significant contribution to major criminal investigation this study highlights the key dangers from emerging telecommunications technology and the doubts cast over its future use within such a setting given the shortcomings of law enforcement to adapt and respond to these developments.

Contents

Acknowledgments

I wish to thank my family and friends for supporting me throughout this degree. In particular my husband Barrie who has endured the tears, tantrums and long hours that have came with this project. I also express my thanks to my friend Kirsty Webster who has provided endless practical support.

I am especially grateful to Colin Atkinson for his guidance and encouragement throughout my two year study and indeed in the research and writing of this dissertation. His expert knowledge and support has been outstanding and I would not have survived without it.

Finally to my unborn son, who has lived and breathed this dissertation with me albeit not in the living world. His gentle kicks have encouraged me to press on and complete this study prior to his much longed for arrival.

Dedication

This dissertation and indeed my post graduate studies have been inspired by my late grandfather James Mallon who always encouraged me to strive to do better in the field of academia. It is to him, that I dedicate this dissertation.

Table of Figures

Chapter 1 | Introduction

On 15th March 2012, 49 year old David Gilroy from Edinburgh was found guilty of killing his ex-girlfriend and work colleague Suzanne Pilley. This was a rare case in which detectives were unable to find a body or any forensic evidence providing he committed the murder. The basis of this conviction rested on a mass of circumstantial evidence which convinced the jury of Gilroy's guilt. Part of this evidence centred on Gilroy's use of telecommunications leading up to and after Pilley's disappearance where it was established that Gilroy had bombarded her with 400 text and voicemail messages in the month before she went missing. Despite the fact that Pilley's phone was never recovered, the content of some of these voice calls was retrieved from the communications service provider and played to the jury. In these calls Gilroy was heard to leave pleading messages asking Pilley to return his calls. The single most important element of this pattern of communication was that all contact ceased immediately after Pilley vanished (*The Guardian*, 15/03/12).

On 4th May 2011, the morning of Pilley's disappearance, after making her way to the city centre office she shared with Gilroy in Thistle Street, Edinburgh, police were able to place Pilley only yards from her workplace by checking the positioning of her mobile phone via satellite following a text message she sent to her father just before arriving at work. Her location at this time was later corroborated by CCTV footage. This physically located her within close proximity to Gilroy who was already in the office premises (*The Herald Scotland*, 15/03/12).

Police discovered that on 5th May 2011 Gilroy had travelled by car to the Argyll area for a work trip. Subsequent telecommunications enquiries found that during this journey, Gilroy's mobile phone had been switched off between Stirling and Inverary and the same on the way back. (*The Herald Scotland*, 03/03/12). This highlighted a course of conduct that raised suspicions around Gilroy's activities and which led police to conclude that he had deliberately switched his phone off to conceal his movements while he conducted reconnaissance for a site to dispose of Pilley's body. He repeated this on the way back when it is assessed he buried the body. Further enquires around the timing of his journey and the physical condition of the undercarriage of his vehicle after the trip corroborated this theory (*BBC News* 18/04/12).

Following his conviction, Stephen McGowan, the district Procurator Fiscal for Edinburgh highlighted the significance of the 'electronic footprint' of our everyday routine and how CCTV footage, mobile phone records, e-mails and shop receipts all contribute to tracking our movements in the smallest of detail. He stated that the course of conduct displayed by Gilroy through the examination of these physical pieces of evidence had a particular significance which helped to demonstrate to the jury that Gilroy was in a jealous and possessive state of mind and that these actions both before and after her disappearance showed that Pilley had been murdered by him (*The Guardian*, 15/03/12).

The Piley case highlighted above clearly displays the contribution telecommunications can bring to a law enforcement setting. This chapter will describe the emergence of modern telecommunications in society and more significantly its increasing use within criminal investigations. It will examine the appeal telecommunications data can have within such an environment highlighting the notable advantages such technology brings to modern day Police investigations.

1.1 | The Growth of Telecommunications in Society

Our use of telecommunications has become a central element of modern life, shaping peoples behaviours, social interactions and in many cases their criminal activities. The public outcry at the recent outage of O2 services (the UK's second largest mobile network provider) which left approximately seven million people unable to make calls, send messages or e-mails for a twenty four hour period in July 2012 was testament to the reliance we now place on mobile phones and highlighted how digitally dependent we as a nation have become. Indeed Jewkes and Yar (2010:42) acknowledge that, 'it is now difficult to deny that the development of networked computer technologies has brought about a transformation in how we communicate and consume, work and play, and engage with others across the spheres of economic, political, cultural and social life'.

1.2| Telecommunications in Law Enforcement

Whether it is the workings of a serious organised crime group or the spontaneous reaction to a crime of murder, it is widely recognised within the field of law enforcement that to undertake effective criminal activity, criminals will need to communicate (Kavanagh[1], 2012; May[2], 2012; Koops, 1999). Ultimately, this will be achieved through the medium of landline and or mobile phone communication as well as a whole host of other emerging technologies (Broadhurst, 2006; Shelly, 2003). Whether facilitating criminal activity or through the physical presence of a phone device when crime occurs this telecommunications footprint creates an additional investigative line of enquiry which police can use to assist in the disruption or detection of those individuals responsible in such crimes.

[1] Stephen Kavanagh, Deputy Assistant Commissioner of the Metropolitan Police (2011 – Present)
[2] Theresa May, UK Home Secretary (2010 – Present)

The investigation into the murder of Suzanne Pilley is not unique in its use of telecommunications as an effective investigative tool. Over the past decade, law enforcement has been turning to mobile call data for crucial evidence in many criminal proceedings. A snapshot analysis of associated UK media coverage reveals an increasing number of reporting around telecommunications related investigation as is highlighted in the news headlines overleaf:

> *'Kevin Carroll trial hears of phone link to murder scene'* (STV News, 30/04/12)
>
> *''Gerbil' murder trial: Trial hears phone evidence'* (Scotsman, 01/05/12)
>
> *'Text messages examined in Danielle murder case (*BBC News, 14/11/02)
>
> *'Soham trial: 'Crucial' phone evidence. Evidence gleaned from mobile phones and landlines will be central to the Soham murder trial, according to the prosecution'* (BBC News, 06/11/03)

This investigative technique is not reserved solely for more commonly reported areas of crime such as murder. Since 9/11 we have also seen its continual use within the area of terrorist investigation (May, 2012: Foreword). In the aftermath of the London terrorist attacks in July 2005, law enforcement and security service personnel were able to bring to light new details about the bombers including new material about the planning of the attacks from detailed analysis of their telecommunications. Such investigation revealed that the four bombers used fifteen 'operational' phones between them for attack planning and logistics. Each also had a personal mobile. These were changed regularly (three or four times) in the months leading up to attacks, and were used exclusively to communicate with each other. (Brigs *et al*, 2011).

It is therefore not difficult to see why such telecommunications and in particular mobile phone data is so appealing. Mobile devices themselves hold a wealth of personal information from contact lists and call history to text messages and location data all of which can be easily accessed with the right software and in accordance with the appropriate legislation. With the introduction of 'smart' phones there is now a significantly greater amount of data available such as digital photographs, e-mails and videos. This increasing capability allows users to communicate, access the internet, connect to social networks, exchange photographs, consume video and audio, and much more, all of which combine to provide the user with a compact, handheld personal computer (Ofcom, 2011). In utilising its diverse functionality, the device generates records of this activity and thus provides a rich source of evidence about the people that use them.

One notable advantage for law enforcement is that, 'no other computing device is as personal as the mobile phone. Whereas computers, laptops, servers, and game machines might have many users, in the vast majority of cases, mobile devices generally belong to an individual (Casey and Turnball, 2011:1). This unique and almost exclusive personal storage facility can therefore assist in providing vital information to investigations revealing whom an individual has been in contact with, what they have been communicating about and where they have been'(Casey and Turnball, 2011:1). In May 2012, whilst promoting the introduction of new computer software to assist in telecoms investigations, Stephen Kavanagh, Deputy Assistant Commissioner of the Metropolitan Police highlighted the advantages that this rapid development of mobile computing and communication technology has created,

> "Mobile phones and other devices are increasingly being used in all levels of criminal activity. The ability to act on 'forensically sound', time-critical

> information from SMS[3] to images on a mobile device quickly gives us an advantage in combating crime, notably in terms of identifying people of interest more quickly and progressing cases more efficiently".
>
> *(The Guardian Online, 2012)*

The cases and comments referred to above provide an insight into the emerging significance of telecommunications data within such settings and the key role it plays in providing a rich source of evidence within criminal investigations. Innes (2003: Preface) has argued that few areas of policing are subject to as much scrutiny as the work that is conducted on major criminal investigations. Stories on television, in the press, and in literature serve as an almost constant reminder that the investigation of serious crime remains a key component of the police function. It is important to note that what sits behind this seemingly simple capture of mobile phone evidence, is a complex and detailed policing framework, supported by tight legislation, significant specialist knowledge, considerable resource allocation and a number of key challenges for law enforcement most notably concerning the future availability and accessibility of such data due to the rapid growth of this technology (Home Office, 2012).

Despite this, the use of telecommunications within criminal investigations is notably under reported and largely under researched. With its increasing prominence and considerable contribution to policing it is therefore appropriate that this area of policing practice be explored further to inform academic understanding and address current gaps in our knowledge.

This dissertation will provide an exploratory study that seeks to understand the practices, thought processes and procedures utilised by detectives and other police practitioners when utilising telecoms data within major investigations. In focusing on this topic it will touch on

[3] SMS – Short Message Service, commonly referred to as a Text Message.

a wide range of issues drawn from the disciplines of criminal investigation, criminal intelligence analysis and the communications industry in an attempt to provide a comprehensive account of the role telecommunications play in criminal investigations. In doing so, this dissertation will address three key areas:

- What significance do law enforcement currently place on the use of telecommunications data within major criminal investigations?
- Are the correct people and practices in place to effectively drive telecommunications investigations within law enforcement?
- Does law enforcement have the capability and capacity to respond to the rapidly changing advances in communication technology?

Given the explosion of the use of mobile telecommunications in the last ten years, this dissertation will therefore look to address the question as to whether law enforcement's current and future response to such technology within an investigative context is fit for purpose.

Chapter 2 |Methodology

As has been mentioned in chapter one, despite its growing significance within criminal investigations the use of telecommunications is vastly under researched with little written on this topic other than what is disclosed during public court proceedings and subsequently disseminated through the media. Although there is vast academic literature available on the policing of criminal investigations and indeed the impact the digital age has had on law enforcement, this specific investigative tactic is vacant from such social research and therefore a considerable knowledge gap exists. As the use of telecommunications data becomes increasingly prominent in major police investigations, commanding significant

resources, it is important that this practice be investigated to probe police practitioners appreciation of the use of telecommunications in criminal investigations, to examine factors governing its collection and interpretation and to assess its potential effectiveness as a developing police practice.

Based on this dearth of available information it was considered that data sourced direct from participants in the field would be the most favourable option in establishing an authentic understanding of this policing area. This chapter will explore the methodologies used in adopting this qualitative research approach providing a detailed account of the practices utilised in terms of primary and secondary data collection, participant selection, and data analysis.

2.1 |Qualitative Research Approach

As is the case in most fields of social research, the use of qualitative methods is a second choice in criminology. With its distinctive epistemological and ontological position, quantitative research has been the dominant strategy for conducting social research emphasising quantification in the collection and analysis of data and entailing a deductive approach to the relationship between theory and research (Bryman, 2004: 19). Despite the prominent focus upon quantitative methods, qualitative research has had a long and distinguished history in the social sciences, arising in part from the limitations of quantitative approaches (Noaks and Wincup, 2004: 3). Qualitative research is a form of social enquiry that seeks to understand the social reality of individuals, groups and cultures. By using qualitative approaches to explore the behaviour, perspectives and feelings of people we can make sense of their experiences and the world in which they live. Despite some who argue that qualitative research is not scientific (Dantzker and Hunter, 2006) it does provide ‘rich

and detailed data and claims to describe life-worlds 'from the inside out', from the point of view of the people who participate' (Flick et al, 2004:3).

It is for the reasons above that this research study employed qualitative methods. The lack of any formal requirement by law enforcement to disclose official figures on the use of telecommunications data leaves no opportunity for the analysis and interpretation of available statistics. Furthermore, it is assessed that, qualitative research which refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things' (Berg, 2007:3) will get to the heart of this undisclosed issue providing passionate, and emotive accounts of how telecommunications is actually used. This approach, will provide a depth of understanding of the social aspects of how crime is constructed, offering an insight into how those agents and organisations that are tasked to respond to such crime operate within a culturally grounded context (Tewksbury, 2009:39). The data collection for this project has been developed through both primary and secondary research methodologies.

2.2 | Primary Data Collection

Primary research, in the form of in-depth interviews has been used in this project for two distinct reasons. Firstly, academic or public sector research in the field of telecommunications within criminal investigations is very limited and no empirical studies are available on this specific topic. This has placed significant limitations on the availability of appropriate literature, making it difficult to draw upon a sound foundation of already existing knowledge. Secondly, my current employment as a Criminal Intelligence Analyst within Strathclyde Police has assisted with negotiating access to this field. Most significantly, it has allowed for access to a number of relevant research participants including Senior Investigating Officers and Criminal Intelligence Analysts working within the area of criminal investigation, who are

exposed to telecommunications data on a routine basis. It is anticipated therefore that this primary research has generated new raw data on a hitherto under-reported topic.

In conducting a series of six qualitative in-depth, face-to-face, one-to-one interviews and by adopting strategies of observation, questioning and listening it has been possible to familiarise oneself with the 'real' world of the participants. This has generated ideas and descriptions of a culture that is relatively undisclosed. Such an approach, as Hammersley and Atkinson (1995: 36) argue, provides an in-sight into how such individuals construct perspectives around people and situations linked to criminality. Such qualitative methodology therefore, works on the premise that individuals are best placed to describe situations and opinions in their own words, thus providing the researcher with an understanding of how participants make sense of their own behaviour and the rules that govern their actions.

As a current Strathclyde Police employee, already immersed and intimately aware of the working practices with a major criminal investigation setting, it has been important to exercise self-reflexivity during primary research, to ensure that important issues are not missed or that nothing is taken for granted. Despite this relative removal from my normal 'native' status, familiarity within the environment has offered a number of advantages. Ease of access to a variety of suitable participants has allowed for a diverse range of informants to initially become engaged in the project within a relatively short timescale. This has been achieved by exploiting existing informal networks providing a flexible approach to research and which has expedited the research process. Notwithstanding, in support of Wolfgang's (1981) position, informed consent has been sought for each active participant summarised in a consent form (Appendix A) and agreed and signed by each to explain as fully as possible, and in terms meaningful to participants, what the research is about, who is undertaking it and why it is being undertaken, and how any research findings are to be disseminated (British Society of Criminology, 2006). 'Informed consent is a key principle in social research ethics.

It implies that prospective research participants should be given as much information as might be needed to make an informed decision about whether or not they wish to participate in a study' (Bryman, 2004: 540)

Familiarity with the participants has also been beneficial in conducting semi-structured interviews, allowing participants to provide detailed and in-depth answers to the questions asked (Bryman, 2008). This style of approach has allowed for improvisation and prompting on the part of the interviewer and offers more opportunity for dialogue between the interviewer and interviewee (Noaks and Wincup, 2004:70). Interview questions were shaped against a backdrop of literature review surrounding policing techniques within criminal investigations and the fast developing communications industry. This allowed for clarity, focus and relevance during the interview process. The questioning took on three broad themes, criminal investigations; constructing the criminal – the art of interpreting telecoms data; and the current and emerging communications landscape within a criminal context. These themes emerged firstly from the literature review in terms of the significance and scrutiny placed on major criminal investigations as a key component in the police function and secondly in attempts to directly address the distinct lack of any available literature or published research involving the use of telecoms within such a setting.

A prior working relationship with the participants has provided an initial level of trust between researcher and informant and has facilitated disclosure to ensure the collection of volumes of rich, high quality, in-depth data. With an already established level of credibility and acceptability a key informant emerged from the interviewees who facilitated further access to additional sources of data and personnel. That said, the prior association and subsequent level of trust has required a more vigilant approach to the issue of confidentiality. As members of the same organisation an expectation existed from participants that certain disclosures made during the course of the interviews would not be disseminated or published

for the purposes of this project. This issue is not exclusive to the situation presented here and indeed the question of protecting the identity of the individuals and or organisational settings is a recurring issue in criminological and criminal justice research whereby assurances regarding confidentiality are important (Noaks and Wincup, 2004:83). Researchers should strive to protect the rights of those they study, their interests, sensitivities and privacy (British Society of Criminology, 2006) and in this instance this was heightened due to the information being disclosed more freely to the researcher. Anonymity was applied to specific details of ongoing cases disclosed and covert tactics highlighted or alluded to through the interviews were omitted from the final research data. It is noteworthy that qualitative data is as subject as quantitative data to the requirements of the Data Protection Act 1998 and it is the responsibility of the interviewer to ensure that data is adequately protected (Noaks and Wincup, 2004:85).

As Noaks and Wincup also highlight (2004: 98), a significant factor in any interview is the location. Due to all of the respondents being senior law enforcement personnel at the rank of Superintendent or above and analysts, all of which were based within office environments within Strathclyde Police, there were no real factors to consider in terms of researcher safety and exposure to dangerous situations or locations. All interviews were conducted within private offices or meeting rooms within a variety of police Stations throughout Strathclyde, the dates, times and venues for which were mutually agreed and organised by the researcher, from the vantage point of having ready access to these locations. All interviews were recorded using a tape recording device and subsequently transcribed. Transcribing interviews can be a long, labour intensive process (Flick et al, 2004:151) and this was a key factor in limiting the sample to only six interview participants.

Despite the recognised limitations of such a limited sample size in terms of both numbers and representation from other forces, such ready access to gather data from Strathclyde Police

represented too good an opportunity to miss and so a deliberate convenience sample was used. ‘A convenience sample is one that is simply available to the researcher by virtue of its accessibility’ (Bryman, 2004: 100). Through this convenience sampling approach, every effort was taken to ensure a diverse and varied sample was selected. This non probability sample was achieved through careful selection of respondents who were chosen on the basis of their ‘straight talking’ approach, vast experience and confidence in the area of criminal investigation and in the specific line of questioning adopted which covered context already known but sought to ensure the social actor’s viewpoint and not one’s own perspective. Other sampling approaches were considered such as snowballing whereby ‘the researcher makes initial contact with a small group of people who are relevant to the research topic and then uses these to establish contact with others’ (Bryman, 2004: 100). However this was discounted due to time restraints and my existing knowledge of police practitioner’s expertise and knowledge in this field which allowed me to target the most appropriate participants first time round. Notwithstanding, during the course of the interviews unintentional snowballing sampling occurred whereby those selected for interview provided contact details and access to others who held additional, more specific knowledge in particular areas of telecommunications investigation.

Despite the many advantages to be gained from face-to-face interviews it is important to be mindful of the pitfalls and limitations of this research method. Interview data is often compelling; it can carry a certain degree of emotion and appeal to us because of its human character (Gillham, 2005: 8) and this was evident in the passionate and frank accounts provided by a number of the more experienced SIOs in the interview sample. As a result, it has been important to consider the data responsibly and use it in an even handed fashion. In addition, ‘most ‘close in’ qualitative research comes up against the generalisation problem’ (Gillham, 2005: 42). ‘Despite the fact that such sampling approaches used in this method will

not allow for definitive findings to be generated, due to issues of generalisation, it can provide a springboard for further research to allow links to be forged with existing findings in an area' (Bryman, 2004: 100).

Although it may be argued that by only using Strathclyde Police personnel and a fairly limited sample size it may not be representative of the opinions, understandings, interpretations and working practices of criminal investigator's use of telecommunications throughout Scotland as a whole, it is anticipated that this will offer useful insights given Strathclyde's experience in this area and provides a useful basis for further research in other Forces or in shaping future policing practices following police reform and the formation of a single Scottish Police Service in April 2013. The Force's experience in dealing with major criminal investigations far outweighs that of any other force in the country. For example, crime statistics indicate that since 2001 Strathclyde Police has conducted more criminal investigations into the instance of murder than any other Force in Scotland. In 2010/11, the homicide rate for Strathclyde represented 64% of the overall Scottish homicides (Scottish Government, 2011).

2.3 | Secondary Data Collection

Secondary sources have also been used in this research project, particularly in relation to gaining an understanding of the telecommunications sector as a whole and in particular the phenomenal social impact such advances in technology have had on human behaviours and social interaction. Furthermore, examining and evaluating policing journals, practical policing manuals, news reports and academic texts in respect of criminal investigations in a wider context has allowed for an analysis of how telecommunications data in investigative work contributes to the social construction of meaning within this setting.

Secondary analysis offers numerous benefits not least in many instances the data sets that are employed most frequently are of extremely high quality having undergone rigorous sampling procedures. In addition the geographical spread of the sample size is often on a national scale covering a wide variety of regions of the United Kingdom not widely accessible to the researcher. Furthermore many data sets have been generated by highly experienced researchers or research organisations with a proven track record in social research (Bryman, 2004: 202).

The internet has been a valuable research tool in conducting secondary research for this project and as Hewson *et al*, argue, 'using the internet to locate secondary sources can have great pedagogical value' (Hewson *et al*, 2003: 1). Facilitating access to information on an international scale, it is easily accessible, vast in terms of volume and is relatively cost effective (Noaks and Wincup, 2004). It has provided access to current information disclosed by commercial communications companies such as O2 and Vodaphone from their authoritative websites as well as providing up-to-date news and findings from market research conducted by Ofcom the independent regulator and competition authority for the UK communications industries.

However, despite the many advantages of secondary research, drawbacks must also be considered. 'To a certain extent there will be a lack of familiarity with the information provided and a period of familiarisation may be required to ensure an understanding of the organisation of the data' (Bryman, 2004: 205). More significantly however is the researcher's lack of control over the quality of the data and as such this method of research was approached with caution.

2.4 | Data Analysis

One of the main difficulties with qualitative research is that it very rapidly generates an extensive and dense layer of data due to its reliance on prose in the form of field notes, and interview transcripts. Furthermore, 'there are few well established, widely acceptable; rules for the analysis of qualitative data' (Bryman, 2004: 399). Miles (1979) has described qualitative data as an 'attractive nuisance' because of the attractiveness of its richness but the difficulty of finding analytic paths through that richness.

The framework used to guide the analysis of data within this project is shaped by a grounded theory approach whereby it has been important to allow the theoretical ideas to emerge out of one's data. Grounded theory has been defined as 'theory derived from data, systematically generated and analysed through the research process' (Bryman, 2004: 401). In this method, 'data collection, analysis, and eventual theory stand in close relationship to one another' (Strauss and Corbin, 1998: 12). This iterative process has resulted in an interplay between the collection and analysis of data whereby as themes have developed from initial interviews, these have been explored and exploited in subsequent interviews and data collection to formulate hypotheses based on conceptual ideas.

In explaining this methodology further it is important to draw on the tools used in this grounded theory approach. A system of coding has been applied to the data whereby information taken from the interview transcripts has been broken down into component parts and given labels or themes. 'Coding is one of the most central processes in grounded theory. It entails reviewing transcripts and or field notes and giving labels to component parts that seem to be of potential theoretical significance and or that appear to be particularly salient within the social worlds of those being studied' (Bryman, 2004: 402). From this process of coding a succession of concepts has developed that have ultimately been used as building blocks to shape the key themes emerging from the data. A breakdown of these themes and concepts is described in Figure one below.

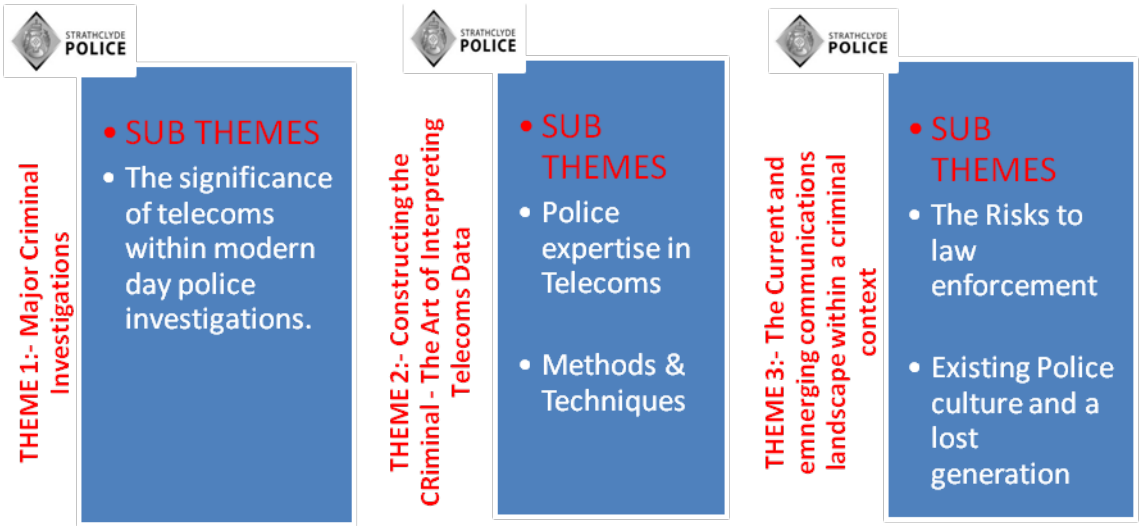

Figure One: Themes /Sub Themes from Data Analysis

In spite of the frequency with which it is cited, grounded theory is not without its limitations. There are practical difficulties in terms of the time taken to transcribe recordings of interviews which can create difficulties for researchers to carry out a genuine grounded theory analysis with its constant interplay of data collection and conceptualisation (Bryman 2004:407). One of the main criticisms however is that the fragmentation of data from the coding process may in some instances result in a loss of a sense of context and of narrative flow and as a result it is often difficult to see what theory, in the sense of an explanation, is being put forward (Flick et al (eds.), 2004: 274).

Nonetheless, for the purpose of this research project grounded theory has proved the most influential strategy for conducting qualitative data analysis. A limited timescale rendered the use of any other data analysis such as analytic induction pointless given that this would have required the researcher to seek universal explanations of phenomena in order to develop concept or ideas. A distinct lack of any other available theory, ideas or interpretations of telecommunications use within a criminal context left no other option but to look to discover the theory through the analysis of data obtained in this field.

Overall it is assessed that the methodological approach to this research project is a systematic and appropriate one that has clear practical benefit to the development of policing practice within and beyond the Strathclyde Police organisation.

Chapter 3 | Literature Review

This chapter will review the available literature on telecommunications within major criminal investigations. It will look to chart the development of this policing practice through the study of available academic research taken from a number of sources including policing journals and books specific to the area of crime investigation. Furthermore, it will review additional literature sources such as government policy documents, practical policing manuals and other open source police studies that may better inform our appreciation of this subject. Ultimately the review will seek to identify the key themes emanating from such literature identifying what areas best inform our understanding as well as highlighting where gaps in knowledge may exist.

3.1 | Academic Research

The most significant point to emerge from the review of available academic literature was that despite the vast research undertaken within the area of criminal investigation and policing practice in general, little study, if any exists specifically on the use or significance of telecommunications within a crime investigation setting.

Policing research specific to Scotland such as Donnelly et al. (eds.) (2005) could offer no local insight into this investigative technique and scrutiny of general wider policing studies such as Reiner (1992) and Newburn (2007) also offered nothing on a national scale that would improve knowledge in this area.

3.1.1 | Strengths

Policing practice and criminal investigation continue to receive much academic attention. Methods of major crime investigation continue to be researched and published on a general scale, (Innes, 2003; Newburn, 2007; Tong et al, 2009) whilst a large number focus on criminal investigations within specialised areas such as terrorism and organised crime (Levi, 2007; Clarke & Newman, 2007; Waddington, 2010; Nunn, 2003). Despite their lack of telecommunications focus, what these studies do provide is an understanding of the policing environment in which telecommunications can feature as well as an insight into the societal issues that have and are currently impacting on this policing function.

Newburn (2007: 869) states that, the policing of major criminal investigations continues to evolve. This is in part due to a changing nature of crime brought about by globalisation, and the opportunities and insecurities this has created. As a result we have seen the emergence of international organised crime and a new concept of 'international terrorism' which has 'threatened society in ways and on a scale beyond imagination' (Newburn, 2007: 869; Koops, 1999: 60).

Innes (2003: 11) highlights that, 'successful and effective detective work requires both individualised perceptual and interpretative faculties, together with knowledge of legal procedures and regulations, and a systematic approach to solving particular investigative problems'. In achieving this, criminal investigators have specialist expertise in a number of areas including interview skills, developing and managing informants, preserving and developing evidence and preparing cases for prosecution.

All of these specialist skills require a certain degree of creativity, persistence and dedication which the investigator must use in solving particular investigative problems. However as criminal investigation become more complex, the need for specialised, technical support

becomes more apparent. This is perhaps most evident in the area of forensic science which during the course of its advancement throughout the twentieth century rapidly became established as a standard yet specialised investigative technique which significantly changed the shape and conduct of major crime investigations (Innes, 2003: 84).

One further area that can be draw upon to further our understanding of telecommunications is the increasing study of advancing technology and its impact on crime. As the digital age has grown, and the exploitation of technology by criminal networks has developed, in particular the use of the internet, it is this specific area which continues to dominate research and discussion around crime and technology. Despite its generalisation and limited focus on telecommunications, many parallels can be drawn from the key themes emerging from this literature and the increasing use of telecommunications within such a setting.

The acknowledgement of technology within a criminal context has been well documented throughout academic research for well over a decade. Indeed as far back as 1998, Shelly recognised the emerging significance of new technology and its impact on the criminal landscape. She stated, ‘‘today, thanks to computer and communications technologies, crime and corruption has diversified significantly. Moreover, technology has transformed the very nature of crime itself,’ (Shelly 1998: 605). The following year, Koops had noted law enforcement’s response to this rapidly developing technology stating, ‘as the ‘information society’ has taken hold bringing with it a new wave of cybercrime, society’s answer to these new crime types has been to intensify investigation and to find new ways to combat these threats’ (Koops, 1999: 60).

By 2001, Whittle had acknowledged its importance within the field of academia and highlighted that since the explosion of the digital age, and the fundamental transformation of social relations in the wake of technological change there was a lack of solid empirical data

which necessitated ethnographic exploration (2001: 70). Consequently, since the explosion of the internet in the early 1990s, an expanding worldwide literature on technological research and debate has emerged. This subsequent study of advancing technologies has continued to shape our understanding of the changing landscape of criminality, bringing with it questions concerning the criminal use of technologies and law enforcement's response to it in the fight against crime.

The significance of technology was again raised by Shelly in 2003 when the extent to which it had taken hold within the criminal fraternity was highlighted. She stated, 'the criminal and terrorist exploitation of information technology has proceeded in tandem with its growth by the legitimate multinational community with evidence to suggest that those who seek to promote illicit ends have been as fast if not faster to introduce this technology into their operations'(Shelly, 2003: 307). In the same year, Innes recognised that as a consequence, criminal investigations and indeed many aspects of detective work had become more technical and complex (Innes, 2003: 11). In 2007, Marx further highlighted its importance stating it would be irresponsible for law enforcement not to seek benefit from the technical developments made available to the police service (Marx 2007: 50).

By 2010, technology's place within law enforcement had been firmly established with Hunton (2010:387) debating how best it should be incorporated into the investigative framework. He argued, 'as the use of networked and internet technology moves firmly into the field of general crime investigations, it will not stand alone as an investigative technique but will form part of much broader investigation practices and procedures'.

In all of these technological studies and debates, telecommunications although not mentioned specifically is clearly recognised as a strand of this technological phenomena. Although it may sit at the lower scale of technology in terms of its sophistication and complexity in

facilitating crime, its vast use and popularity make it a key technological method which, as the literature highlights is impacting greatly within the structure and practices of police investigation.

One of the main themes to be drawn from the wider research of crime and technology is an acknowledgement of the risks such technological advances bring to law enforcement. Again although not specific these challenges can be clearly aligned to the use of telecommunications within an investigative setting.

By the late 1990s as mobile telecommunications began to take hold, Shelly (1998:607) had recognised a significant area of concern around the corporate control of technology. She highlighted that the majority of telecommunications systems were in the private hands of multinational corporations where control was out with state authority. This problem was further compounded by the fact that the global information infrastructure was outside the jurisdiction of any one country and was becoming increasingly problematic as communications services from overseas providers became more available to UK customers (Shelly, 1998: 309).

Shelly, (2003: 309) also acknowledged the lack of coordinated legislation between countries as a further vulnerability that criminals would seek to exploit, emphasising that such developments would pose important challenges to governments and their law enforcement authorities and would have the potential to shift significant power to criminals. Broadhurst (2006: 409) reinforced this position by arguing that a variety of new police networks were required to be established across national borders.

Law enforcement's capability and capacity to respond to technology-related crimes has been fiercely debated over the last decade within much of the available literature. Many have identified that the pace of technological change will continue unabated with the adaptability of cyber-criminals continuing to pose challenges for law enforcement (Broadhurst, 2006: 409; Hunton, 2010: 385). In 1998 Shelly stressed the importance of the restructuring of law enforcement bodies to address high-technology crimes highlighting the need for specialists to be hired to help combat this new and advancing threat (Shelly, 1998: 618). In subsequent studies she highlighted the difficulties this created whereby law enforcement could not hire or retain the personnel needed to combat the technological knowledge gap, emphasising that IT experts chose employment in the private sector where pay and conditions were more desirable (Shelly, 2003: 305). By 2006, the picture looked no better with Broadhurst (2006: 410) arguing that many law enforcement agencies had been unable to respond effectively to cyber-crime and even in the most advanced nations, they were only 'playing catch up' with technologically aware criminals.

From this available literature we can begin to establish a picture of how technology and indeed telecommunications has proved popular within the criminal fraternity. We can note law enforcement's initial attempts to adapt and alter investigative practice to facilitate such technology and gain an understanding around the associated risks that make this transition more challenging.

3.1.2 | Weaknesses

Despite its partial insight into the role of telecommunications within criminal investigations, current academic research lacks any in-depth account of its use as an investigative tactic. There are no current, up-to-date studies to better inform our understanding of this subject and

there is no ‘local’ perspective within a Scottish policing context. What does exist is restricted to studies undertaken by a limited number of researchers captured within a broader arena of technological debate.

Furthermore, there is no real evidence of strong, ethnographic exploration that captures the people, processes and methodologies of those utilising telecommunications at a local policing level. It has therefore been a requirement of this project to look to alternative sources and expand research into non academic areas in attempts to further enhance our understanding of this subject.

3.2 | Other Literature

On a general scale our use of telecommunications within society can provide clues as to its significance within a crime investigation setting. ‘Over the last decade there has been a significant growth in communications services and the increasing time we spend using them. The findings from the Ofcom 2012 Communications Market report highlight the influence that communications technology now has on our daily lives and on the way we behave and communicate with each other’(Ofcom, 2012).

The results show that as landline subscriptions continue to drop the proportion of adults who now personally own or use a mobile phone in the United Kingdom (UK) currently sits at 92% with the average Briton now sending 50 text messages per week (Ofcom, 2012). Given its universal appeal, it is inevitable that telecommunications will play a part in the facilitation of criminal activity and the extent to which mobile telecommunications will impact on criminality cannot be underestimated.

The significance of telecommunications data in criminal investigations can be found in an expanding political discourse surrounding its current and future use by law enforcement and

within the official practices and procedures of police and intelligence agencies. It is therefore appropriate to begin by considering what the official definition for telecommunications data is within a criminal justice context. This can be found in the Home Office definition which incorporates telecommunications within the wider communications sphere:

> *'Communications data is the information about a communication. It can include the time, duration and dialling numbers of a phone call, and the location from which a mobile call is made, or the 'to' and 'from' addresses of an email. Sometimes it includes the location of the originator of the communication. It does not include the content of any communication - the text of an email or a conversation on a telephone. It is information about a communication - not the communication itself' (Home Office, 2012).*

This definition of communication works within a tight legislative framework that controls the retention and availability of such information for appropriate official use. The significance of telecommunications data and the demand for access to such information is evidenced by the fact that within the United Kingdom (UK) companies providing communications services are required by law to collect and securely store communications data for a designated period of time. 'The police and others can obtain access to such data if they can demonstrate that it is necessary and proportionate in an investigation. Access is on a case by case basis and is subject to oversight' (Home Office, 2012). The legislation that governs such practices is known as The Regulation of Investigatory Powers Act 2000 or The Regulation of Investigatory Powers Scotland Act 2000 more commonly referred to as RIPA or RIPSA. This legislation regulates the powers of public bodies to carry out surveillance and investigations and covers the accessing of communications data as well as the interception of communications.

Part 1, Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA) is the primary legislation governing the access to communications data (Kent Police, 2012). It states that 'Communications Data can originate from postal/ freight, telecommunications or internet related communications and can be accessed lawfully for a number of purposes ranging from issues of national security and in an emergency, of preventing death or damage to a person's physical or mental health to issues such as the prevention and detection of crime or preventing disorder.

Such legislative measures indicate the acknowledgment by government of the importance of such data in preventing and detecting crime. Indeed in 2012, the Home Secretary, Theresa May highlighted, 'that communications data is used by the police and the security agencies in the investigation of all crimes, including terrorism, and in addition, is routinely used as evidence to support prosecutions in court' (Home Office website 2012).

Indeed, as the demand for its use has increased, its importance has continued to be reinforced. No more so than in June 2012 when the government launched the Draft Communications Bill in attempts to adapt and enhance legislative powers in line with the diversification of the communications industry to capture the increasing data generated from a number of new communication methodologies. In doing so, the government stated, **'**For many years police and security and intelligence agencies have used communications data from landline telephones and mobiles to catch criminals and to protect the public. In doing so communications data has played a role in <u>every</u> major Security Service counter-terrorism operation over the past decade and in 95 per cent of all serious organised crime investigations' (Home Office Website, 2012).

This revealing statement gives an indication as to the extent that this policing practice is utilised throughout the UK and the significance it has in contributing to the investigation of serious areas of crime.

Despite any formal requirements for law enforcement to provide regular statistics on the use of telecommunications data, in attempts to obtain a more in-depth understanding of the extent to which telecommunication legislation is utilised in a local policing context, an examination of police disclosures resulting from Freedom of Information (FOI) requests[4] and published on individual force websites can provide some indication as to its use. Figure two below highlights responses provided from four police forces throughout the UK to a general request to provide details on the number of times each force has requested communications data under the RIPA and RIPSA legislation between 2009 and 2012:

FOI Request: - How many times has your police force requested communications data under the RIPA and RIPSA legislation in the following periods?	Avon & Somerset Constabulary	Northumbria Constabulary	Fife Constabulary	Strathclyde Police
30th April 2009 – 1st May 2010	3986	3503	587	8490
30th April 2010 – 1st May 2011	5510	2825	598	8364
30th April 2011 – 1st May 2012	8049	4319	531	8848

Figure Two: Police Access to Communications Data

As can be seen from the figures displayed, with the exception of Fife Constabulary who record a slight reduction, all of the other three forces note an increase in requests throughout 2011 – 2012 with figures peaking when comparing against the last three years. Although only a snapshot of police activity this provides some insight into the growing trend in the use of telecommunications by law enforcement, corroborating the increased media reporting of this police tactic (as highlighted in Chapter 1) and supporting the UK government's position that such data is vital to law enforcement in the prevention and detection of crime.

[4] The Freedom of Information Act gives you the right to ask any public body for all the information they have on any subject you choose subject to conditions and availability of data.

Further exploration of open source police literature also provides some insight into the use of telecommunications within criminal investigations where its use is specifically mentioned in a number of practical policing manuals dating back to the year 2000. The importance of a robust telecommunications strategy within major investigations is laid out in the ACPO 2005 Core Investigative Doctrine with regular telephone strategy meetings identified as an area of best practice in the Home Office Review of Murder Investigations (2004: 37). Both the 2009 and 2011 National Policing Improvement Agency (NPIA) Journals of Homicide and Major Incident Investigation each provide case studies where compelling mobile phone evidence has contributed to the secure convictions of those responsible. These crimes include the 2007 murder of Gerald Tobin, a motorcyclist with links to the Hells Angels, shot dead on the M40 near Warwickshire and the murder of David Daly whose body was recovered from the Birmingham main line canal in 2008. All of these references support the use of telecommunications as a vital and established standard investigative technique within law enforcement.

In terms of law enforcement personnel and specialist knowledge in the area of telecommunications, policing manuals such as those mentioned above make reference to the use of police analysts as key stakeholders in the telecommunications process, however information is limited. What can be highlighted is what appears to be the increasing use of specialists from private commercial companies to support this service. Online research shows an increasing number of companies entering the market in the last ten years offering ‘Digital Forensic Services’. A snapshot analysis of such company websites reveals a number of acknowledgments from police forces throughout the UK supporting the delivery of telecommunications related services from these companies in various cases of murder, missing persons and drug importations (Forensic Telecommunications Services, 2012; Intaforensics, 2012). Such companies offer access to the relevant equipment and the services

of experienced and qualified engineers who can not only provide the technical know-how during the investigation but can act as expert witnesses in delivering this information in a court of law.

From the available literature, some conclusions on the use and significance of telecommunications within criminal investigations can be drawn. Firstly, as a single strand of the technological phenomena that has affected crime in the last two decades, it is one that has impacted greatly on the ability of both criminals and law enforcement agencies to function more effectively. Yet despite its role in a number of successful convictions concerning serious organised crime and acts of murder, it is fair to assess that the criminal use of telecommunications has been quick to adapt to the advancing technologies of telecommunications whereas law enforcement have been unable to respond in equally as good a fashion.

Secondly from the dip sample analysed, the legislative framework which supports the access and use of telecommunications data appears to be actively utilised throughout the UK by a number of police forces on a particularly large and frequent basis and this is shown to be growing.

Thirdly, it has been identified that police analysts form a key role in the processing of telecommunications data. This appears to be augmented by the provision of digital forensic services from a growing number of private commercial companies. However the strong theme to emerge from much of the literature is the associated risks from advancing technology and the questions around law enforcements capability and capacity to respond to such changes.

Despite these notable themes emerging significant knowledge gaps remain. There is still no clear insight as to how telecommunications data is managed locally within an operational setting. There is no understanding of the thoughts and opinions of practitioners who work with this data on a daily basis or indeed any knowledge of the skills, expertise and experience of those who deliver this service. In the absence of broad academic research no conclusions can be drawn as to its true effectiveness or significance within a police investigation, if it is favoured over other policing techniques or indeed if law enforcement really has the capability and capacity to support its use.

This lack of important information renders it impossible to accurately evaluate and assess current policing practices in the area of telecommunications and thus provides justification for an empirical, rigorous and academic survey to be conducted as has been undertaken for the purposes of this project. A review of this research can be found in the following substantive findings section of this report.

Chapter 4 | Research Findings

This chapter will draw on the key themes of the research question to consider the significance, interpretation, understanding and technological issues associated with the use of telecommunications within a criminal investigation setting. Drawing on the experiences and opinions of practitioners currently in the field it will look to explore the tactics used, the people involved and the problems encountered to better inform our understanding around the use of this under-reported police tactic.

4.1 | The Significance of Telecommunications within Criminal Investigations

From the case study examples highlighted throughout this project the significance of telecommunications within police investigations is clearly evident however in what particular

circumstances of crime it is utilised and to what extent it is used has not been made clear. The following participant accounts on the specific use and significance of telecommunications within a criminal investigation setting will look to enhance this existing knowledge and where possible, address these knowledge gaps.

All of the interviewees highlighted that the primary role of telecommunications lay in either, major criminal investigations, most commonly reactive enquiries or force operations, most likely to be of a pro-active nature. All such enquiries were noted as being headed by a Senior Investigating Officer (SIO) at a rank of Detective Inspector or above and commanded the provision of additional resources and policing techniques that were above and beyond the requirements of any normal policing enquiry.

In assessing a crime to be worthy of such 'major investigation' a number of factors were found to be considered, not least the type of crime. Many interviewees were keen to point out that major investigations did not just deal with instances of murder but could involve critical incidents such as a plane crash, an abduction or a terrorist attack. It was highlighted that an assessment of the complexity and risk of the crime or incident would be undertaken and would involve the consideration of a number of factors such as the victim status, whether it was linked to serious organised crime, media and public interest and the potential threat, risk and harm to the community. In cases of homicide investigation, a further categorisation applied (Category A, B and C) in line with a UK wide law enforcement directive.

It was explained that once established as such, a key element of any major criminal investigation was the gathering of key personnel and the formation of a number of dedicated, specialist teams to support its function. 'Vast specialist resources' was a term used to describe what set major criminal investigations apart from normal everyday policing enquiries. It was highlighted that the provision of telecommunications investigation lay

within this specialist arena and was the most prominent area of policing where telecommunications featured. This supports findings from the literature review where reference to telecommunications was most commonly found in policing manuals specific to the areas of homicide and major incident investigation (NPIA Journal of Homicide and Major Incident Investigation 2009 & 2011).

The severity of the crime seemed to play some part in the request for telecommunications data being granted. This supported its prominence within major criminal investigations where crimes of a more serious nature were examined. One officer highlighted this issue,

> *"..... you might not get it (telecommunications) for another type of enquiry but you will get it for a murder because a murder is so critical that it its justified because of the serious nature of the crime under investigation"*. (SIO A)

In turning to consider the extent and significance of telecommunications within a major investigation setting, all participants reported its use within almost every case they had worked on in recent years. This supports Home Office claims, as highlighted in chapter three that communications data has played a role in 95 per cent of all serious organised crime investigations over the last decade (Home Office Website 2012). All interviewees emphasised its significance, with half describing it as 'almost' as significant as forensic evidence. The following statements provided examples of these claims,

> *"Telecoms are more likely to provide you with the evidence than other aspects of the enquiry..... every SIO will need telephony work done without a shadow of a doubt"*. (SIO A)

> *"Telecommunications are absolutely crucial to a major investigation".* (SIO C)

> *"Telecoms tell you about so many things about so many people involved in your investigation and I would argue that it is an instrumental part of any critical investigation".* (SIO B)

A deeper exploration of the reasons why telecommunications were so significant to investigations provided explanations given that were broad and diverse. Throughout many of the accounts, telecommunications as both a time and money saver were highlighted as key factors in its appeal. This was most notable when using such data as a surveillance or 'location' tool or in its ability to identify new lines of enquiry.

One major benefit highlighted by the majority of participants was the satellite positioning data available from a mobile phone able to locate the geographical position of the mobile handset (and, potentially, its user) at any given time. This was noted as a favourable means by which to either implicate or exculpate individuals from an enquiry and was particularly beneficial when dealing with multiple suspects or persons of interests to a crime scene.

The analysis of call data to identify additional lines of enquiry, whether that be in relation to associations or relationships or to identify places frequented by the victim or suspect was also noted as of 'considerable value' as was its use in establishing a pattern of lifestyle for an individual based on an analysis of who their mobile contacted, when it was used and where it was located.

A key element in the significance of telecommunications was its popularity and prevalence within modern society, a point emphasised earlier in this study from the findings of the Ofcom 2012 Communications Market report. Indeed when expressing its significance

interviewees often supplemented their praise of its use with an acknowledgement of the prominence mobile communications currently has in society and its importance in facilitating criminal activity. The following quotations serve to explain this further,

> "*Virtually everyone has use of a mobile phone now"* (Analyst B)

> *"criminals still have to communicate with each other and if they're not going to communicate by telephone and everything is going to be face to face then that is time and money and it's not easy to do that because the fact of the matter is criminals are communicating in different parts of the country, they are communicating in different countries"* (SIO B)

> *"you cannot operate as a criminal at any level unless you can communicate, they can't operate successfully in terms of power and influence and profit"*. (SIO C)

Despite the many benefits of telecommunications to the investigative team of which many more examples were given, it was interesting to note that the lack of any available evidence elsewhere (such as eyewitnesses) or restrictions on other investigative techniques contributed to its popularity within an investigative setting. Its appeal therefore was in part by default. When probed further as to its overall critical status within an investigation the majority of interviewees acknowledged that if telecommunications were removed from the investigative arena then the same outcomes could potentially be achieved only over a protracted period of time and with much more difficulty. In explaining this, interviewees were keen to highlight the importance of not detracting from the fundamental basics of tradition investigative tactics; however it was the lack of available opportunities in these areas coupled with the time critical nature of major crime enquiries that drew investigators to exploit the criminal use of such modern technologies. The following interview segments give a flavour of this sentiment,

"..... at the end of the day it's not the be all and end all. If we never had telephony it wouldn't mean that the enquiry would come to a halt it's just a major factor of a major line of enquiry..... If you've not got that you'd just have to do it by other means.... you could go CCTV, would have CHIS reporting, various other aspects coming in" (SIO A)

"specialist tactics can be critical to your overall investigative strategy but that said its absolutely essential that as SIOs we stick to basics and ensure that the basics are being done properly because very often in any major enquiry that's what solves it" (SIO C)

"I've been involved in many enquiries where telecoms is your life blood of the whole investigation but not over the top of your traditional methods of gathering evidence which would always be the way you would be expected to do it" (Analyst C).

"as much as telecoms is critical, I would bin the telecoms if you could give me two eye witnesses in a minute but realistically that just doesn't happen now in this day and age" (SIO B).

In considering the drawbacks of telecommunications further, all participants highlighted that when dealing with the data (whether that be the call traffic or the geographical location data), it was extremely important, particularly when using it as an evidential product, to acknowledge that the data was specific to the telephone device and not the suspected user. It was therefore often described as 'not specific' and not always 'best evidence'. As such, the attribution of the phone to a particular individual was highlighted as of extreme importance by both the SIOs and analysts interviewed as was the need to corroborate the telecommunications by other means such as CCTV and witness statements.

The difficulty of telecommunications as an evidential product was another key point keen to be expressed by those interviewed. The common perception amongst participants was that its complexity often made in difficult for the normal lay people on a jury to understand and it was acknowledged that further development work was required by both police and the crown / procurator fiscals office to ensure that the presentation of such evidence was simplified to guarantee those within the court have a proper appreciation of its worth.

On conclusion, from the sample examined, it is reasonable to infer that great significance is given to the use of telecommunications within major criminal investigations which seek to solve the most serious of crimes. The benefits of its use have clearly been explained as has the recognition that its popularity is not due to its capability to perform as a robust and exceptional line of enquiry but indeed emanates from a lack of alternative lines of enquiry that can deliver as quickly and as consistently as telecommunications. It can also be suggested that society's use of telecommunications has determined its significance within law enforcement and as criminals continue to rely on such technology, law enforcement will continue to assess its use to either support or discount the notion of guilt.

Thus we must now turn to look at those involved in the handling of such data to examine the methodologies behind the inferences drawn from the use of telecommunications and how these are applied within a criminal context.

4.2 | The Art of Interpreting Telecommunications Data

From the available literature it is understood that telecommunications data can serve two distinct purposes. Firstly, it can determine the geographical location of the telephone device and thus, by implication, the person using it. Secondly, it can determine key communications, associations and relationships from the analysis of the call patterns and contacts. The methodologies behind such practices have been largely un-explored. As such, this research

looks to identify how those responsible for its analysis interpreted the data and apply meaning within the criminal context of a police investigation.

In terms of personnel responsible for the interpretation and analysis of call data, all interviewees cited the criminal intelligence analyst as the key post holder in its delivery. Again this corroborates findings taken from the research of available ACPO and NPIA policing manuals which acknowledge the analyst as a key individual in the delivery of this service. Their enhanced IT skills and ability to interpret vast volumes of data was given as the main factor in their contribution to this process. All SIOs and the majority of analysts perceived the role to be specialist in nature with all emphasising that considerable experience was essential in carrying out this role effectively. All interviewees also agreed that the interpretation of the data required a collective effort with inclusion from additional police personnel such as the telecoms officer and the intelligence cell manager to ensure a complete understanding of its meaning within the context of the investigation.

It was highlighted that different methodologies of analysis and interpretation applied depending on the different criminal setting being considered. The three main categories most commonly encountered were,

- **Spontaneous Crimes** (Often murders)
- **Pre Planned Crimes** (Such as armed robberies)
- **Serious Organised Crime** (Such as drug importations)

For each of the above categories, different communication behaviours were notable in facilitating or surrounding each crime type. Such behaviours were known to both the analysts and SIOs and formed the basis of trigger points or suspicious activity that would be looked for when analysing the data.

The majority of practitioners commented that the key starting point of any telecommunications analysis lay in establishing a normal pattern of communication for the user. This would involve gauging how frequently the phone was used, who was being contacted, when the phone was active and when it was inactive. Once this 'normality' was established, things out with the ordinary could then be looked at particularly around the time of the crime in question. The following participant's accounts serve to explain this further,

> *"A break in the norm is where you would start..... We would look at patterns before and after the event to see what the normal pattern of behaviour for the person was and in a lot of instances it's just that the pattern either before during or after will be totally different from the previous week's worth"* (Analyst B)

> *"if you've got like a bulk of data say and you've looked at a person's lifestyle over a period of time then you notice something changes then I would flag that up. On one of the cases I've worked on recently there was frequent communication between the victim and accused, after the murder there was no attempt at contact for over a fortnight so from my point of view I thought that that was highly suspicious"* (Analyst A)

> *"you need to know what normality looks like before you can make any assessment of any criminal inference that can be taken from the call pattern" (*SIO C)

In cases of spontaneous crime (most commonly murder), it was highlighted by participants that breaks from the norm in terms of communications always occurred after the event, whereby a common behavioural trait was for the culprit to either cease all communication with the deceased (in the knowledge that they were dead) or to dispose of their mobile phone

handset in the hope that any contact or location data would be lost. This was referred to by many participants as ‘conduct after the crime’. Two SIOs highlighted that such spontaneous crimes usually offered good telecommunications opportunities as those responsible were unlikely to have been mindful of their telecommunications activities prior to the event and may invariably have used their mobile phone in the ‘panic stricken’ moments afterwards providing vital witness and location information. One SIO explained the benefits further,

> *“The spontaneous crime that happens, pub murder, shooting where it happened in rage etc it’s far harder for people to hide that because who you phoned five minutes before you murder somebody is captured then, if there’s no planning it’s far easier for us to pick up the picture and invariably even in those types of enquiries the telecoms can still put people at the scene of a crime, tell me who they spoke to right after the crime, right before the crime etc”* (SIO B)

Despite criminals’ consideration of telecommunications in pre-planned crimes, participants highlighted that there were still learnt behaviours that were commonly looked for within associated patterns of communication. Many acknowledged that as the use of telecommunications as an investigative tactic became more commonly known within the public domain, efforts to elude police in the use of such technology had become apparent. These efforts themselves served to act as suspicious behaviour and often featured as a presumption of guilt in investigations and subsequent criminal trials. Common use of telecommunications in the context of a pre-planned crime involved the criminal switching their phone off or not taking their phone with them to the scene of the crime. One SIO explained,

> *"They would maybe go to Tesco and buy a £10 phone and use that or they'll just not take their phone with them, they'll leave them in the house or in possession of an individual who is going to alibi them"* (SIO A).

In the instance of serious organised crime, both intelligence analysts and SIOs highlighted that the understanding of telecommunications within this arena proved much more difficult given the lengths such criminals would go to avoid detection. The majority of interviewees highlighted that the analysis of call patterns was favourable in this particular crime setting to establish lifestyle on the user considering factors such as criminal associates, financial interests and places frequented. From the sample interviewed, such criminals were perceived to have the greatest understanding and were the most common users of advancing technology in their attempts to keep ahead of law enforcement. One SIO highlighted that it was not uncommon for a member of a serious and organised crime group to operate ten to twelve phones at any one time. The swapping of a SIM[5] card or the rotation of mobile phones on a monthly basis was described as common practice within criminal networks as was the increasing use of advancing technologies such as blackberry messenger, e-mailing, and social networking sites where it was known that retrospective data capture of such communication by law enforcement was not always possible. One SIO summarised the avoidance tactics of some individuals involved in serious organised crime deployed in their use of telecommunications,

> "*.....the fact is criminals use mobile phones and they try and sit under the radar to avoid detection so they constantly change their phones, constantly buy pre pay, don't register their phones and that's a lot of work for us..... They are aware of our tactics and they try to avoid speaking on*

[5] SIM Card – Subscriber Identification Module: - A removable card inside a mobile phone that stores data unique to the user.

> *the phone, they try to avoid registering phones some will even avoid carrying phones to certain locations if they think the police can track and obtain cell site analysis"* (SIO B).

In assessing these risks, some of those interviewed described telecommunications data as a 'double edged sword' whereby its evidential appeal and subsequent public exposure in high profile criminal trials had led to a greater understanding within criminal networks of its worth to law enforcement. This in turn had created additional challenges in terms of combating the counter measures subsequently applied by criminals to disguise or secrete their communications.

In considering the location data that telecommunications provided, little detail could be gained from the participants around the methodologies applied to its interpretation and analysis other than the basic premise that the satellite positioning of a mobile phone could determine its location at any given time. This information was provided on the 'call data' received from the service provider and came in the form of a post code or 'mast location' indicator. It was expressed that this was not always specific and could place the mobile within a particularly wide geographical area. Further technical interrogation of the data was therefore required to gain a more accurate and precise location of the mobile. There was universal agreement from all participants that the interpretation and understanding of this location information most commonly referred to as 'cell site data' was best deciphered by those with engineering expertise located within the telecommunications sector. None of the analysts interviewed were of the opinion that they were qualified or held the technical expertise to work with this data on anything other than a basic level or indeed speak to it in a court of law. All participants indicated that they had worked on cases where a private commercial firm had been instructed to deliver this service.

It was emphasised by the majority of those interviewed that such companies were used due to their state of the art equipment to pinpoint location data and in providing 'expert' evidence in court from an engineering perspective. This provides further understanding as to the increasing number of digital forensic companies entering the market as highlighted in the earlier review of literature. The lack of technical facilities in-house was cited as the main driver for the appointment of such commercial companies and this caused concern for at least one police officer who had already considered this issue in terms of the move towards a single Scottish Police Force,

> *"If you ask should we employ someone within the organisation – I've already put this through as a recommendation in relation to the new Scottish Police Service, we should employ our own engineers - independent but their only duty is to do the kind of work of FTS. We will save ourselves millions because we outsource this primarily to a number of other telecoms companies"* (SIO B).

From the research undertaken it has been established that the art of interpreting telecommunications data is a complex and specialist task dependent on a number of factors and permutations of the crime presented. The intelligence analyst is clearly identified as a key player in the delivery of telecommunications where an understanding of human behaviours within a number of different criminal contexts is crucial in drawing meaning from the data. The research has emphasised that as the understanding of such behaviours becomes more refined and thus more pertinent within an evidential arena, the exposure of this tactic becomes commonplace. As criminals look to counteract these tactics law enforcement to some extent have become a victim of their own success. The outsourcing of certain areas of telecommunication interpretation seems inevitable given the advances in technology and is clearly common practice within the organisation researched. This failing in technical

expertise both in terms of personnel and physical equipment from an in-house perspective is not uncommon and brings us on to discuss the wider technological issues surrounding telecommunications.

4.3 | Technology

As we have established, telecommunications are both significant to criminals in facilitating their illicit activities and to law enforcement in their efforts to combat crime. However whilst the criminal fraternity proceed with great earnest in their use of such technology, its advancing capabilities create major challenges for its use by police practitioners. As academic research has informed us, the corporate control of telecommunications, the requirement for co-ordinated legislation between countries and the lack of suitably trained personnel are all identified as issues hindering law enforcement's capability and capacity to respond to these technological advances (Shelly 2003, Broadhurst 2006, Hunton 2010).

We now turn to consider the way in which the sample of police practitioners studied have responded to these technological developments to establish if indeed these issues are evident in the context of a local operational police setting and to better assess if current policing practices in the use of telecommunications are fit for purpose.

Recognition of the rapidly changing pace of technology and its risk in the fight against crime was universal throughout the participant's accounts. Given the monumental influence mobile communication and its advancing capabilities have on society as a whole, the police practitioners interviewed; being general consumers of the products themselves, immersed within this new technological age of smart phone, internet communication, and Wi-Fi could easily comprehend the looming problems that such advancing technology would have in the work place. When assessing the growing impact of telecommunications within law

enforcement many unearthed grave concerns regarding its future contribution to police investigations.

In addressing the technology issue those holding a SIO role seemed more attuned to the potential risks to the organisation than the intelligence analysts. Some SIOs had considered potential solutions to the problem whilst others had at least identified key areas of vulnerability.

Indeed all three SIOs concluded that the single biggest problem they faced in conducting major investigations where telecommunications were present lay in the lack of suitably trained and knowledgeable people, a problem previously identified by Shelly (1998) in her study of '*Crime and Corruption in the Digital Age'*. The 'people' problem was diverse and split in terms of both the provision of adequately trained staff to deal with the current use of telecommunications and those that would have the knowledge and skills set to tackle the future threats from the advancing technology. Succession planning was identified as a concern whereby those SIOs with a relatively good grasp of telecommunications within an investigative arena were nearing the end of their service and a danger existed that such experience would be lost if their skills were not transferred. One SIO remarked,

> *"my concern is we have a group of people who, and it's the same group of people, who are building up all the experience and expertise and they're getting on a bit in service. We need to be better at bringing some younger people in and what I mean is younger in service, as for every major investigation we still tend to use the same people..... I would like to see some practical experience in getting people to shadow major investigations..... If we lose the people that know then we're not going to have the people there"* (SIO B).

In assessing further the current cadre of suitably trained telecommunications personnel within the realms of major crime investigation the majority of people currently involved were described as ‘not match fit’. Interestingly it was acknowledged that this issue spanned way beyond the confines of the major investigation team with one officer highlighting,

> *“We don’t have people who have experience, we don’t have people who can speak to it in court, we don’t have people within the fiscal’s office who understand it, we don’t have people within the crown who understand it and we don’t have juries who understand it or judges who understand it and we don’t have enough SIOs who understand how it works in order to gather the evidence” (*SIO C*).*

In terms of the risks from advancing technology, this presented a whole new set of challenges involving an intertwined problem of both ‘people’ and technical issues. In contrasting the current organisational personnel against the rapidly changing telecommunications picture one SIO described current police practitioners as a ‘completely lost generation’. Indeed all three SIOs acknowledged the cultural change in social interaction generated by the technological age expressing their unfamiliarity with the many new modes of communication utilised by the ‘youth of today’. Underpinning these opinions was the notion that having not been ‘brought up’ in this social context it was difficult to grasp a complete understanding of the complexities of modern communication.

The technical problems of advancing technology were captured within the key theme of the corporate control of telecommunications again an issue of concern highlighted in previous academic studies (Shelly 1998; Broadhurst 2006). The general flavour of opinion from interviewees was that technology and the business decisions supporting its use were likely to dictate how police will conduct investigations in the future. The significant component of this

concern was the move from the traditional engineering aspects of landline and mobile telecommunications routed through the use of masts towards voice over internet communication (VOIP) and the subsequent loss of conventional telecoms billing data. Officer's sentiments were captured in the following statements'

> *"In terms of VOIP communication, law enforcement is massively behind the game, top to bottom, left to right, right across the whole world without a shadow of a doubt. We're rapidly moving forward to a time when the phones aren't going to be connected to masts, they're going to be connected to Wi-Fi, that information isn't available so we'll not be able to get a billing. You won't be able to get a traditional billing that says that phone contacted that phone on that day. So the information that we currently rely on just now for our MIs which is huge, is now shrinking and all that information is in the dark and it's not readily accessible without applying extremely sensitive techniques to that which we currently don't have access to"* (SIO C).

> *"In terms of the technical aspects with Skype when the call leaves the handset it breaks up into various different pieces and then it only arrives back into one the second it arrives back into the other handset to the other person you are calling and you can't capture it in-between so therefore you cannie get that data that you really require. It will make life much more difficult for SIOs if we are not in a position to capture that data. If we don't have the phones it's a major line of investigation that isn't available and we've almost went full circle where we have went back to where we were before mobile phones came along."* (SIO A).

> *"VOIP, Skype, all these things.... everything is done on the internet, everything is done by Blackberry Messenger etc, things that are untraceable or undetectable from a law enforcement perspective. That is a challenge for us. "*(SIO B)

A further technical area of concern rested with the encryption of internet data specific to e-mail communication. Marketed by key leaders within the telecommunications sector as a considerable benefit to its customers, this has proved increasingly problematic for law enforcement to subsequently unlock and gain access to the details. Shelly's (1998) point of the global information infrastructure being outside the jurisdiction of any one country is emphasised here whereby SIOs highlighted that this encryption issue is difficult to resolve given that the communication companies concerned are based in America and therefore fall out with the requirements of RIPA legislation. One SIO reiterated the point that 'offshore service providers are a bit of a problem for us'.

In addressing the overall challenges from advancing technology, some SIOs acknowledged the risks but assumed or at least hoped that due to its global impact others within the world of telecommunications and law enforcement were seeking to address these issues. The following interview segments serve to illustrate this point:

> *"I am hoping that those in the world of telecommunications and those that move in those circles are ahead of the game. It's no' my area of business but if we don't then we are going to lose potentially so many opportunities in the future as people get more intelligent around their use of telecoms.….. This cannot just be an issue for Strathclyde – this must be an issue for policing and law enforcement worldwide because that's what the internet brings us now.…… we've got a whole industry of telecoms thinking about*

these things but the fine detail around about that – about who does that, who's got ownership of that I really couldn't tell you". (SIO B)

"It will make life much more difficult for SIOs if we are not in a position to capture the data and I know there's work ongoing to try and keep law enforcement ahead of the criminals.....". (SIO A)

One SIO, who was both pro-active and assertive in style, took a more committed approach to the problem and whilst recognising advancing technology as a national policing issue considered it within a local context as a problem Strathclyde Police must seek to rectify. In terms of the 'people' problem he stated,

"We are too old.....we will never get ourselves match fit because we don't get it we don't understand it. The problem with that is you need to find staff that are.... and I've discussed this at very senior levels within the organisation, we should be going to Caledonian University, and just recruiting people at 19 years of age who are brought up in that whole X Box, Playstation, online environment..... We need to be able to recruit the right people which are kids... That means that there needs to be a massive change in our attitude towards recruitment of staff. The average age of a probationer in policing terms is 26 year old – too old.... we need to be recruiting people who when they're no' doing the work for us they're going home at night and developing apps and selling them. These people are out there and they cannie get work" (SIO C).

The available literature (Shelly 1998; Broadhurst 2006) on the risks of telecommunications and its advancing technology, although now somewhat dated, resonated with the primary research conducted for this study. Areas such as inappropriately trained personnel or

unknowledgeable practitioners within the criminal justice system coupled with a continued lack of state influence over the commercial operation of communication service providers (most notably on an international level) appear to be have remained relatively unchanged over the last decade with no obvious signs of development or real improvement for the future.

From the sample studied, it is possible to conclude that from a technological aspect, law enforcement's knowledge and use of telecommunications is not fit for purpose in the current investigative setting nor is it ready to tackle the future challenges from advancing technology. Despite the relative achievements to date from the application of this investigative tactic it is suspected that such success has been limited and may indeed be short lived. Both changing technology and the practitioners involved create the two distinct areas that require attention.

Whilst individual law enforcement agencies can attempt to combat the 'people' problem through changes in local recruitment strategies to acquire the appropriately trained personnel a complete solution cannot be sought without intervention at a national level to tackle the technical aspects of this problem. Without this two pronged approach, vital communications and their interpretation and understanding within the criminal justice system such as those used to help convict Edinburgh murderer David Gilroy will no longer exist.

Chapter 5 | Conclusion

Given the growth of telecommunications in today's society and the reliance we now place on mobile phones in our interaction with others, this dissertation set out to probe the use of telecommunications in the field of criminal investigation. Despite the proclamations of high ranking police officers and government politicians declaring its widespread use and significance within law enforcement little was known as to why this was other than the notable advantages that were evident from the media coverage of a number of high profile murder trials where telecommunications featured. Despite its public status as a key

investigative technique, its position as such has remained notably under reported and largely under researched. This dissertation therefore looked to explore how significant telecommunications was to law enforcement. In particular it sought to examine if the right people and practices existed to support its delivery and indeed if law enforcement's current and future commitments to its practice were fit for purpose.

In recognising the distinct lack of any empirical research in past studies, data sourced direct from participants in the field was considered the most favourable option in establishing an authentic understanding of this policing practice and indeed proved extremely worthwhile. The interview of six police practitioners from Strathclyde Police provided emotive and passionate accounts of this investigative practice resulting in the collection of rich and detailed information. Data was gathered and analysed using a framework of three broad themes emanating from the associated review of available literature which included criminal investigations, the art of interpreting telecommunications data and current and future technologies.

This study has highlighted that as a single strand of the technological phenomena that has affected crime over the last two decades, telecommunications is one that has impacted greatly on the ability of both criminals and law enforcement agencies to function more effectively. Its significance as an investigative tactic is therefore without question. Findings from primary data collection indicate that its popularity and prevalence within society, its cost effectiveness and the lack of alternative lines of enquiry all contribute to its appeal.

It has been identified that a tight legislative framework supports the use of telecommunications and is frequently and increasingly used by law enforcement in criminal investigations which seek to solve the most serious of crimes.

The research has highlighted the role of the criminal intelligence analyst as a key stakeholder in the delivery of telecommunications. This specialist role requires a complex and varying methodological approach to the interpretation of associated data that requires extensive knowledge and experience of criminal behaviours.

The study noted a distinct lack of understanding around the more complex, technical aspects of telecommunications particularly when referring to ‘location data’. It was assessed that given the prominent outsourcing of this function to private companies, any future study in this area would require exploration out with the realms of law enforcement.

A significant finding from the overall study and universal to all areas of the research was the ‘people’ problem and the recognition that there is a lack of suitably trained staff to effectively drive telecommunications investigations within law enforcement. This is further compounded by a number of key risks identified from the research that cast doubt over its future use. The corporate control of technology, offshore service providers and the lack of a ‘technical fix’ to combat the challenges from advancing technology are all areas of concern where no imminent solution is evident. It is therefore assessed that law enforcements’ knowledge and use of telecommunications is not fit for purpose in the current investigative setting nor is it ready to tackle the future challenges from advancing technology.

APPENDIX A

CONSENT FORM

Full title of Project: MSc Criminology and Criminal Justice Dissertation:

"Constructing the Criminal: An Exploration of Police Practitioners' Understanding of the Use of Telecommunications Data in Criminal Investigations".

Nicola Moffat, MSc Criminology Student
C/O University of Glasgow
School of Social & Political Science
Glasgow
Tel: 07793288212

Please note - This research study is not a critique of the use of telecommunications data in a particular case or of Strathclyde policing practice - its intention is to gain an appreciation of the issues framing the use of telecommunications in police investigations in general.

Please initial box

I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions. ☐

I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason. ☐

I agree to take part in the above study. ☐

Please tick box

	Yes	No
I agree to the interview being audio recorded	☐	☐
I agree to the use of anonymised quotes in publications	☐	☐

Name of Participant	Date	Signature
Name of Researcher	Date	Signature

The requirements of the Data Protection Act and the Freedom of Information Act will be observed in respect of any information obtained and the anonymity of participants and investigations will be ensured at all times.

APPENDIX B

University of Glasgow

INFORMATION SHEET

"CONSTRUCTING THE CRIMINAL: AN EXPLORATION OF POLICE PRACTITIONERS' UNDERSTANDINGS OF THE USE OF TELECOMMUNICATONS DATA IN CRIMINAL INVESTIGATIONS".

You are being invited to take part in a research study. Before you decide whether or not to take part, it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully.

Purpose of the study?
My name is Nicola Moffat and I am a MSc student at the University of Glasgow. I am also a Criminal Intelligence Analyst based at Strathclyde Police Force Headquarters.

As part of my MSc dissertation I am currently conducting research into the use of telecommunications data in criminal investigations. I have three main research interests,

1. How does telecoms data shape police understanding of culpability, social relationships and involvement in crime?
2. What significance do telecommunications play over other investigative techniques?
3. How is the delivery of telecoms analysis achieved in its current form and is it fit for purpose.

It is important to highlight that this research study is not a critique of the use of telecommunications data in a particular case or of Strathclyde policing practice - its intention is to gain an appreciation of the issues framing the use of telecommunications in police investigations in general.

Why have I been invited to participate?
You have been selected as one of six police practitioners (3 SIOs and 3 Criminal Intelligence Analysts) based on your varied experience within the disciple of criminal investigation. You will have a range of opinions on many aspects of such investigations. This will range from attitudes to how the use of telecommunication contributes to the notion of guilt, how its use is applied in a practical setting and the value it brings to criminal investigation. Your views and opinions will be vital to

understanding why human behaviours linked to the use of telecommunications are of potential importance in this area of policing.

What does taking part in the study involve?
Taking part in the research is entirely voluntary. If you agree to take part in the study you will be asked to participate in one interview lasting for around 45 minutes. The interview will be conducted face-to-face in a private area of your workplace, or another police office or location if you feel that you would prefer this option.

With your permission I would like to tape record the interview. You do not have to answer any questions you do not wish to, and you may stop the interview at any time.

APPENDIX B

What will happen to your answers?
The requirements of the Data Protection Act and Freedom of Information Act will be observed. All your comments will be anonymised and you will not be identified in the final research report. Only I will have access to data arising from the research and this will be stored securely. All computer-held data will be password-protected.

All information collected will also be treated confidentially, unless you reveal details of harm or danger towards yourself or that you are causing harm or danger to others. If this occurs, ethical guidelines will be followed which involves contacting relevant bodies to enable help and advice to be given. Your answers will not be shared with your employer unless serious issues of harm or danger arise.

If you request it, you will be given a transcript of any interview(s) you undertake to view and comment upon before the research document is finalised.

Further questions or concerns

The study has been approved by,

- School of Social and Political Sciences at the University of Glasgow.

If you have questions or concerns about the research at any time you can contact me Nicola Moffat, the researcher, at: 1007896M@student.gla.ac.uk. If you need to speak to me in person you can contact me on: 07793288212.

If you would prefer to do so, you can contact my supervisor at the University of Glasgow, Jon Bannister (Jonathan.Bannister@glasgow.ac.uk Tel. 0141 330 3782).

Thank You for taking the time to read this information sheet.

2nd July 2012

APPENDIX C

INTERVIEW SCHEDULE

Student: Nicola Moffat

Student No: 1007896m

Dissertation Topic: *Constructing the Criminal – An Exploration of Police Practitioners' Understandings of the Use of Telecommunications*

Interview Questions

Q1. Can you tell me a bit about your police career to date?

Q2. Can you describe to me what a major criminal investigation or a major enquiry is and what sets it apart from normal policing enquiries?

- Prompts – Resources / Budget / Tactics Used

Q3. Is the expectation or demand for a successful outcome greater on a major enquiry and if so why?

- Prompts – Police investment / Media Interest / Public interest / Performance Targets

Q4. Moving on to Telecoms, what significance would you place on the use of telecommunications within a criminal investigation?

Q5. Percentage wise – how often would you say you use telecoms in major investigations?

Q6. To what degree do you think telecoms shapes the decisions taken by SIOs in a major investigation?

Q7. Can you describe the difficulties you think you would encounter without the availability of telecoms data within a major investigation?

Q8. What are the expectations of SIOs, Analysts and others within the criminal justice system i.e. Crown office in relation to telecoms analysis and do these match reality?

Q9. Do you favour the use of telecoms data over other forms of data and if so why?

Q10.How is telecoms data used to discount or support the notion of guilt?

- Prompts – What kind of telecoms use would make you suspicious?

Q11. How does telecoms data shape your understanding of culpability, social relationships and involvement in crime?

- Prompts – What is it that makes it so good / what are the benefits?

-

APPENDIX C

Q12. Do you have any concerns over the use of telecoms data in major criminal investigations?

Q13. Before the use of telecoms data where did you find the info that this source of data provides?

- Prompts – Location of suspect
- Relationships and associations

Q14. How comfortable are you with the accuracy of the telecoms data provided?

Q15. Who do you believe to be the key personnel in the delivery of telecoms within a major investigation?

Q16. Do you consider the analysis of telecoms data to be a specialist role?

Q17. What are your thoughts on the use of commercial companies assisting law enforcement with the delivery of telecoms support in major investigations?

Q18. From your experience of criminals and their networks what is your knowledge of their awareness of the interrogation of telecoms as a police tactic to detect crime and what is your awareness of the counter measures they impose to combat this threat?

Q19. Given advances in technology, what do you think is the future for the use of telecoms data within criminal investigations?

Bibliography

Ainsworth, P.B. and Pease, K. (1987) *Police Work*, Leicester: British Psychological Society

Association of Chief Police Officers (ACPO) (2005) *Practice Advice on Core Investigative Doctrine 2005*, Centrex
http://www.ssiacymru.org.uk/media/pdf/6/c/Core_Investigation_Doctrine_Interactive_1_.pdf [Accessed 16.08.12]

Association of Chief Police Officers (ACPO) (2010) *The Journal of Homicide and Major Incident Investigation Volume 6 Issue 2*, National Policing Improvement Agency (NPIA)
http://www.npia.police.uk/en/docs/Journal_6.2__FINAL.pdf [Accessed 10.08.12]

Association of Chief Police Officers (ACPO) (2011) *The Journal of Homicide and Major Incident Investigation Volume 7 Issue 1*, National Policing Improvement Agency (NPIA)
http://www.npia.police.uk/en/docs/Journal_7.1_Locked.pdf [Accessed 10.08.12]

Avon and Somerset Constabulary (2012) *Freedom of Information Request Response*
http://www.avonandsomerset.police.uk/information/foi/QandA_Question.aspx?qid=1881 [Accessed 01.08.12]

BBC News (14/11/02)'*Text messages examined in Danielle murder case*
http://news.bbc.co.uk/1/hi/england/2478639.stm [Accessed 04/08/12]

BBC News (06/11/03) *'Soham trial: 'Crucial' phone evidence*
http://news.bbc.co.uk/1/hi/england/cambridgeshire/3246111.stm [Accessed 04/08/12]

BBC News (18/04/12) *How Surveillance Society Solved a Murder with No Body*
http://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-17727255 [Accessed 16.06.12]

Berg, B. (2007) *Qualitative Research Methods for the Social* Sciences *6th Edition*, Boston: Pearson Education

Briggs, R. et al. (2011) *Anatomy of a Terrorist Attack - What the Coroner's Inquests Revealed about the London Bombings* (Occasional Paper), The Royal United Services Institute (RUSI)
http://www.rusi.org/downloads/assets/anatomyofterror.pdf [Accessed 21.07.12]

British Society of Criminology (2006) *Code of Ethics for Researchers in the Field of Criminology*,
http://www.britsoccrim.org/codeofethics.htm [Accessed 21/07/2012]

Broadhurst, R. (2006) *Developments in the Global Law Enforcement of Cyber-crime*, An International Journal of Police Strategies & Management Vol. 29 (3): 408 - 433

Brownlie, A.R. (1984) *Crime Investigation Art or Science?,* Edinburgh: Scottish Academic Press

Bryman, A. (2004) *Social Research Methods* 2nd Edition, Oxford: Oxford University Press

Bryman, A. (2008) *Social Research Methods* 3rd Edition, Oxford: Oxford University Press

Donnelly, D. and Scott, K. (eds.) (2005) *Policing Scotland*, Devon: Willan Publishing

Casey, E. and Turnball, B. (2011) Digital Evidence on Mobile Devices in *Digital Evidence and Computer Crime*, 3rd Edition, Elserier Inc.
http://www.elsevierdirect.com/companions/9780123742681/Chapter_20_Final.pdf [Accessed 09.08.12}

Cherkasov, V. (2009) *Information Technologies and Organised Crime*
http://www.crime-research.org/library/Cherkasov.html [Accessed 07.08.12]

Clarke, R.V. and Newman, G.R. (2007) *Police and the Prevention of Terrorism,*
Policing Journal – A Journal of Policy and Practice 2010 Vol.1 (1), Oxford Journals

Dantzker, M. L. and Hunter, R. D. (2006) *Research Methods for Criminology and Criminal Justice: A Primer* 2nd Edition, London: Jones and Bartlett

Fife Constabulary (2012) Freedom of Information Request Response
http://www.fife.police.uk/default.aspx?page=6902 [Accessed 01.08.12]

Flick, U. and Kardoff, E. and Steinke, I. (eds.) (2004) *A Companion to Qualitative Research*, London: SAGE

Forensic Telecommunications Services (FTS) (2012)
http://www.forensicts.co.uk/ [Accessed 13.08.12]

Guardian Online (15/03/12) *Suzanne Pilley Murder: David Gilroy Found guilty of Killing Former Girlfriend*
http://www.guardian.co.uk/uk/2012/mar/15/suzanne-pilley-murder-david-gilroy {Accessed 18.06.12]

Guardian Online (17/05/12) *Met to Use Software that can Crack Mobile Phones even with Locked SIM*
http://www.guardian.co.uk/technology/2012/may/17/met-software-mobile-phones [Accesssed 06.08.12]

Gillham, B. (2005) *Research Interviewing: The Range of Techniques*, Maidenhead: Open University Press

Hammersley, M. and Atkinson, P. (1995) *Ethnography: Principles in Practice, 2nd Edition*, London: Tavistock

Hewson, C. et al. (2003) Internet Research Methods: *A Practical Guide for the Social and Behavioural Sciences*, London: SAGE

Homan, R. (1991) *The Ethics of Social Research*, London: Longman

Home Office (2012) *Communications Data* webpage
http://www.homeoffice.gov.uk/counter-terrorism/communications-data/ [Accessed 05.08.12]

Home Office (2012) Draft Communications Data Bill
http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf [Accessed 22.08.12]

Hunton, P. (2010) *Cyber Crime and Security: A New Model of Law Enforcement Investigation,* Policing Journal – A Journal of Policy and Practice 2010 Vol.4 (4): 385-395, Oxford Journals

Innes, M. (2003) *Investigating Murder: Detective Work and the Police Response to Criminal Homicide*, Oxford: Oxford University Press
Intaforensics (2012)
http://www.intaforensics.com/ [Accessed 13.08.12]

Jewkes, Y., and Yar, M. (2010). 'Introduction: The Internet, Cybercrime and the Challenges of the Twenty-First Century', in *Handbook of Internet Crime*. Devon: Willan Publishing

Kent Police. (2012) *N27 Accessing Communications Data* webpage
http://www.kent.police.uk/about_us/policies/n/n027.html [Accessed 30.07.12]

Koops, B. (1999) *The Crypto Controversy,* The Hague: Kluwer Law International

Lee, R. (1993) *Doing Research on Sensitive Topics*, London: SAGE

Leishman, F. and Loveday, B. and Savage, S.P. (eds.) (2000) *Core Issues in Policing 2nd Edition*, Harlow: Longman

Levi, M. (2007) 'Organised Crime and Terrorism', in Maguire, M. and Morgan, R. and Reiner, R.(eds.) *The Oxford Handbook of Criminology 4th Edition*, Oxford: Oxford University Press

Marx, G.T. (2007) *The Engineering of Social Control*: *Policing and Technology*
Policing Journal – A Journal of Policy and Practice 2010 Vol.1 (1), Oxford Journals

Mason, J. (2004) *Qualitative Researching* 2nd Edition, London: SAGE

McLaughlin, E. And Muncie, J. (eds.) (2001) *Controlling Crime* 2nd Edition, London: SAGE

Miles, M.B. (1979) 'Qualitative Data as an Attractive Nuisance', *Administrative Science Quarterly*, 24: 590 -601

Newburn, T. (2007) *Criminology*, Cullompton: Willan Publishing

Nickolls, L.C. (1956) *The Scientific Investigation of Crime*, London: Butterworth

Nicol, C. et al. (2004) *Reviewing Murder Investigations: An Analysis of Progress Reviews from Six Police Forces*, Home Office Online Report 25/04
http://library.npia.police.uk/docs/hordsolr/rdsolr2504.pdf [Accessed 02.08.12]

Noaks, L. & Wincup, E. (2004) *Criminological Research: Understanding Qualitative Methods*, London: Sage.

Northumbria Constabulary (2012) Freedom of Information Request Response
http://www.northumbria.police.uk/faq/other/answer.asp?id=63019 [Accessed 01.08.12]

Nunn, S. (2003) *Seeking Tools for the War on Terror: A Critical Assessment of Emerging Technologies in Law Enforcement,* An International Journal of Police Strategies & Management Vol, 26 (3): 454-472, Hein Online

Ofcom (2011) *A Nation Addicted to Smart Phones*
http://consumers.ofcom.org.uk/2011/08/a-nation-addicted-to-smartphones/ [Accessed 10.08.12]

Ofcom (2012) *Communications Market Report 2012*
http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf [Accessed 17.07.12]

Reiner, R. (1992) *The Politics of the Police 2nd Edition,* New York: Harvester Wheatsheaf

Scotsman.com (2012) *Kevin 'Gerbil' Carroll murder trial: Trial Hears Phone Evidence*
http://www.scotsman.com/the-scotsman/scotland/kevin-gerbil-carroll-murder-trial-trial-hears-phone-evidence-1-2266534 [Accessed 16.06.12]

Scottish Government (2011) Statistical Release Crime and Justice Series: *Homicide in Scotland, 2010-11*
http://www.scotland.gov.uk/Publications/2011/12/14124940/3 [Accessed 21/07/2012]

Shelley, L. I. (1998) 'Crime and Corruption in the Digital Age', *Journal of International Affairs*, Vol. 51, (2): 607-620

Shelly, L.I (2003) 'Organized Crime, Terrorism and Cybercrime' in Bryden, A. and Fluri, P. (eds.), *Security Sector Reform: Institutions, Society and Good Governance pp. 303-312,* Nomos Verlagsgesellschaft: Baden-Baden

Strathclyde Police. (2012) Freedom of Information Request Response – Reference 0432/12
http://www.strathclyde.police.uk/assets/pdf/22915/response_letter_for_website.pdf04322012 [Accessed 01.08.12]

Strauss, A. and Corbin, J.M. (1998) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory,* Thousand Oaks, California: Sage.

STV News (30/04/12)'*Kevin Gerbil Carroll Trial hears of phone link to Murder Scene*
http://local.stv.tv/glasgow/305493-kevin-gerbil-carroll-trial-hears-of-phone-link-to-murder-scene/ [Accessed 04/08/12]

Tewksbury, R. (2009) *Qualitative versus Quantitative Methods: Understanding Why Qualitative Methods are Superior for Criminology and Criminal Justice*,
Journal of Theoretical and Philosophical Criminology, Vol 1 (1)

The Herald Scotland (03/03/12) Accused put Make-up on Hands
http://www.heraldscotland.com/mobile/news/crime-courts/accused-put-make-up-on-his-hands.16915059 [Accessed 18.06.12]

The Herald Scotland (15/03/12) David Gilroy Guilty of Suzanne Pilley Murder
http://www.heraldscotland.com/mobile/news/home-news/david-gilroy-guilty-of-suzanne-pilley-murder.1331810187?_=b2bf3374a4e4da46c6a82edb4055fa52286731e6 {Accessed 16.06.12}

Tong, S. and Bryant, R. P. and Horvath, M. A. H. (2009) *Understanding Criminal Investigation*, Chichester: John Wiley & Sons Ltd

Waddington, P.A.J. (2010) *Are We Really Serious about Organized Crime?* Policing Journal – A Journal of Policy and Practice 2010 Vol.4 (1), Oxford Journals

Wittle, A. (2001) Towards a Network Sociality, Theory Culture and Society Journal Vol.18 (6), SAGE

Wolfgang, M. E. (1981) *Confidentiality in Criminological Research and Other Ethical Issues,* The Journal of Criminal Law & Criminology, Vol. 72 (1): 345-361