Social Media and Police investigations: Understanding the strategies that officers pursue when they encounter social media in their investigations

by

Wojciech Stanislaw Spyt

A thesis submitted in partial fulfilment of the requirements for the award of the degree of Professional Doctorate in Criminal Justice of the University of Portsmouth.

Institute of Criminal Justice Studies

University of Portsmouth

2017

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

Word Count: 49270

Abstract

This research addresses the investigative strategies that police officers from traditional police departments pursue when dealing with social media in their investigations. There are a variety of ways in which social media can feature within a case. This study focused only on one of these - the social media material generated by the actors (victims, witnesses and suspects) within an investigation. It identifies the decisions that officers make when presented with social media within an investigation and what drives officers to make those decisions. It utilises the most up to date guidelines for good practice in relation to digital evidence centrally available to officers in England (ACPO, 2012) in order to provide a benchmark against which to compare officers' decisions and rationale. Due to difficulty in identifying established theory on investigator decision-making around social media encountered in investigations, grounded theory was adopted to analyse the primary data collected. This methodology is well-suited to building theory in a relatively unexplored field (Glaser, 1978; Schreiber, 2001; Goulding, 2002). Two police forces provided data for the research these being Thames Valley Police and Avon and Somerset Constabulary with two different data collection methods being used. The first was the collection and examination of crime reports and the second comprised of semi-structured interviews with investigators. In laying out the decision- making process that officer's use, the research highlights where the opportunities lie for best practice and how to influence the behaviour of investigators in the future. The research identified social media as a new problem for investigators with unique facets to it. However, it found that investigators were using heuristics to inform their decision-making process. In so doing they were applying strategies to social media that are were not adequate to deal with it when considering their objectives.

Contents

Table of Figures

Chapter 1 - Thesis Overview

1.   Introduction

In the current era of information-technology the use of the internet has become ever more prevalent. It affects almost every feature of people's lives, from making transactions, storing personal and business information, advertising, exchanging legal documents to various forms of communication. A large part of internet use is concerned with social media. Social media began to have a mass public appeal from the early 2000's, the following marking the development of some of the better-known platforms: Wikipedia (2001), Myspace (2003), Facebook (2004), Flickr (2004), Bebo (2005) YouTube (2005), Twitter (2006). These and other social media platforms have allowed for the sharing of diverse types of information between individuals and communities including, music, education, movies, photographs and personal information. Along with many other platforms they have succesfully permeated everyday personal aspects of people's lives, who through those platforms also lose a measure of their privacy (Silverstone & Haddon, 1996; Trottier, 2012; Goldsmith, 2015). By encroaching into the personal aspects of people's lives they have also become intertwined in the everyday criminal conduct of individuals (O'Keefe & Clarke-Pearson, 2011; Hinduja & Patchin, 2013; Wall & Williams, 2013). Examples of such criminal conduct range from the grooming of children (Wall, 2001; Jewkes & Andrews, 2005; Holt & Bossler, 2012; Gilespie, 2015), cyberbullying (Kwan & Skoric, 2013; Kokkinos, Baltzidis, & Xynogala, 2016), commuincation relating to terrorism (Mahmood, 2012; Weimann, 2014) to burglars using social media to identify when persons are on holiday so that they can target their houses whilst they are away (Rose, 2011; Weir, Toolan & Smeed, 2011).

Social media's impact on policing was however delayed until the latter part of that decade (Crump, 2011; Trottier, 2012). Information that would previously not have been disclosed has slowly drifted into the public domain (Wall &

Williams, 2013) and become available for the police to both see, collect and use in their investigations (Trottier, 2012; Goldsmith, 2015). Furthermore, not only is the information available but the police in England and Wales are under an obligation under the Criminal Procedures Investigatons Act 1996 (CPIA, 1996) to pursue all reasonable lines of enquiry. If a social media platform holds material that is relevant in an investigation then it may well be a proportionate line of enquiry to attempt to obtain that material.

However social media platforms are numerous, different in nature and constantly evolving (Quan-Haase, 2008; Hogan & Quan-Haase, 2010; Kaplan & Haenlein, 2010; Kim, Jeong, & Lee, 2010; Lenhard, Purcell, Smith, & Zickuhr, 2010; Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). Previous research has suggested that front line police lack the skills and knowledge to deal with social media evidence (Jewkes & Andrews, 2007; Jewkes & Yar, 2008; Nicol, Innes, Gee, & Feist, 2004). Coupled with this is the difficulties that government agencies have with accessing social media content that is not publically available on profiles. The reasons for this are numerous. Social media providers are loathe to engage with law enforcement agenices for reasons of both cost (Hunton, 2009; Kardasz, 2012) and reputation (Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). This is further complicated by the providers being in different jurisdictions to the law enforcement agencies seeking information from them (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015), which in turn requires cross border co-operation (Brenner, 2007; Hutnon, 2009; Jewkes, 2013; Bryant & Stephens, 2014). Two further related issues arise. The first is that the majority of the information sought by the police is held in cloud storage systems and traditional approaches to evidencing digital evidence cannot be easily applied to these external systems (Garfinkel, 2010; Ward, 2011; DeSousa, 2013). The second is that by attempting to access external devices via communications links, legislation pertaining to communications data, the Regulation of Investigatory Powers Act 2000 (RIPA, 2000) may be invoked creating further barriers for the police to obtaining the information they seek (Locke, Cooke, & Jackson, 2013; Qi & Edgar-Nevill, 2011; Edwards & Urquhart, 2016). All of these factors have the potential to cause

social media as a source of information and evidence for the police to be problematic.

Although social media is often associated with cybercrime, in this research the focus is on social media in criminal investigations in general and not cybercrime specifically. Social media incidence in an offence may not necessarily fall under the umbrella of cybercrime (Ward, 2007; Stuart, 2014). However, cybercrime offences have been noted to have a significant occurrence of social media (Wall, 2001; Jewkes & Andrews, 2005; Holt & Bossler, 2012; Gilespie, 2015). As such whilst cybercrime is not the direct focus of this research an overlap between the two exists, and so literature and previous studies on cybercrime were an important consideration. Academic research around the issue of cybercrime and police investigation is present, wide spread and has a strong focus on proposed models of investigation and frameworks that investigators can follow (Reith, Carr, & Gunsch, 2002; Casey, 2004; O'Ciardhuain, 2004; Perumal, 2009). They often include a strong technical aspect concentrating on devices that can be physically seized and then forensically examined (Casey, 2002; Carrier, 2003; Lyle, 2003; Baggili, Mislan & Rogers, 2007). As such, a large segment of this literature appears to be aimed at forensic investigators rather than general law enforcement practitioners. It is recognised however that cybercrime impacts on investigation strategies outside of the confines of digital forensic examination (Hunton, 2009). Information and communications technology is seen as moving from the realm of specialist forensic investigations into general everyday policing.

However, there is a limited understanding of how detectives in particular identify strategies and the reasons for doing so in order to deal with social media. This research addresses the investigative strategies that police officers from traditional police departments pursue when dealing with social media in their investigations. It identifies the decisions that officers make when presented with social media within an investigation and what drives officers to make those decisions. It utilises the most up to date guidelines for good practice in relation to digital evidence centrally available to officers in England (ACPO, 2012) in order to provide a benchmark against which to

compare officers' decisions and rationale. In laying out the decision- making process that officer's use, the research highlights where the opportunities lie for best practice and how to influence the behaviour of investigators in the future.

The overall aim of the research is to ascertain how social media impacts on officers' investigative strategies within their investigations. There are a variety of ways in which social media can do this. This study focused only on one of these - the material generated by the actors (victims, witnesses and suspects) within an investigation. The reason for this focus is driven by the researcher's own experience as a detective working in a Criminal Investigations Department (CID). The incidence of social media in their investigations posed questions as to how social media should be dealt with. These questions could not be adequately answered by colleagues or supervisors and as a consequence the researcher became interested in how social media is addressed in reactive investigations.

2.   Research questions

This research was designed around five questions. Together they sought to ascertain the impact of social media on investigations and the investigative strategies that police officers from traditional 'detective' departments pursue when dealing with it in their cases. They further looked to understand the decision-making processes behind those strategies. They then sought to identify the most up to date guidelines for good practice in relation to 'social media as evidence' available to officers and finally ask what recommendations could be made for policy and practice. The five questions are explored in more detail below:

The first question was to identify 'what proportion and type of investigations are impacted upon by social media?'. Social media was judged to have had an impact on an investigation where social media content was generated by the actors involved in the investigation. Social media content was further reduced into three categories: relevant material (CPIA, 1996), evidence in the investigation, evidence critical to the outcome of the investigation. How

investigations were impacted upon by social media was assessed in terms of a percentage of the total number of cases investigated by officers.

The second question was to identify 'what types of strategies detectives and investigators deploy when they encounter social media in a criminal investigation?'. This objective focused on identifying the practical decisions that officers made when they came across social media.

The third question went further and sought to understand 'what are the decision-making processes behind the strategies chosen by detectives when dealing with social media?'. In so doing an understanding was sought as to why officers pursued a certain strategy to fill a gap in our knowledge. First, if it is not understood why a decision is made, it is difficult to make a judgement on how sound that decision is. Secondly, this knowledge is required, if a meaningful attempt is to be made at altering decisions that are made by investigators. It was envisaged that these first three objectives would be achieved by two separate data collection methods.

Both data collection methods focused on investigations conducted by officers who are working in 'detective' roles. The first method examines crime reports generated or dealt with by officers in those departments. The second utilises interviews with officers on those departments. The rationale for focusing on detectives was driven by the previous small-scale studies conducted by the researcher, which gave an indication that detectives are more likely to deal with social media than their uniformed colleagues. Information from four different departments was sought for research data regarding investigations that had been conducted. They were from CID, Child Abuse Investigation (CAIU), Domestic Abuse Investigation (DAIU), and finally the authorities' bureau. The reason for choosing the first three departments, as opposed to any others, is that they are the most heavily populated departments with an investigative (detective) role. The final department – the authorities' bureau is a point of contact for officers requesting permissions for communications data of any type and they act as an advisory resource. It was chosen as they deal with any applications concerned with RIPA (2000) which is noted as having the potential to be

11

invoked when officers seek social media content held by providers (Locke, Cooke, & Jackson, 2013; Qi & Edgar-Nevill, 2011; Edwards & Urquhart, 2016).

Two police forces provided data for the research, these being Thames Valley Police and Avon and Somerset Constabulary. The purpose of obtaining data from more than one police force was to identify whether there are any differences in the data stemming from the culture and organisation of different police areas.

The fourth question posed was to identify 'what bench mark exists for investigators to assist them in choosing their strategies?'. To allow for an assessment of the strategies chosen by the officers, a bench mark is needed for comparison. A way of achieving this was to identify guidelines already in existence for dealing with digital evidence. The guidelines must not be so abstract that no tangible investigative strategy can be identified for investigators. A set of guidelines (ACPO, 2012) fitting these criteria was found to be provided by the Association of Chief Police Officers (ACPO).

The final question was to identify 'what recommendations can be made to investigators as to their strategies when they come across social media?'. The strategies offered by the guidelines were compared against those that officers were noted as having used themselves. The data obtained was scrutinised to ascertain any themes that are raised across different departments and different police areas. An analysis was conducted to determine any differences between the strategies suggested by the guidelines and those used by officers and then to identify best practice from the two. Best practice was constructed against three criteria:

1) That the material gathered through the strategies identified could be relied upon in court as evidence if so required.
2) That the strategies identified would provide for the easiest possible collection of the material.
3) That strategies identified would allow for the least resource intensive collection of the material.

Having identified the decision-making process, recommendations were made in how to achieve that best practice.

3.   Thesis Structure

The remainder of the thesis comprises of 5 chapters. Chapter 2 details the literature that was reviewed and was found to be relevant throughout the course of the study. The focus in this chapter is on problem solving models and decision making. In so doing the individual steps of problem solving models are examined. Then issues that social media poses to law enforcement agencies are explored. Subsequently an analysis is conducted of three specific heuristics - decision making rules that are noted as being particularly pertinent to policing. Finally, the ACPO guidelines and their suggested strategies in relation to social media are discussed.

Chapter 3 explains the methodology that was used together with the data collection methods. Due to difficulty in identifying established theory on investigator decision-making around social media encountered in investigations, grounded theory was adopted to analyse the primary data collected. This methodology is well-suited to building theory in a relatively unexplored field (Glaser, 1978; Schreiber, 2001; Goulding, 2002). Within grounded theory, the subjective position of the researcher is important in data analysis (Goulding, 2002; Mruck & Mey, 2007). In this study, the researcher is also an investigator with experience in working on criminal offences that involve social media. The impact of this insider perspective has been identified as being significant in the small-scale projects taken to date by the researcher and this position is explored in more detail. The rationale for using the two separate data collection methods is discussed as are their individual strengths and weaknesses.

Chapter 4 concerns itself with the analysis of the data obtained from the crime reports. It describes the categories of offence which are found to contain social media. Crime reports from each police area are examined separately, as are they for the three distinct departments of CAIU, CID and DAIU before being compared against one another. Strategies for dealing

with social media are identified and then their frequency is correlated against whether social media constitutes relevant material, evidence, or critical evidence to the outcome of an investigation.

Chapter 5 analyses the data captured from the interviews conducted with investigators. From the data are drawn a number of findings. These include the aims and objectives of investigators, how they view social media in terms of distinct properties, strategies that they use when dealing with social media and the rules that are utilised by officers when making a decision as to which strategy to choose. The findings in chapters 4 and 5 draw on the literature reviewed and are cross referenced against each other.

Chapter 6 evaluates the study, highlights the main conclusions regarding the impact of social media on investigator decision-making strategies from the data analysis and makes suggestions based on the results of the research. It identifies unique and original ideas that have been found during the course of the research. On the basis of this it makes recommendations as to the content of guidelines and equipment and practices that could be made available for investigators. The following chapter examines the literature that was reviewed prior and during the research. Significant due to the grounded theory methodology employed in this research was the timing of the literature review and this is discussed initially.

1.   Introduction

To begin with the timing of the literature review is discussed and the significance of when a review takes place when using a grounded theory approach. This provides an explanation as to why the evaluation of the data against existing academic literature was an ongoing process througout the course of the research and did not fully take place prior to the start of data collection.

Literature pertaining to the research aims was reviewed with each research question being considered individually. The researcher failed to uncover any literature that would inform the first question posed, which concerend itself with identifying the proportion of investigations impacted upon by social media within the parameters set by this study. The second and fourth research questions were found to be closely related when applied to a review of existing academic and professional knowledge. As such, they were considered jointly after literaure relating to the third research question was scrutnised. This third question sought to identify the decision making processes behind investigators' choice of individual strategies. Literature found to be relevant to this centred around decision making and problem solving. The individual steps of problem solving models were found to mirror investigators' behaviour seen in the data collected during the research. These steps included recognising social media as a problem, identifying its facets, defining the goals of the decision makers as investigators, and identifying rules by which decisions were made. Ten facets of social media were identified by investigators that defined social media as a 'problem'. Each of these is considered against existing literature. Four investigator goals were noted in the data collected from the interviews. These concerned the collection of evidence for court, identifying the suspect for the purposes of the investigation, maintaining the engagement of the victim and the safeguarding of individuals. These goals have previously been recognised

as relevant to investigators and police officers in general. Literature concerning these investigator goals is reviewed and their application to social media considered. Finally, three heuristics were identified as the main decision-making rules which investigators used. These were: Confirmation Bias, the Availability Heuristic, and the Representiveness Heuristic. These decision making rules and how investigators applied them to social media in their investigations is examined.

The second and fourth research questions identified strategies suggested for and used by officers. A review of academic and professional literature found processes present for dealing with digital forensic evidence. Issues with these processes when trying to apply to them to cloud based computing are analysed, the impact that this may have on the collection of social media evidence is reviewed and their general suitability for mainstream investigators considered. The ACPO (2012) guidelines were found to best address the question of a bench mark for strategies to be employed when investigators come across social media. The ACPO (2012) guidelines are outlined and subsequently analysed.

2.   The timing of a literature review when using grounded theory

In submitting a proposal for research the purpose of an initial review into existing literature is in order to identify gaps in existing knowledge (Hutchinson, 1993) and secondly to avoid methodological and conceptual hazards that have already been recognised (McGhee, Marland, & Atkinson, 2007). The knowledge however that a researcher holds and their prior experience regarding the area that is being researched is an important consideration when using a grounded theory approach (Glaser, 1978; Strauss & Corbin, 1994). This in turn has implications for when a literature review is conducted. The reason for this is that within grounded theory although the theory is seen to emerge from the data collected (Glaser & Strauss, 1967; Glaser, 1992), the researcher is a key component of the emergence of that theory as the theory is created through and by them (Cutcliffe, 2000). The literature review will affect the researchers knowledge

and so the timing of the literature review will have the potential to impact on the emergence of theory (McGhee, Marland, & Atkinson, 2007; Cutcliffe, 2000). As such reflection is critical for the researcher otherwise there is a risk that any theory construction is not impartial and overly influenced by the researcher's previous experiences and knowledge (Cutcliffe, 2000; Kennedy & Lingard, 2006; McGhee, Marland, & Atkinson, 2007).

Strauss and Corbin (1990) argued for reviewing literature early in the research for a number of reasons including: the stimulation of theoretical sensitivity; providing a secondary source of data; stimulation of thought in the researcher; and providing validity for the research. Glaser (1992) disagreed with this approach and in particular awareness of professional literature prior to the research and prior to codes and categories emerging from the data in order to prevent the emergence of new theory being affected by current knowledge. The approach adopted in this research as to when a literature was undertaken was that advocated by Strauss and Corbin (1990). The choice of this approach being adopted as opposed to that advocated by Glaser (1992) was influenced by three factors. The first of these factors is the process that is in place through which a proposal for research is submitted to the university, specifically the requirement for it to be accepted by the ethics committee prior to any research being undertaken. This has been noted by Strauss & Corbin (1998) as a structural barrier to not undertaking a literature review prior to any research being endorsed by a university. Secondly, the researcher's position as an insider researcher (Brannick & Coghlan, 2007; Drake & Heath, 2011), meant that a certain amount of professional knowledge in the area that the research was being conducted in was already held by the researcher. Thirdly the researcher had previous academic experience on decision making theory relating to economic theory.

In order to and whilst constructing the proposal for the research, literature was reviewed on decision making and strategies used in relation to social media and digital evidence specifically within the field of criminal justice, to idenfify whether the proposed research addressed a gap in current knowledge. Subsequently the knowledge regarding decision making that

17

was already known to the researcher through previous academic and professional experience was formalised through a review of normative and prescriptive models and heuristics. Accepting that this knowledge was already present in the researcher and that there was potential for it to influence theory building, further knowledge concerning decision making was sought to broaden the outlook of the researcher and in order to stimulate thought as suggested by Strauss and Corbin (1990).

3.   Literature pertaining to decision making

The third research question sought to ascertain the decision-making process behind the strategies deployed by investigators. This question sought to understand why a strategy has been chosen and the decision-making process behind the choice of a particular strategy. How a strategy is defined in the context of this thesis is in line with the meaning ascribed to it by Freedman (2013) and is detailed in the glossary.

Literature surrounding decision making is widespread amongst different academic (Dorfman, 1997, Jones, 2004; Chibnik, 2011) and professional (Cole, 2005; O'Neal, 2012; Moriarty, 2015) disciplines and can be divided into three categories: Heuristics (Elio, 2002; Gigerenzer, 2008), Normative / prescriptive models (Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011) and Positive or descriptive models (Einhorn & Hogarth, 1981; Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011). Whilst Heuristics can be subsumed within descriptive models, they are distinct enough that it is useful to identify them as a separate way to describe decision making. Furthermore, heuristics specifically have been identified as important in the way that investigators within the police make decisions (Adhami & Brown, 1996; Smith & Flanagan, 2000; Youngs & Canter, 2006; Stelfox, 2009; Rossmo, 2009; Zalman & Carrano, 2014; Smith & Tilley, 2015). Aspects of normative / prescriptive models of decision making were known to the researcher from the sphere of economic theory because of previous academic undertakings and heuristics because of professional learning prior to the research being commenced.

Normative or prescriptive models look to identify the optimal decision given a certain set of circumstances (Crozier & Raynard, 1997; Camerer, Issacharoff, Loewenstien, O'Donoghue, & Rabin, 2003). Such models can assist decision makers to identify this optimal choice where a decision is required. Positive or descriptive models in contrast seek to describe, understand and model the actual choices that are made by individuals (Einhorn & Hogarth, 1981; Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011). Heuristics describe rules that individuals fall upon when asked to make decisions often when faced with an inability to process all the information at their disposal. They explain some decision making, offering a quicker way for an individual to make a decision with less information whilst offering a degree of optimisation (Simon, 1955; Elio, 2002; Gilovich & Griffin, 2002; Snook & Cullen, 2008). What all these models of decision making have in common is that a distinct set of circumstances has been identified within which a choice is being made by the decision maker. The parameters in which the choice is being made are well defined and often observed under laboratory conditions. These models were examined against the data obtained from the interviews. It became clear however that they did not adequately explain the process that investigators were undergoing when coming across social media, and with reference to heuristics only offered a partial explanation.

4. Problem Solving vs. Decision Making

Four goals became apparent for investigators from the coding of the data obtained from the interviews that could not, other than ordering them from one to four as preferences when faced with a choice, easily be overlaid onto the models of decision making identified above. As such, a wider search took place within literature of how individuals approach not just decisions in specific settings but more widely situations where choices are made. This literature search took place during and after the coding process and thus was more in line with the approach advocated by Glaser (1992). That the literature reviewed prior to the coding process was rejected by the researcher as explaining what was found in the data was seen positively in

the context of the grounded theory methodology used. It demonstrated that that literature and models that the researcher believed to be relevant at the start of the research did not influence the researcher when seeking theoretical models to explain patterns in the data.

The core issue seen throughout this thesis and identified during the coding and analysis of the data is not solely that of decision making but more broadly problem solving. Therefore, in order to understand the findings, it is necessary to have an understanding of the literature surrounding problem solving. Models outlining situations where individuals are faced with an issue that is not clearly defined were found to be more aptly suited to the scenarios described during the interviews and how investigators approached social media. These models fall under the heading of 'problem solving' but are also in some cases described as 'decision making' models although they differ significantly to the models described earlier. There are many definitions of 'decision making' and 'problem solving' when considering situations where there is an undefined problem facing an individual with various overlapping characteristics identified under both definitions (Frauenknecht & Black, 2010; Hickson & Khemka, 2013). As an example, the definition of 'decision making' offered by Izzo, Pritz and Ott (1990) involves (1) stating what the problem is (2) setting out what choices are available to deal with the problem, (3) identifying what the consequences of each choice are, and (4) selecting the preferred or best choice to deal with the identified problem. This is similar to the definition of 'problem solving' as put forward by Wilson and Kirby (1984) which involves (1) defining the decision that has to be made, (2) collecting information on the issue, (3) considering what options are available to deal with the issue, (4) identifying the preferred option of how to deal with the decision, (5) planning and carrying out the chosen course of action, and finally (6) assessing the outcome of the decision that was made.

The interchangeable nature of the meaning assigned to problem solving and decision making in these models where there is an undefined problem facing an individual creates potential for any analysis of data against theoretical concepts to become confused (Frauenknecht & Black, 2010). This is particularly the case in view of the decision-making models described at the

start of this chapter which differ in nature to that described for example by Izzo, Pritz and Ott (1990). To avoid confusion, a set definition first of problem solving and secondly of decision making was used in this research. The intention in doing this was not to attempt to give preference to particular definitions of problem-solving and decision-making over others, but rather set out the definition for the purpose of clarity and applying clearly identifiable frameworks to what has been noted in the data.

The definition of problem solving as put forward by Pretz, Naples, & Sternberg (2003) was adopted. This model is represented in five clear and separate stages that an individual progresses through when encountering an unidentified problem, the model being cyclical in nature. These stages are as follows:

- Recognition that a problem exists

- Defining or framing the problem

- Identify the goals

- Developing a strategy to reach goals.

- Evaluation of actions in relation to the goals

In this definition, decision making is seen as being subsumed within the problem solving process but not fully constituting it (Shogren, et al., 2008; Frauenknecht & Black, 2010). Although this definition has been chosen, the five steps noted in the model or close approximations to them are seen in other problem-solving models (Bransford & Stein, 1984; Sternberg, 1985). A well-defined problem may have a relatively straightforward way to reach the goals of the person presented with it. However, if the problem is not well defined then the person who is presented with it must first frame what the problem is, subsequently identify goals that they wish to reach and then develop a strategy to achieve them. Factors that are found to influence this process are knowledge, cognitive processes, ability and structural context (Pretz, Naples, & Sternberg, 2003).

Decision Making for the purpose of this research is also defined in 5 separate stages as: "*a process used to make choices among contending*

21

courses of actions and includes the following steps: (1) identify possible
options, (2) identify possible consequences for each option, (3) evaluate
desirability of each consequence, (4) assess likelihood of consequences,
and (5) use a "decision rule" that identifies the best option and maximizes
well-being based on current beliefs and knowledge" (Frauenknecht & Black,
2010, p.113).

In the definition of decision making as depicted by Frauenknecht & Black
(2010) similarly to problem solving as put forward by Pretz, Naples, &
Sternberg (2003), there are clear and separate stages that an individual
progresses through. However, the steps involved in decision making as
defined by Frauenknecht & Black (2010) can be subsumed or form part of
the stages encapsulated in the problem-solving model as put forward by
Pretz, Naples, & Sternberg (2003).

5. Identifying social media as a distinct and unique problem

The two definitions of 'problems solving' and 'decision making' as used in
this research detail two distinct situations that an individual may experience.
In the first, there is a 'fuzzy' scenario (Pretz, Naples, & Sternberg, 2003)
where the problem is not initially clear to the person who comes across it.
This scenario falls under the definition of problem solving. In the second
scenario, the problem is well defined to the individual. This scenario falls
under the definition of decision making. Where a person comes across a
situation where a problem is not well defined, they must first recognise it as a
problem and subsequently define it (Getzels, 1982). An individual may not
even recognise the situation or scenario that they come across as presenting
a problem (Pretz, Naples, & Sternberg, 2003) and it has been suggested that
a significant amount of domain-specific expertise is required before an
individual is able to recognise and define the boundaries of a problem
(Simonton, 1999; Pretz, Naples, & Sternberg, 2003). As such, there was a
possibility that there would exist a correlation between the length of time
investigators had served in the police or worked in detective roles and
whether social media was recognised as a 'problem' and this was examined.

Recognition of a problem, as a first step in this process is often easier though than defining its boundaries. Having recognised a problem, the next stage as put forward in the model by Pretz, Naples, & Sternberg (2003) involves framing or defining it. This stage is influenced by knowledge, cognitive processes, ability and structural context (Pretz, Naples, & Sternberg, 2003). The study did not address cognitive processes or measure the ability of the investigators.

5.1 Distinctive facets of social media in relation to investigation

Social media has been noted as providing a number of issues for law enforcement agencies. Providers are seen to fail to engage with the police. There are two drivers of this behaviour identified in literature. The first is that of cost (Hunton, 2009; Kardasz, 2012). Responding to law enforcement requests inevitably requires person hours to provide the information requested. The preservation of information also illicits costs in the form of hardware. The second is that of reputation. Each social media provider has a unique identity which is coupled with the reputation that it has (Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). A part of this repution relies on the privacy that a social media platform offers its users and in particular privacy from government agencies (Barnes, 2006; Etzioni, 2016). Privacy as a marketing feature has become central to high-tech companies including but also beyond social media (Etzioni, 2016). There exists a fear that if this privacy is surrendered to state law enforcement agencies then users will move to a different social media application based in a state or region where that privacy is protected or not infringed upon (Greenberg, 2016). The most recent high profile case involving a tech company and the government is that of Apple's refusal to comply with a court order to assist the FBI in overriding the security features of the latest i phone (Etzioni, 2016).

This lack of response to law enforcement agencies has been noted not only on a voluntary basis but also when law enforcement agencies have applied for information using subpoenas and search warrants (Hodge, 2006; Boyd & Ellison, 2007; Ward, 2011; Kardasz, 2012). Although this refers to

applications through criminal justice mechanisms in the United States and not England in Wales, the majority of social media applications that are used in the UK are based in the United States (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015). As such they lie outside of the jurisdiction of UK law and any requests that rely on legislation that compels service providers based in the United States to divulge information takes place through judicial mechanisms in the United States. That co-operation between law enforcement agencies across different legal jurisdictions is required causes barriers in itself to the effective investigation of crime (Brenner, 2007; Hunton, 2009; Jewkes, 2013; Bryant & Stephens, 2014). In response, social media providers including Facebook, MySpace and Twitter have created their own protocols which dictate the information that they will provide in response to law enforcement requests (Trottier, 2012). This demonstrates a measure of their independence and ability to dictate rather than be dictated to. Law enforcement agencies however are pushing for greater access in both Canada and the United States to the content that social media providers hold through legislative and judicial measures (Trottier, 2012).

Whether social media is different in nature to previous types of communications data such as physical letters, telephone calls or e mails has been debated in U.S. courts of law (Hodge, 2006; Petrashek, 2010; Gagnier, 2011). This research failed to identify any criminal cases in Crown Court in England and Wales pertaining to the same issue.

Further to this the changing nature of social media has been widely acknowledged (Quan-Haase, 2008; Hogan & Quan-Haase, 2010; Kaplan & Haenlein, 2010; Kim, Jeong, & Lee, 2010; Lenhard, Purcell, Smith, & Zickuhr, 2010; Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). When new forms of social media develop they become an unknown quantity to investigators who need to acquire new knowledge in order to be able to adequately understand and frame them, as identified in the third category above. Although this research challenges the notion that the police lack the knowledge and skills to effectively deal with digital evidence (Jewkes & Andrews, 2007; Jewkes & Yar, 2008; Nicol, Innes, Gee, & Feist, 2004) or a new scenario that they have previously not dealt with (Stelfox & Pease,

2013) the acquisition of new knowledge nevertheless takes time and effort which competes with the normal demands on time that investigators have to manage (Innes, 2003).

The social media content of a given user account unless specifically or incidentally recorded on a physical electronic device of a user is held in a cloud based system or external storage (Garfinkel, 2010; Ward, 2011; DeSousa, 2013). The issue of how to access this information for any given account poses difficulties for the investigator (Ryan & Shpantzer, 2002; Sommer, 2004). Traditional approaches to collecting electronic evidence focus on seizing a physical electronic device and then creating an image of that device (Casey, 2002; Carrier, 2003; Ryan & Shpantzer, 2002; Lyle, 2003; Mocas, 2004; Baggili, Mislan, & Rogers, 2007; Biggs & Vidalis, 2009; Damshenas, Dehghantanha, Mahmoud, & Solahuddin, 2012). The image can then be presented in court as an exact duplicate of the original. It is argued that a copy of the data present on a device is not adequate and that a mirror image needs to be created in order for a court to accept any electronic data as evidence (Ryan & Shpantzer, 2002; Mocas, 2004; Damshenas, Dehghantanha, Mahmoud, & Solahuddin, 2012) otherwise the reliability and validity of the evidence can be challenged in court (Ryan & Shpantzer, 2002; Mocas, 2004).

This is the same advice that is provided to the police through the ACPO (2012) guidelines (Biggs & Vidalis, 2009; Damshenas, Dehghantanha, Mahmoud, & Solahuddin, 2012). That traditional approaches to recording electronic evidence were not applicable to social media was identified by investigators. The data that comprises the social media accounts of users is held on external to user electronic storage devices (Garfinkel, 2010; Ward, 2011; DeSousa, 2013) as identified above mainly in the United States (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015). These electronic devices cannot be seized and cannot be copied directly by UK law enforcement agencies. Whilst some data may be retained on electronic devices such as laptops, pads and smart phones in the memory cache (Garfinkel, 2010; Said, Al Awadhi, & Guimareas, 2011; Geddes & Pooneh,

2016), this will be incidental and a reflection of what the user has last viewed rather than the sum total of what is contained in their social media account.

6. Investigator goals

The identification of goals for individuals is the third step in the problem-solving model as put forward by Pretz, Naples, & Sternberg (2003). The following four goals were found to be both well documented in literature on investigators and pertinent to findings of the research as ranked aims of officers. These aims were identifed through the coding process from the data obtained from interviewing investigators:

1. Safeguarding individuals
2. Maintaining the engagement of the victim.
3. Identifying the suspect for the purposes of the investigation.
4. Collecting evidence in such a way that it would be accepted in court.

Each of these goals is explored in more detail below.

6.1 Collecting evidence in such a way that it would be accepted in court.

The collection of evidence for the purpose of satisfying prosecution requirements and subsequently the criminal court is a well-recognised and established objective of detectives and investigators (Maguire, 2003; Stelfox & Pease, 2005; Tong & Bowling, 2006; Stelfox, 2009). There are number of drivers for this objective.

First, even though a suspect may have been identified and arrested, there is a need for evidence to be collected. In England and Wales, it falls to the prosecuting agency to offer proof in the vast majority of criminal cases that the defendant has committed the offence, rather than the defendant proving that he is not guilty of the offence (Connor, 2009). This evidence must be collected in a way that is acceptable to a court (Stelfox & Pease, 2005; Tong & Bowling, 2006; Stelfox, 2009) before it can be put before a jury. Whether evidence is acceptable to a court is determined by several pieces of

legislation (Flanagan, 2008). This includes: The Police and Criminal Evidence Act (PACE 1984); The Criminal Procedure and Investigations Act (CPIA 1996); The Humans Rights Act (HRA 1998); The Regulation of Investigatory Powers Act (RIPA 2000) and the Investigatory Powers Act 2016 (IPA 2016). The latter, although clearly able to encompass social media communications data, was not found in the context of this research to generate any significant changes to legislation contained within RIPA (2000). Should evidence not be collected in line with those Acts then the court has the power to exclude the evidence, which may in turn threaten any potential prosecution (Stelfox, 2009). It is therefore not enough for an investigator simply to collect material but it must be collected in a manner which is acceptable and in line with legislation, which in itself takes considerable skill (Maguire, 2003). The Human Rights Act (HRA 1998) and The Regulation of Investigatory Powers Act (RIPA 2000) have been identified as impacting on the ability of the police to collect evidence from suspect social media profiles when using covert profiles or tactics to do so (Locke, Cooke, & Jackson, 2013; Qi & Edgar-Nevill, 2011; Edwards & Urquhart, 2016). However, there is a lack of literature concerning non-covert access to profiles of suspects and victims that is specific to the UK.

Evidence of cybercrime in general is more difficult to collect than traditional crime due to its physical absence at the locality of the offence (Wall & Williams, 2013). The difficulties in doing so are identified above when considering the facets that social media poses as an issue: social media providers' failure to engage with the police (Barnes, 2006; Hunton, 2009; Kietzmann, Hermkens, McCarthy, & Silvestre, 2011; Kardasz, 2012; Etzioni, 2016; Greenberg, 2016), a lack of legislation in relation to social media providers (Hodge, 2006; Boyd & Ellison, 2007; Brenner, 2007; Hunton, 2009; Ward, 2011; Kardasz, 2012; Jewkes, 2013; Bryant & Stephens, 2014; Duggan, Ellison, Lampe, Lenhart, & Madden, 2015), and the issue of 'accessing social media' (Ward, 2011; DeSousa, 2013).

Secondly, the police are required in law to pursue all reasonable lines of enquiry and collect and retain material that is relevant to the investigation that is obtained during those enquiries as set out in s.22, CPIA 1996. The

courts as a consequence of this legislation require the retention of material whether that assists or undermines the prosecution case in offering proof of the suspect's guilt. The reason for the introduction of this legislation is as a result of high profile wrongful convictions where the police were shown to have ignored, failed to investigate, failed to record or manufactured evidence to ensure a conviction (Jones, Grieve, & Milne, 2008; Milne, Poyser, Williamson, & Savage, 2010). The collection of material which may subsequently be introduced as evidence assists investigators in building a narrative to explain the events that they are investigating, which includes identifying what offences if any have taken place and suspects (Maguire, 2003).

Thirdly, there has been a drive to professionalise the police service (Stelfox, 2007; Flanagan, 2008) initially through the National Policing Improvement Agency (NPIA) and subsequently through the National College of Policing. A significant part of this drive to professionalise the police has focused on the collection of evidence. This has been conveyed to officers either through manuals and guidance (ACPO 2000; 2005; 2005a, 2006; 2012) or through training for example in the introduction of the Professionalising Investigation Programme (Stelfox, 2007). This guidance and training sets out standard operating procedures which place a requirement on investigators to both collect evidence and provide practical steps to do so. Further to what has been provided to the police as professional guidance there is also a significant amount of academic literature on proposed models of investigation and frameworks that investigators can follow (Reith, Carr, & Gunsch, 2002; Casey, 2002, 2004; Carrier, 2003; Lyle, 2003; O'Ciardhuain, 2004; Baggili, Mislan & Rogers, 2007; Perumal, 2009). Whilst it was evident during the interviews that investigators were not clear on the details contained within the guidance produced around dealing with digital media (ACPO, 2012), there was an appreciation expressed by each of the investigators interviewed that there were such rules in place and explanations offered of why such rules existed. Given the outlined statutory requirement for investigators to preserve material for court which if admissible may be presented as evidence; statuary rules setting out how

material can be collected by the police; and training that instructs officers to preserve and collect evidence, it is not surprising that investigators have identified collection of evidence for court as an aim with regard to social media.

6.2 Identifying the suspects

In addition to dealing with the collection and retention of material, s.22, CPIA 1996 defines an investigation as seeking to identify whether a person should be charged with an offence, or, if they have been charged with an offence, whether they are guilty of it. If consideration is given as to whether someone should be charged with an offence then they become a suspect in the investigation. In so doing, CPIA 1996 sets out the goals of officers undertaking an investigation. Whilst not specifically directing officers to identify suspects, in order to consider whether a suspect should be charged, they first need to be identified, and so this step of suspect identification is a prerequisite of what is required of officers in an investigation as set out by the law.

The goal of suspect identification has, however, been recognised previous to the enactment of this legislation in some of the earliest studies that specifically examined the work of detectives. These studies focused on the efficacy of detective work and the contribution that detectives had on solving crime (Isaacs, 1967; Greenwood, 1970; Greenwood, Chaiken, & Petersilia, 1976; Eck 1983) rather than explicitly on the decision-making processes used by them. The authors examined the ability of detectives to identify the suspect in a case (Isaacs, 1967), whether the suspect was arrested (Greenwood,1970), the amount of work or detective effort that was involved (Greenwood, Chaiken, & Petersilia, 1976) and whether a case had a successful resolution (Greenwood, Chaiken, & Petersilia, 1976; Eck 1983). The choice however of using suspect identification and 'clearances' in court as a function of the success of detective work was made by the researchers in these studies, as opposed to being identified by the detectives themselves and the organisation for which they worked. Greenwood (1970) for example writes:

"*The apprehension of criminal offenders is central to the criminal justice system*" and "*Few will disagreee, however, that killers, rapist, robbers, thieves, and those who commit violent attacks should be arrested and punished. This is one reasons that this study is confined to programs leading to the arrest of the most serious criminal offenders*" (Greenwood, 1970, p.1).

This may well have reflected public opinion of what was seen as the role and primary aim of the police at the time that this research took place (Braga, 2008) and it is difficult to argue against the need to arrest serious offenders. However, in their development these studies (Isaacs, 1967; Greenwood, 1970; Greenwood, Chaiken, & Petersilia, 1976; Eck 1983) other than to change the emphasis from whether the suspect was identified to whether they were arrested or succesfully convicted in court, did not alter the focus from the suspect as the function of the success of detective work. Furthermore, these studies form the basis of subsequent literature (Bayley, 1998, 2002; Tong & Bowling, 2006) that identified detective work as 'suspect-centred'.

Other research (Brandl & Frank, 1994; Maguire, 2003) though has questioned the measurement of the effectiveness of detective work in terms of focusing solely on arrests or clearances. It was highlighted that the weakness of focusing on arrests was that an investigation may uncover that an offence did not actually take place (Brandl & Frank, 1994), or that during the investigation the victim had withdrawn or made a wish that they did not want the suspect to be arrested (Brandl & Frank, 1994). In those circumstances an arrest would not be appropriate, but yet the work of the detective had by other measures been effective. In so doing, although Brandl & Frank (1994) did not identify this explicitly as an aim for detectives in their work, the third goal identified in this research was touched upon, which was importance of the victim and maintaining their engagement in the investigation. Maguire (2003) whilst giving a system level explanation as to why the identification of suspects is a central aim of investigative departments also identifies other aims of detective work including the collection of intelligence.

Social media has been credited with being used to identify suspects in a number of police investigations (Trottier, 2012). During the Vancouver riots of 2011 images of rioters captured on the phones of members of the public were subsequently posted on Facebook and used by the police to identify suspects. However suspect identification through social media can be achieved with other means than just by photographic evidence. The content of suspect social media profiles are often scrutinised for information by law enforcement agencies to obtain more information about them (Cheng, 2010; Lynch, 2010; Kerrigan, 2011; Denef, Kaptein, Bayerl, & Ramirez, 2012), including who their friends and family are (Trottier, 2012) leading to their identification and physical location. Furthermore, telecommunications data such as IP addresses can identify the physical location where suspects are or have used social media, that can subsequently lead to their arrest (Schell, Martin, Hung, & Rueda, 2007; Kao & Wang, 2009; Brunty & Helenek, 2015). Whilst collection of evidence and identification of the suspect have been identified as clear goals of investigators in this study, they do not hold primacy against the remaining two discussed below.

6.3 Maintaining engagement with victims

Police attitudes and behaviours towards victims have changed significantly over the last 30 years (Temkin, 1997) becoming more positive (Stelfox, 2009) and resulting in a more positive experience for victims at the hands of the police (Temkin, 1997; 1999). The identification of maintaining victim engagement as the secondary aim of investigators is in line with this change. In particular, the way that victims of rape and sexual offences are treated appears to have been influenced through significant changes that were introduced in the late 1980s as a result of criticism of police practices (Adler, 1991; Lees & Gregory, 1993; Temkin, 1999; Jordan, 2001; Horvath & Brown, 2009). This included the introduction of special examination suites, greater numbers of female investigators and training programmes that challenged perceptions of rape victims (Temkin, 1997). Training for officers in the police has also been noted to shift towards more postitive attitudes with regard to victims with intellectual disabilities (Bailey, Barr, & Bunting, 2001). Further to

this, studies which have focused on investigators' choice as to when victim interviews should take place, evidence sensitivity and concerns about victim care on the part of the police (McMillan & Thomas, 2013).

The growing importance of the victim in the criminal justice process has also been reflected in legislation that has been enacted, beginning with the first Victim's Charter published in 1990, revised in 1996 with a new code coming into force in 2013 (Ministry of Justice, 2013). Whilst these studies show a more positive experience from the perspective of victims, other research on investigator beliefs shows an attitude of suspicion towards victims of rape and serious sexual assault whilst acknowledging that there are policies in place to encourage belief in the victim (O'Keeffe, Brown, & Lyons, 2013). Other studies have highlighted a tension between the 'responsibilities of the police' and the 'needs of the victim' (Jordan, 2001) showing the aims of investigation and the victim to be competing.

Attempting to evidence social media often resulted in investigators wishing to seize the electronic device on which the victim had accessed social media on, and in so doing taking it away from them. This was often at odds with the wishes of the victim and thus created a barrier to maintaining their engagement. This reflects the strong attachment of individuals to their electronic mobile communications devices and specifically mobile phones (Oksman & Rautiainen, 2003; Rosen, 2004; Campbell, 2007; Green & Haddon, 2009; Vandebosch & Van Cleemput, 2009). The attitudes of investigators in this study appear to suggest that first of all, engaging and maintaining a relationship with the victim is the second goal (out of four) of officers when ranked and when dealing with cases that involve social media. Secondly, whilst a tension clearly exists between the needs of the investigation and the needs of the victim, the needs of the victim take primacy over the needs of the investigation in all the cases discussed. This may represent a shift in attitudes towards victims by investigators.

6.4 Safeguarding individuals

There are different focuses on how to identify individuals that require 'safeguarding'. (Madoc-Jones, Hughes, & Humphries, 2015). Some literature identifies at risk groups (Walkalte, 2007) including children, adults with learning disabilities, elderly persons (Stevens, 2013) or individuals in particular social circumstances (Madoc-Jones, Hughes, & Humphries, 2015) whilst other literature focuses on the type of crime that the individual has been a victim of, for example violent crime and sexual offences (Madoc-Jones, Hughes, & Humphries, 2015). It is recognised that assessing the needs of a victim is a complex task (Simmonds, 2009) but that the requirement for safety and protection from future victimisation is a key need for victims (Spalek, 2006; Walklalte, 2007). During the course of the interviews questions were not posed as to how officers defined safeguarding as it was not until the interviews were concluded and the coding process was quite advanced that the significance of 'safeguarding' became apparent.

The importance of 'safeguarding' as a concept in policing has emerged and developed as the police, its activities and how it is structured has shifted towards a 'problem orientated' approach (Eck & Spelman, 2005). The shift towards safeguarding has been gradual and sustained (Richardson-Foster, Stanley, Miller, & Thomson, 2011) and is most evident in the areas of domestic violence, children, adults with learning disabilities, elderly persons. Following a similar pattern to that described above regarding victims of rape, police were subject to substantial criticism around their response to domestic violence and the needs of the victim during the 1980s and 1990s, which led to an improvement in both identifying victims and tending to their needs (Buzawa & Buzawa, 2002; Richards, Letchford, & Stratton, 2008; Richardson-Foster, Stanley, Miller, & Thomson, 2011; Madoc-Jones, Hughes, & Humphries, 2015).

Over time the focus from female and adult victims has widened to encompass children (Burton, 2000; Shields, 2008) and legislation was introduced, which places obligations on public agencies including the police to protect vulnerable children and adults (Adoption and Children Act 2002; Children Act 2004; Laming, 2009). The response to these requirements has

been seen in the creation of Multi Agency Safeguarding Hubs in which the police are embedded whose role is to: 1) identify risk, 2) identify victims and intervene in order to, 3) reduce harm to individuals, families and communities (London Borough of Merton, 2014). Through these hubs a high volume of referrals are made to social services by police officers (Rivett & Kelly, 2006). Officers are also required to undertake risk assessments on both adults and children present at domestic incidents (HM Government, 2010) and studies have shown that officers attending domestic violence incidents consider the welfare of children and adults present (Buzawa & Buzawa, 2002; Richards, Letchford, & Stratton, 2008; Richardson-Foster, Stanley, Miller, & Thomson, 2011). The comments made by investigators in this study shows them identifying risk, seeking to identify victims at risk and attempting to reduce the harm to them. This demonstrates that 'safeguarding' as a concept is being applied to investigations involving social media and not just in the confines of domestic violence incidents. Safeguarding was identified as the most important aim in investigations that involved social media. However the concept of safeguarding is not simply tied to protecting victims from interaction with social media through education (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006; Griffith & Roth, 2007; Savirimuthu, 2012), increasing privacy settings (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006; Griffith & Roth, 2007; Savirimuthu, 2012), or blocking other users from making contact with them (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006; Griffith & Roth, 2007; Savirimuthu, 2012). It also relates to using social media to identify the location of a victim (Schell, Martin, Hung, & Rueda, 2007), identifying whether there are any other victims in danger (Carr & Hilton, 2011), and locating the suspects (Schell, Martin, Hung, & Rueda, 2007; Kao & Wang, 2009; Brunty & Helenek, 2015) in order to prevent serious harm from coming to victims. All of these aspects of safeguarding were identified from the coding of the interview transcripts.

Within UK policing structures, protecting and safeguarding has been organisationally placed under the remit of Public Protection Units or departments (Sherlock & Cambridge, 2009; Coliandris, 2015). The exact

structures and names between different police areas vary but Public Protection Units invariably encompass the areas of Child Abuse Investigation, Dangerous, Violent and Sex Offenders, Vulnerable Victims and Domestic Abuse Investigation (Sherlock & Cambridge, 2009; Coliandris, 2015). The areas where safeguarding applies has continued to expand with the internet being recognised as being an area of risk and posing a threat to individuals (Coliandris, 2015; Wate & Boulton, 2015). Given this substantial cultural, organisation and statutory shift, it is not suprising that safeguarding was evidenced as an important consideration for investigators in this research.

7. Decision rules used by investigators when choosing how to physically secure evidence

When considering how to physically secure social media evidence investigators who were interviewed were shown to rely on their previous experiences. They directly transposed their experience from past events relating to the collection of non social media evidence and applied it to social media. This pertained to taking statements, photographing, obtain screen shots of and printing off social media content. The ability of an individual to associate a new situation with a past one is well documented (Orasanu, Martin, & Davison, 2001; Moriarty, 2015; Cookson, 2017). A perfect match is not required with a previous situation for the individual to make use of the rules that they used in the previous incident (Orasanu, Martin, & Davison, 2001; Moriarty, 2015; Cookson, 2017). This is true of the use of previous situations by investigators to inform their behaviour around social media even though as discussed above social media poses a new problem for investigators with facets that make it unique and different from previous problems encountered by them.

A number of heuristics have been identified that shape individuals behaviour in relation to police work. Heuristics have been portrayed in both positive (Gigerenzer & Todd, 1999; Snook & Cullen, 2008; Rossmo, 2009) and negative ways (Findley & Scott, 2006; Zalman & Carrano, 2014). From a

negative perspective heuristics have been singled out as the central cause of a number of miscarriages of justice and labelled under a catch all term of 'tunnel vision' (Findley & Scott, 2006; Snook & Cullen, 2008; Rossmo, 2009; Zalman & Carrano, 2014). Conversely the positive perspective on heuristics is that whilst legislation prescribes that officers are evidence gatherers and should pursue all proportionate lines of enquiry (CPIA, 1996) officers are constrained by: the amount of time and information (either a lack or excess of) that is available to them, their experience, distractions to their work, a lack of resources and co-ordination with other personnel (Youngs & Canter, 2006; Snook & Cullen, 2008; Rossmo, 2009; Zalman & Carrano, 2014). For this reason, it is not only impossible for officers to examine all possible lines of enquiry and all possible suspects, but also not desirable (Snook & Cullen, 2008). In these instances, where the investigators are bound by non optimal circumstances, heuristics allow for effective decisions to be made (Snook & Cullen, 2008; Rossmo, 2009). Whilst this previous work on heuristics has focused on lines of enquiry that investigators pursue and their approach to suspects (Findley & Scott, 2006; Rossmo, 2009; Rassin, 2010; Stelfox, 2009; Smith & Tilley, 2015), witnesses (Ask & Granhag, 2007) and what evidence they gather, this research identifies that heuristics are also evident in the process that investigators use to gather evidence and specifically evidence found within social media.

Three heuristics were identified during this research as cognitive biases influencing officers to use previous approaches to evidence collection when considering how to physically evidence social media. These are Confirmation Bias, the Availability Heuristic, and the Representiveness Heuristic. Although labels have been attached to these heuristics or biases, such as 'confirmation bias', it should be noted that different authors use slightly overlapping defnitions and terminology (Klayman, 1995; Nickerson, 1998; Findley & Scott, 2006). This research does not seek to address the superiority of one term over another when applied to a particular concept but uses specific labels for the purpose of clarity.

Confirmation or verification bias describes the behaviour of individuals searching for information that confirms their view or hypothesis in such a

way that it impedes their ability to challenge that view or hypothesis (Klayman, 1995; Nickerson, 1998; Oswal & Grosjean, 2004). It has been widely recognised that police officers seek evidence that confirms their hypothesis of a set of events or that build a case against a suspect that they have in mind for an offence (Findley & Scott, 2006; Rossmo, 2009; Rassin, 2010; Stelfox, 2009; Smith & Tilley, 2015) as well as their approach to witnesses (Ask & Granhag, 2007). By doing so, they effectively speed up the process of investigation. However, at the same time they do so to the detriment of keeping an open mind to other scenarios that may have taken place and what a witness may offer. This bias is also evident in relation to how the evidence is collected. By putting emphasis on cues around social media that correspond to previous experiences and disregarding cues that identify social media as a different and unique type of evidence, investigators avoid cognitive dissonance. This enables investigators to continue using known methods of evidence collection without having to build a new mental model and consider new ways of collecting and evidencing social media.

The Availability Heuristic describes the tendency of individuals to utilise information, tactics or strategy that is easily available. By doing so, officers can make more effective use of their time by gathering evidence which is easily available and less resource- intensive to collect. The weakness that manifests itself is that evidence, which may be pertinent and point to a different hypothesis and suspect, but which is not readily available, is overlooked (Rossmo, 2009; Stelfox, 2009). This heuristic has been widely acknowledged as having a bearing on the evidence that police officers collect (Ask & Granhag, 2005; Rassin, Eerland, & Kuijpers, 2010). It can also be applied to using a strategy or tactic that has been recently used to collect evidence (Ask & Alison, 2010; Kebbell, Muller, & Martin, 2010; Moriarty, 2015).

The representativeness heuristic (Garb, 1996; Brannon & Carson, 2003; Moriarty, 2015) describes individuals comparing the similar features of a previous situation that they have been in to a current one and on that basis using the same decision-making rationale to reach an outcome. Investigators during the interviews spoke about cases that they had taken to court and

strategies and tactics that were used in those investigations not with regard to social media material but other electronic evidence. They then applied those same strategies and tactics to social media based on their positive experience in court. Whilst this type of behaviour can be seen as driven by the representativeness heuristic (Stelfox, 2009; Moriarty, 2015) it is also reflective of professional learning cycles (Dewey, 1933; Argyris & Schön, 1978; Kolb, 1984; Gibbs, 1988; Johns, 1995; Brookfield, 1998; Thompson, 2000; White, Fook, & Garnder, 2006) and inductive reasoning (Keane & Eysenck, 2010). Professional learning cycles incorporate past professional experience into present practice, whilst models of inductive reasoning allow individuals to reach conclusions based on the expanding of a particular observed set of circumstances into a generalisation (Sloman & Lagnado, 2005; Bryant, 2009a, Keane & Eysenck, 2010). Although heuristics describe the decision making of individuals based on previous experience, they may not include all of the individual's current knowledge and experience. As such heuristics may distort an individual's inductive reasoning by for example only identifying readily available knowledge to support a conclusion (availability heuristic) or identifying knowledge in line with a conclusion that the individual is seeking to confirm (confirmation bias). Furthermore, heuristics need not require a conscious process of reasoning. The closeness of various models describing human thought processes, in this case inductive reasoning (Sloman & Lagnado, 2005; Bryant, 2009a, Keane & Eysenck, 2010), heuristics, reasoning by analogy (Holyoak, 2005; Bryant, 2009a) and professional learning models has been identified as showing that such models are somewhat arbitrary in delineating and camouflaging what are similar forms of thinking (Keane & Eysenck, 2010). All of these models fall under the umbrella of 'positive' or 'descriptive' models that seek to describe and understand the actual choices that are made by individuals (Einhorn & Hogarth, 1981; Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011). Whilst not excluding the validity of models of inductive reasoning and reasoning by analogy or their potential application to decision rules employed by investigators during the problem-solving process, clearly identifiable examples of such rules were not visible in the data.

8. ACPO (2012) guidelines and strategies for investigators to use when encountering social media found within professional and academic literature

The second research question sought to identify strategies that investigators used when they came across social media in their investigations. This objective was rooted in the coding and examination of the data collected from both the crime reports and the interviews. In contrast the fourth research question, sought first to find and then compare guidelines against the strategies identified as being used by investigators in answer to the second research question. From the perspective of a literature review however, these two research objectives were closely aligned. The search criteria used to review literature to find strategies that have been noted as being used by investigators simultaneously found strategies suggested for use by officers. When searching for strategies and guidelines that investigators both used and could follow when coming across social media, both academic and professional literature was considered.

Although literature examining decision making by investigators when encountering social media in their cases has not been identified, academic research around the issue of cybercrime, police investigation and preservation of digital evidence from seized devices is wide-spread. In this literature there is a strong focus on proposed models of investigation and frameworks that investigators can follow (Reith, Carr, & Gunsch, 2002; Casey, 2004; O'Ciardhuain, 2004; Perumal, 2009; Biggs & Vidalis, 2009; Damshenas, Dehghantanha, Mahmoud, & Solahuddin, 2012). In other words laying out standard operating procedures that make some of the decisions on behalf of officers. They often include a strong technical aspect concentrating on devices that can be physically seized and then forensically examined (Casey, 2002; Carrier, 2003; Lyle, 2003; Baggili, Mislan & Rogers, 2007). As such, a large segment of this literature appears to be aimed at forensic investigators rather than general law enforcement practitioners. Whilst the forensic examination of electronic devices in line with those guidelines was not conducted by officers themselves, one identified strategy and tactic that investigators were using to evidence social media when coming across it, was to seize electronic devices such as computers, tablets

and mobile phones and submit them to HTCUs to extract the information from them.

The closest and most up to date guidelines aimed at investigators rather than forensic scientists was found to be that provided by the ACPO (2012) guidelines. At the time of writing (September 2017) these are the guidelines that are still in place (Bryant, 2016), directed to be followed by the National College of Policing and employed by digital investigators in the UK (Biggs & Vidalis, 2009).

There are four general principles that are at the centre of the guidelines stemming from the 5 principles introduced by the High-Tech Crime Conference in 1999 (Ryan & Shpantzer, 2002). The first is that investigators should not change the original data in any way that is held on an electronic device. It goes on to say as identified above that computer software may change data without the user being aware that this has happened. The second principle is that if original data is accessed it should be done by persons who are competent to do so and be able to give evidence in court. It further identifies that some data will not be stored locally but externally. If this data is to be recovered then it stipulates that the person doing so is competent to do so and give evidence in court, and that consideration is given to legislation in the jurisdiction from which the data is being obtained. It does not specify who would be competent to obtain this information or by what means this could be done. The third principle states that there should be an audit trail kept so that an independent party could achieve an identical result if the same steps were pursued by them as the investigator undertook. The final principle is that the investigator in the case is responsible for ensuring that the above principles are adhered to.

Investigators were however also conducting the analysis of devices themselves and introducing digital evidence in ways that did not incorporate the imaging of the original data. This included taking screen shots of and photographing social media accounts. In so doing they were not adhering to the suggested digital forensic models. The use of forensic models of digital recovery cited above in criminal cases stems from the US Supreme Court judgement of Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579

(1993) (Ryan & Shpantzer, 2002; Berger, 2005; Meyers & Rogers, 2005).
This ruling introduced tests of scientific validity and reliability (Ryan &
Shpantzer, 2002; Berger, 2005; Meyers & Rogers, 2005) that requires expert
principles and methodology to be followed when dealing with evidence that
is to be accepted by the court. Subsequently The International High-Tech
Crime Conference in 1999 adopted 5 principles (Ryan & Shpantzer, 2002)
which the ACPO (2012) guidelines mirror, for dealing with digital evidence.
This research has failed however to find case law in England and Wales in
relation to digital evidence and more specifically social media (Biggs &
Vidalis, 2009) that related to the exclusion of digital evidence. In the absence
of a court ruling in the UK, the implications of investigators not adhering to
these guidelines and forensic models of recovery of digital evidence are
explored further below.

8.1. ACPO guidelines and examination of electronic devices

The four principles as set out above are most easily applied to digital
evidence that is contained on a device that can be examined. The guidance
is reflective of the literature on forensic recovery of evidence from devices
(Reith, Carr, & Gunsch, 2002; Casey, 2004; O'Ciardhuain, 2004; Perumal,
2009). That these guidelines were being adhered to was clearly visible in
both the crime reports and from the interviews. Investigators were seizing
items and then either submitting them to the HTCUs or using specifically
sanctioned equipment at police stations for imaging the devices that they
were seizing. There were two barriers that were identified in both the crime
reports and the interviews to submitting devices to HTCUs. The first was the
amount of time that it took to examine a device. The second was that the
HTCU within TVP would not accept multiple devices but rather employed a
triage process for submissions. As mentioned above this resulted in some
items that investigators had a suspicion contained material relevant to the
investigation not being accepted for examination. As a consequence, one of
the investigators examined a device themselves to ascertain whether there
was evidence present on it. Once they identified that there was the HTCU

then accepted the device for examination. By this point however data on the device is likely to have been altered by the investigator accessing it, violating both the first and second principles of the guidelines. Given the pressure on HTCUs (Kshetri, 2009; Yar, 2013; Bregant & Bregant, 2014), their reluctance to accept all devices for examination is understandable and the triage of devices has become an accepted process. However, the investigator without having violated the first two principles would have never recovered the evidence. The question then arises if the purpose of the examing the device by the investigator is to find evidence for the purpose of court, is there any point in doing so if this evidence will be subsequently excluded by the court due to the principles in the guidelines being violated.

There are two principal mechanisms for excluding evidence in court. The first is through s.78 of PACE 1984 and the second is the ability for a judge to stay proceedings on the grounds of abuse of process under common law (Fitzpatrick & Taylor, 2001). Under common law evidence can be weighed up with on the one hand its probative value considered and on the other whether it causes prejudice against the aggrieved without being sufficiently connected to the case itself (Murphy, 2007). Although this principle is encompassed by common law in the UK it is also well recognised in other jurisdictions (Murphy, 2007). S.78 of PACE 1984 refers to the exclusion of evidence if it interferes with the defendants ability to have a fair trial (Murphy, 2007). Thus evidence which has been obtained illegally or unfairly can be excluded (Murphy, 2007).

With regard to the exclusion of evidence there are identified principles under which evidence can be excluded from a trial (Fitzpatrick & Taylor, 2001). These include 'bad faith' on the part of investigators, 'impropriety' which relates to breach of codes of practice and how bad faith and impropriety will subsequently affect the outcome of the case (Fitzpatrick & Taylor, 2001). A factor which falls under these headings is that of reliability and how evidence has been obtained (Fitzpatrick & Taylor, 2001). If there is reliable evidence available then this should be the principal evidence used (Fitzpatrick & Taylor, 2001). If evidence has been obtained that breaches the rights of suspect then similarly it may be excluded (Fitzpatrick & Taylor, 2001).

However simply because evidence has been gathered in an improper way does not mean that this will happen. In the United States if evidence has been gathered in a way that has violated the rigths of the accused then it will not be accepted in the court. This is not the case in England and Wales, rather the fairness of the trial is considered (Murphy, 2007). This is crucially important as even if the way in which evidence has been obtained breaches ACPO's (2012) own guidelines it may still be accepted. If identifying with the goal of the investigator to obtain evidence that is presentable in court, having some evidence, whether obtained improperly or not is better than having no evidence at all, as this evidence may still be accepted. The research has failed to find case law in England and Wales in relation to digital evidence and more specifically social media (Biggs & Vidalis, 2009) that related to exclusion of digital evidence.

8.2. ACPO guidelines, social media and identified objectives

Whilst the guidelines (ACPO 2012) are fairly extensive with regard to obtaining evidence from devices that have been seized, in relation to social networking they are limited. There are two identified objectives in the guidelines with regard to 'internet chat' which would as a term appear to encompass social media. The first is to ascertain who the suspect is and the second is to capture the content of the communications. These objectives clearly fit with the investigators goals identified from the interviews of obtaining evidence for the purpose of court; identifying the suspect; and partly that of safeguarding other victims by identifying the suspect. The objective of safeguarding does however include further elements as discussed above, for example identifying other possible victims in order to protect them. Furthermore, the third objective of maintaining victim engagement is not touched upon at all in the guidelines. It is perhaps unsurprising that aims other than evidence are not present in guidelines specifically constructed to deal with evidence. However the aims of 'maintaining victim engagement' and 'safeguarding' are not encompassed by other guidelines relating to digital material. Furthermore if guidelines relating

to evidence are to be overridden due to other objectives, it may be helpful to investigators if the circumstances in which this may happen were detailed.

8.3. ACPO guidelines, social media and suggested strategies

The guidelines suggest a total of four strategies / tactics for obtaining evidence when dealing with social media. First, they identify that networking sites often contain a function that allows chat logs to be saved. This was a tactic to physically collect social media evidence found to be used by investigators from the data obtained during the interviews. The guidelines are somewhat vague however in how this information is to be extracted. It suggests that these saved logs be placed onto a removable media device. Who completes this extraction onto the removable storage devices is not stipulated. However, the copying of such information from an electronic device as discussed above will not be a mirror image of the information on the device but rather a copy. If the user of the device or the investigator were to do it then it would likely infringe upon the first, second and third principles of the guidelines. It is not clear why having saved the chat logs onto the device, they should not be then evidenced by downloading the information using equipment at police stations or through submission to the HTCU. This is the course of action suggested with regard to electronic devices containing data earlier in the guidelines.

Secondly, the guidelines go on to state that if no removable media is available that the logs should be printed out. The printing out of chat logs and social media pages from a given profile was a tactic that was evidenced as being used by investigators in the data. This tactic was used by investigators when using accessing social media profiles from computers that were connected to printers. However as revealed during the course of the interviews many of the electronic devices where such 'chat' took place include mobile phones and tablets where removable storage is not possible nor is there a straightforward ability to connect the device to a printer.

The third recommendation in the guidelines is that if information is being accessed that is in transit then the authorities bureau should be contacted.

Accessing information on social media servers will undoubtedly mean that information will be in transit from the server to the user's device or whatever device the investigator is working and attempting to access the information from (Taylor, Haggerty, Gresty, & Hegarty, 2010; Mason & George, 2011; Taylor, Haggerty, Gresty, & Lamb, 2011; Chung, Park, Lee, & Kang, 2012). However no further guidance is provided as to what the contact with the authorities bureau should achieve or the aims of doing so. Contact with the authorities bureau was a tactic seen during to the interviews to be adopted by investigators either for the purpose of obtaining advice or for the purpose of obtaining the content of a social media profile from the provider directly.

Finally, in line with the above the only direct reference made to social media in the guidelines states that the best information will be provided by the service provider. It recognises however that the service provider may not be based in the UK and may not provide the information on request in any case. As such ACPO (2012) guidelines recommend that the investigator "*should always secure a copy of what is seen as this may be the only opportunity to secure this evidence before it changes*" (ACPO, 2012, p.34). This comment is not expanded upon and appears to be a catchall strategy that is at odds with the rest of the guidelines and particularly with regard to the four principles detailed above.

Established methods of digital forensic collection of evidence concern themselves in the main with the seizure of devices (Casey, 2002; Carrier, 2003; Lyle, 2003; Baggili, Mislan, & Rogers, 2007; Biggs & Vidalis, 2009; Damshenas, Dehghantanha, Mahmoud, & Solahuddin, 2012) and not 'cloud computing' as discussed above. For this reason, it has been suggested that the ACPO (2012) guidelines specifically do not easily encompass new forms of digital evidence such as cloud computing (Biggs & Vidalis, 2009; Damshenas, Dehghantanha, Mahmoud, & Solahuddin, 2012; Zargari & Benford, 2012).

Whilst all the investigators made reference to being aware of guidelines around digital evidence, none of them referred directly to the ACPO (2012) guidelines although there were aspects of these guidelines that were mentioned such as not using work computers to conduct research on profiles

in order not to leave a footprint. The finding that investigators were not aware of where specific guidelines originated from or their detail, has significance for the dissemination of any future professional practice, but was outside of the scope of this research. However, a repeated view of investigators was that if the situation justified it particularly in relation to safeguarding, then these guidelines could be over ridden.

9. Conclusion

The reasons for the researcher conducting a literature review prior to the collection and coding of the data whilst employing a grounded theory methodology was explained. This is the method that is espoused by Strauss and Corbin (1990) and during this review models of decision making were considered. It was however found during the research that the approach taken by investigators when social media was encountered could not be overlaid onto descriptive or normative models of decision making or those that encompassed heuristics that had been reviewed. Due to this further literature was assessed during and after the coding process and it was found that 'problem solving' models (Bransford & Stein, 1984; Sternberg, 1985; Pretz, Naples, & Sternberg, 2003) are better equipped to describe how investigators approach social media. This was significant as it validated the independence of theory emerging from the data rather than the researcher being overly influenced by the content of the literature reviewed prior to the start of the research.

The first four steps of 'problem solving' as defined by by Pretz, Naples, & Sternberg (2003) were recognised as being acted out by investigators and this evidenced in Chapter 5. The first of these steps is a recognition that social media presents a problem, which was identified by all the interviewees. The second step is to identify the facets of the problem that social media presents. Facets that frame social media as a problem for law enforcement agencies have been recognised in existing literature and were explored. These facets were identified by investigators and noted in the data from the interviewees. The third step - the identification of the goals of the

problem solver was seen in terms of four hierarchical aims that investigators pursue. All four aims have been previously identified in literature examining police and more specifically detective work. However, they have been either assumed to form part of detective work by researchers in the case of evidence collection and suspect identification or in relation to all four goals they have been noted as being prescribed onto the police through legislative changes and governmental pressure. The identification of these aims by investigators themselves and in a hierarchical order is an original way of identifying how investigators approach the issue of social media and will be discussed in chapter 5. The remaining steps of the 'problem solving' model correlate to the processes noted as occurring within normative, descriptive and heuristic decision-making models (Shogren, et al., 2008; Frauenknecht & Black, 2010).

Strategies used by and available to officers examining social media during their investigations were searched for. The majority of these pertained to processes related to examining physically recovered electronic devices and were aimed at digital forensic investigators rather than general officers. The closest and most up to date guidelines aimed at investigators rather than forensic scientists were found to be those provided by the ACPO (2012) guidelines. It was shown that although social media is considered within them, there are significant inconsistencies with the strategies / tactics offered for dealing with social media and the principles on which the guidelines are built on. Furthermore, the guidelines do not fully encompass two of the aims that investigators have, namely maintaining the engagement of the victim and the safeguarding of individuals.

The following chapter discusses methodology employed in this research, including grounded theory that was touched upon in this chapter when considering the timing of a literature review.

1.   Introduction

This chapter concerns itself with the methodology employed during the research and the approach taken to collecting data from two separate sources, crime reports and interviews conducted with investigators. To begin with, the grounded theory methodology and the approach to coding the data that was adopted is discussed. The issue of being an insider researcher when employing a grounded theory approach is then considered. Following this each of the two data sources are examined individually, beginning with crime reports. An explanation of police crime recording systems is given. The reasons for using crime reports in this research are outlined as is their predicted strength and the constraints that they have in providing data to answer the research questions posed. The sample size of the crime reports is discussed as are the problems that were encountered in collecting the data. Next the decision as to why crime reports from the three investigative areas of child abuse, domestic violence and general office criminal investigation were chosen as opposed to more specialised departments that may have a higher likelihood of dealing with cybercrime is explained.

The second source of data for the research were interviews conducted with investigators. To start with, the reasons are given for choosing interviews, specifically semi-structured interviews as a method of collecting data to answer the research questions posed and in particular the third research question. Next, the content of the interview schedule consisting of five separate sections is outlined. Sample size is then considered with attention given to the obstacles that are present in gaining access to investigators for research interviews. Following this, the limitations of semi-structured interviews and of using qualitative data to examine cognitive processes are reflected upon.

2. Grounded Theory Methodology

As was discussed in the introductory chapter, there was no established theory identified on investigator decision making around social media. For this reason, grounded theory was adopted to analyse the primary data collected. This methodology is well-suited to building theory in a relatively unexplored field (Glaser, 1978; Schreiber, 2001; Goulding, 2002). Glaser and Strauss identify two separate types of theory generation – substantive and formal. Substantive theory is formed specifically in relation to the data from which it originates and does not attempt to generalise outside of this. Formal theory seeks to explain relationships between concepts found in the data (Goulding, 2002). This research sought to build more than Substantive Theory by taking data from different police areas and investigative departments.

A system of coding was used to examine the crime reports and the interview transcripts. The way in which data is coded, seperates two distinct approaches in grounded theory (Kendall, 1999), that proposed by Strauss and Corbin (1990) and that presented by Glaser (1992). During this research, the system of coding that was put forward by Strauss and Corbin (1990) in *Basics of Qualitative Research* was used. This is a three step system of coding, which in contrast to the model offered by Glaser (1992) uses an additional intermediate step in the data analysis named 'axial coding'. The first level of coding, groups data together into categories. To begin with, these are likely to be numerous and based on description. However, as the coding process goes on categories are collapsed into each other to form fewer overarching ones. These overarching or higher categories become more conceptual in nature. The relationships between these conceptual categories can then be sought, which provides the theory. Axial coding develops these conceptual categories by formally identifying the conditions that allow each category to be formed. These conditions include the context, strategies and outcomes in which that category can exist.

This intermediate step it is argued allows the researcher to add structure to the way that the data is examined and allows the researcher to be systematic in their approach. The detractors of this method argue that axial

coding places a restrictive framework on the data that prevents theory that otherwise might emerge, from doing so (Kendall, 1999). The reason for this is that the conditions identified by Strauss and Corbin (1990) as pertinent for understanding how categories are formed may not encompass all the theoretical links that are present in the data between categories. Not withstanding this argument, the more systematic approach was adopted. The reason for this was that as an insider researcher, as was demonstrated in the pilot studies undertaken prior to this research, there were preconceptions present around anticipated results in the data. The systematic approach to analysing the data was used in order to curtail the influence of the ideas that may have been introduced into the research due to this insider perspective, which is further discussed below.

3.   Police Crime Recording Systems

Each police force uses crime recording systems, which record criminal incidents in line with Home Office national crime reporting standards (Home Office, 2018a). Each crime recording system if used diligently records the type of criminal incident that has been brought to the attention of the police. An offence is recorded either if:

1. There is an identified victim
2. The police to their knowledge believe that an offence has taken place.
3. On the balance of probabilities there is no credible evidence to the contrary that a crime has taken place

or

4. If the points to prove that an offence has taken place against the state are evidenced.

However, if it is used effectively it should also provide a comprehensive overview of an investigation and the investigative actions that have been considered by officers conducting the investigation. The National College of Policing, provides draft national standards for professional investigators

(National College of Policing, 2014), which includes those officers qualified as detectives. Within the core performance criteria expected of a detective is included: "*Fully document all decisions, actions, options and rationale in accordance with current policy and legislation.*" (National College of Policing, 2014, p.2). There are various places where these decisions, actions and rationale can be recorded, however it is often the case that the crime recording system is designed so that this information can be recorded within it, and is used to do so by officers (National College of Policing, 2014). As such, within each crime report there exists the strong possibility that the circumstances of the investigation as well as any actions undertaken or considered are recorded, including investigative actions around social media. Crime reports have clearly not been created for the end purpose of academic research. As such using the definition that primary data is "*collected at first hand for the specific purpose of addressing the criminological issues in questions*" (Jupp, 1989, p.46) and that secondary data is "*observations collected by other people or other agencies with other purposes in mind*" (Jupp, 1989, p.46) this form of data collection falls into the latter category. However, crime reports in the context of this research are akin to self-reporting surveys. Officers and investigators, whose decision making is at the centre of this research have the opportunity to detail the information sought in the first three objectives outlined in the introduction within crime reports. They record the type of crime that has been reported and / or investigated and the elements of the crime itself, which in turn has the ability to identify whether social media is involved and in what way. Furthermore, as detailed above, crime reports are also designed to allow officers to record decisions, actions, options and rationale. In addition, there exists a framework put forward by the National College of Policing for officers to use when making decisions (National College of Policing, 2014a) termed the 'national decision model' (NDM). The model was initially developed by the National Police Improvement Agency on behalf of ACPO (NPIA, 2012). The model is purported to be suiteable for all decision making in a police setting including operational and non operational situations. As such there may have been an expectation that this model would feature in

51

investigators' decision making and been either visible in the crime reports examined or discussed during the interviews.

This was precisely the data that was sought in order to achieve the first three research objectives.

As a result, crime reports as a method of data collection in this research proposal, enjoyed the benefits noted in both primary and secondary data (Kothari, 2004). This included the following advantages that secondary data collection offers: minimal preparation time as no data collection mechanism had to be constructed (for example a questionnaire or interview plan); no organisation was needed with regard to the distribution of a data collecting mechanism; and as permissions were given to have access to the data by both Avon and Somerset Constabulary (ASC) and Thames Valley Police (TVP), the issue of low response rates associated with collecting primary data via questionnaires was avoided. These facets meant that a large amount of data was collected with a lower cost placed on the researcher. Importantly however, the crime reports had the potential to provide the benefit that primary data offers, in that data collected was in line with the objectives of the research.

3.1 The choice of department

Three police forces in England and Wales were initially approached and asked to provide anonymised crime reports that pertained to cases that civilian investigators and detectives had investigated. The choice of departments from which to obtain a sample of crime reports was a significant issue. There exist numerous roles and departments within the police that detectives traditionally occupy. These include: Major Crime enquiry teams; CID, CAIU; DAIU, Specialist Rape and Serious Sexual Offence Units; Serious and Organised Crime Units, Burglary and Robbery Teams, Area Intelligence Teams, Economic Crime Units, Cyber Crime Units and many others. Although the study was exploratory, the wider the range of case types and sample of investigators that was examined, the greater the extrapolation that could be drawn from the data.

For this study, three areas of investigative policing were chosen from which sample crime reports were taken. These areas of investigation were: CAIU; DAIU and CID. When deciding which areas of investigation to focus the research on, literature concerning social media that was examined prior to the submission of the research proposal was considered. Although literature does exist specifically concerning strategies employed around social media and police investigations it relates to either the use of social media as an intelligence tool (Trottier & Lyon, 2011; Trottier, 2012; Schneider, 2016) or as a communication aid for the police (Trottier, 2012; Denef, Bayerl, & Kaptein, 2013; Schneider, 2016). In contrast, this research focuses on strategies used relating to social media content that is created by the actors within the investigation and that is subsequently treated as relevant material or evidence. More generally, literature that examines cybercrime describes types of offences that may feature social media as generated by the actors in the investigation, for example crimes concerning child grooming (Wall, 2001; Jewkes & Andrews, 2005; Holt & Bossler, 2012; Gilespie, 2015). In these cases, the social media content would likely form part of the relevant material and / or evidence. This literature recognises that local police areas have created specialist units that deal specifically with offences like child grooming and more generally cybercrime, such as Paedophile Online Investigation Teams or dedicated cybercrime units (Jewkes & Andrews, 2005; Manzhai, 2012; Wall & Williams, 2013; Nowacki & Willts, 2016). Furthermore, it is highlighted that some areas of investigation are more likely to come across cybercrime than the three areas of investigation chosen, for example the area of Fraud Investigation (Burns, Whitworth, & Thompson, 2004). Thus, a consideration existed whether to draw on crime reports from investigative areas that the literature highlighted as more likely to encounter cybercrime. These as discussed above would likely have a significant incidence of social media in their cases generated by the actors in the investigation.

Whilst acknowledging this, the focus has remained on the three chosen departments for two reasons. First, this research seeks to understand how social media affects the bulk of front line detectives and not a smaller

specialised section of the police. Police officers not only from specialist departments including general response officers are expected to deal with cybercrime (Holt, Belvins, & Burkert, 2010; Taylor, Fritsch, Liederbach, 2014; Bossler & Holt, 2012). The distinction between larger established departments and smaller more specialist units is important. Smaller units have access to greater resources, training and equipment (Jewkes & Andrews, 2005; Marcum et al., 2010; Wall & Williams, 2013). As a consequence, there may be significant differences between their approach, strategies and decision making in relation to social media to that employed by detectives in other departments. Furthermore, there is a lack of literature examining how the majority of police officers approach and deal with cybercrime (Holt & Bossler, 2012).

The three chosen areas of investigative policing are staffed by detectives or experienced civilian investigators that either support or are the officers in charge of their own investigations and take up the bulk of serious and complex crime investigation at a Base Command Unit (BCU) level (Maguire, 2003; Chatterton, 2008). Whilst in different forces at different times specialist units of investigators are set up to deal with particular aspects of crime (Maguire, 2003), at the start of 2014 (the time frame from which the samples were obtained) these three areas of investigation were distinct within the two forces that the crime reports were taken from.

There does not exist at the point of writing a comprehensive list of the number of detectives that operate within England and Wales or the numbers in which they occupy specific departments (Police Federation of England and Wales, 2015). However, Home Office data (2015) on police officer functions gives an indication of possible numbers totalling 27,626 police officers working within general office Criminal Investigation Departments (CID), specialist units made up from CID, Child, Sexual, and Domestic Abuse investigation departments and missing persons. Additionally, 2036 civilian staff members are shown as working in those departments. A further 9190 police officers are shown to be working across the areas of intelligence, vice, vehicle crime, special branch, fraud, drugs and burglary.

54

Although each of these departments would traditionally involve detective roles, there are no current figures of the ratio of police to detective constables in those departments, only numbers of officers and civilians working within them. Furthermore, the figures do not capture the number of officers and detectives that are working on regional teams or within the National Crime Agency. However, what is shown is that the three investigative areas chosen in this study occupy a significant portion (approximately 3/4's) of the total pool of officers and investigators in departments that detectives occupy.

Secondly, the focus of this research is on social media and not cybercrime in general. The distinction between the two is significant. Whilst cybercrime offences may involve social media (Wall, 2001; Jewkes & Andrews, 2005; Holt & Bossler, 2012; Gilespie, 2015), social media incidence in an offence may not necessarily fall under the umbrella of cybercrime (Ward, 2007; Stuart, 2014). Although widely written about, there is no universal definition of what cybercrime constitutes and it seen as covering a wide range of activities (Wall, 2001; Gordon & Ford, 2006; Jewkes & Yar, 2008; Clough, 2011; Newman & Clarke, 2003; Gilespie, 2015). However the main approaches of how to define cybercrime require that at least part of the offence is formed or facilitated by a cyber element – not in terms of evidence but about how the crime is committed (Wall, 2001; Broadhurst, 2006; Gordon & Ford, 2006; Ajala, 2007; Jewkes & Yar, 2008; Clough, 2011; Gilespie, 2015).

However, social media does not need to feature in the commission or facilitation of the offence for it to form evidence or relevant material in an investigation (Hodge, 2006; Petrashek, 2010; Gagnier, 2011). For example, communication via social media between offender and victim that pertains to a domestic rape that has already occurred and is being investigated becomes very relevant to the offence. It was unknown prior to the analysis of the data what proportion of cases that contained a social media element would fall outside of the definitions of cybercrime. As such, literature which identified departments that dealt with the highest incidence of cybercrime

were not used to inform which areas of investigation would be sampled for incidence of social media.

3.2 Crime reports and sample size

The sampling size in grounded theory is determined by the data collected. Data collection stops when new data that is being collected no longer modifies or adjusts the theory that is built by the researcher (Schreiber, 2001; Day, 2002). Ideally therefore, crime reports would have been requested in small batches until a saturation point had been reached with regard to the data and theory construction. However, it is the case that the request for anonymised crime reports incurs a cost on the police forces providing them due to the need for someone to first identify them and then secondly provide them in a useable format to the researcher. Furthermore, an organisation such as a police force will be better placed to decide whether to accept a request for this information if the request is not open ended (for example a researcher asking for permission to have access to an unknown number of crime reports) but finite in number. For this reason, a fixed number of crime reports were requested. Had it become clear after the analysis of the requested crime reports that saturation of data had not occurred, then the position would have been re assessed with a view to further crime reports being requested. This would have been done with consideration being given to this having an impact on the police forces providing them and whilst knowing that further data collection methods would be employed. In this case, no more additional crime reports were asked for as saturation was deemed to have occurred.

It was initially envisaged that each of the three forces would provide 150 crime reports, 50 from each of the three areas of investigation outlined above, which would allow a total of 450 reports to be examined. All three forces initially agreed to provide this data. However, one later declined to participate citing limitations on the resources that would be needed to provide the data. This meant that first of all, the amount of data obtained would have been reduced by a third. Secondly the breadth of data was

limited to two forces rather than three, which in turn limited the findings of the research, if compared to a study in which there were three participating forces. To compensate for this loss, an additional 150 crime reports were obtained from each of the two forces that did agree to participate bringing the total examined to 600.

In line with the accepted ethical guidelines for the research (British Society of Criminology, 2006; ESRC, 2012), the crime reports were requested with the investigating officer's details, their supervisor, the names of the actors within the investigation and geographical locations having been anonymised. It became clear however within a short space of time to both police forces providing the data that the resources that were required for this, were not available. There is no automated way to anonymise crime reports, and for anonymisation to take place each report had to be examined by someone and personal details manually anonymised. This was too costly a process for the forces to undertake in terms of working hours incurred. Consequently, a substantial amendment to the ethics documentation was submitted and accepted that allowed the researcher themselves to anonymise the crime reports. The anonymization was carried out by the researcher on police IT systems and once completed, the data was removed from police premises. This allowed data to be collected that would otherwise have not been made available.

Crime reports were provided in the chronological order that they were created in from the start of 2014. This constituted a consecutive sampling technique (Schuster & Powers, 2005; Bowers, House, & Owens, 2011; Acharya, Prakash, & Nigam, 2013; Sharma, 2017). Outside of seasonal and temporal bias it provided a random allocation of investigators within each of the three chosen departments, not differentiating between age, sex, length of service, experience, geographical location or type of investigation. The data collection began in earnest midway through 2015. There was a balance to be struck between obtaining the most recent crime reports and allowing investigations to be completed to see what strategies had been pursued. The investigation of cybercrime within which as discussed above social media is noted to feature is relatively fast moving (Gillespie, 2015; Moore,

2016). Therefore, the older the data collected, the greater the chance that investigative strategies noted in that data will have changed in comparison to the present moment. Conversely, complex cases take time to investigate. On average across England and Wales in 2015 it took 20 weeks from when an offence took place to when a person was charged in relation to it, with the longest average period of 25 weeks in the force areas from which the crime reports were taken (Ministry of Justice, 2016). Obtaining a sample of investigations that were instigated too recently would mean that they would be devoid of data. A period of 18 months was judged prior to the point from which data collection began to be sufficient for the majority of investigations to have been concluded. As such crime reports were requested to be collated chronologically from January the 1st 2014. This allowed time for investigations to have been completed whilst giving reasonably current officer investigative practice.

3.3 Constraints in the data offered by crime reports

Two criteria have been put forward as important when determining the quality of research data gathered through self-reporting. They are reliability and validity (Lincoln & Guba, 1985; Kirk & Miller, 1986; Winter, 2000; Golafshani, 2003; Gadd, Karstedt, & Messner, 2011). Reliability is described as consistency in the data that is being reported (Kirk & Miller, 1986; Winter, 2000; Golafshani, 2003; Gadd, Karstedt, & Messner, 2011). Put a different way, it is whether the same reporting tools examining the same data on more than one occasion provide the same or similar response (Thornberry & Krohn, 2000).

Validity refers to the concept of whether the information that is recorded is truthful (Kirk & Miller, 1986; Winter, 2000; Golafshani, 2003; Gadd, Karstedt, & Messner, 2011). A more apt way of describing it is whether the responses that are recorded match the interpretation of what has occurred or subjective reality of the researcher. Reliability and validity can vary without correlation to each other. The concept of reliability and validity with regard to qualitative data is important as it describes how dependable, consistent and

transferable the research is (Lincoln & Guba, 1985; Patton, 2002; Golafshani, 2003) and ultimately makes the research defensible (Johnson, 1997).

There are two well-practiced methods for testing the reliability of data (Thornberry & Krohn, 2000). Both were used in this study to check the reliability of the data. The first method is the re-testing of the data collection method used. The second is the cross-checking of the results of the analysis of the data using other indicators. The sample size in this study consisted of 600 crime reports, from two different police forces and three different departments within those two separate police forces. This effectively allowed for the re-testing of the data in different geographical and professional areas. With regard to cross checking the results from the data analysis of the crime reports, this was conducted through two different methods. The first was by examining the information that had been recorded in the supervisory reviews of the investigators' managers. This provided a second source of information from a different individual on the same circumstances of an investigation. The second was through comparison of the data obtained from the crime reports to a different data set that being semi structured interviews with officers.

With regard to validity, a number of facets have been put forward as assisting in its measurement (Thornberry & Krohn, 2000), with three being commonly cited. The first of these is criterion validity. This describes the measurement of results against an external bench mark (Thornberry & Krohn, 2000; Crow & Semmens, 2008). During the review of the literature no previous studies with similar objectives or methodology were found. In line with the fourth objective however, a set of guidelines were identified (ACPO, 2012) that give a point of reference regarding decision making around social media. The fifth objective requires comparison of the data collected against this benchmark. This provided some validity for the data collected. The second facet is that of content validity. This describes whether the method of data collection is suited to measuring what the study sets out to achieve (Thornberry & Krohn, 2000; Crow & Semmens, 2008). As has been detailed above, the data that was sought contained in the crime reports had the

potential to answer the first three research objectives. The third facet is that of construct validity. This describes whether the data being collected is related in theoretically expected ways to other concepts or constructs that can be measured (Thornberry & Krohn, 2000; Crow & Semmens, 2008). Three objectives in this study are set out that are closely linked with each other, those being the first three. If data became apparent in relation to one of the objectives and had this type of validity, then it would likely become evident in one of the other two objectives.

There are however limitations with collecting data through crime reports. Case files, which encompass not only the crime report that contains the investigation log but all other relevant material (for example statements, officers written notes, computer and phone downloads) do not contain a full record of what has taken place in an investigation and often contain errors (Alison, Snook, & Stein, 2001; Canter & Alison, 2003; Horvath & Brown, 2006). Furthermore, the third research question seeks to ascertain the decision-making process and case files as a whole have been noted as not revealing the personal, professional and case specific knowledge on which detectives base their decisions (Feist, Ashe, Lawrence, McPhee, & Wilson, 2007). This was highlighted in a pilot study undertaken prior to this proposal. An examination of 100 crime reports showed then that the depth with which officers recorded their decisions was not always detailed enough to allow for meaningful analysis of the data to take place. Secondly with anonymised crime reports, there is no possibility to further explore information and decisions taken by investigators noted in the crime reports. This would be desirable even if the crime reports contained a rich amount of information, as it would allow for clarification of issues and questions that arise as a result of what is contained in the crime reports.

As such, from the outset it was anticipated that the data collected through the analysis of crime reports was likely to only fulfil the first two objectives of the research. A further method of data collection was deemed necessary to achieve the third objective, which is addressed below and involved conducting interviews with officers and investigators.

3.4 Classifying crime reports that have social media involvement

In all, a total of 600 crime reports were reviewed and anonymised. Each crime report from both policing forces comprised of four distinct parts:

- Crime categorisation. This defines the category of offence that best describes the circumstances of the incident.
- The initial description of the circumstances of the incident. This description may not have been completed by the detective or investigator overseeing the case, but rather by the creator of the report. This could be the first attending officer to a report of a crime or police call centre operator to whom the crime is reported to.
- The log of the investigation maintained by the officer or investigator in the case.
- Supervisory reviews of the officer in the case.

Each report was examined for any reference of social media within it. When mention of social media was found that was in line with the parameters set out in the introduction, the type of crime that it referred to was noted in conjunction with the area of investigation that it fell under – CAIU, DAIU or CID.

Although ostensibly appearing a fairly simple process of classification, it presented a difficulty in terms of identifying the correct category of crime. The reason for this is that a set of circumstances that falls into or is encompassed by one type of crime category will often also naturally fall into other crime categories. The following circumstances are an example of a situation which could be classified under different crime definitions: an offender sending harassing and malicious communications via 'Facebook messenger'. This set of circumstances could be classified under the offence of harassment as defined by s.1 of the Protection from Harassment Act 1997 or the offence of malicious communications as defined by s.1 of the Malicious Communications Act 1988 (Geach & Haralambous, 2009). Furthermore, had a substantive offence taken place prior to the sending of these messages and the recipient was the victim of the substantive offence, with the person sending the messages being the offender of the substantive

offence, then it might also fall under the crime definition of 'witness intimidation' as defined by s.51 of the Criminal Justice and Public Order Act 1994. In addition to this, as an investigation progresses, it may become clear that the incident would be more accurately classified under an alternate offence category with any charges brought against a suspect having the potential of being different again - for complex cases a decision which is undertaken by the Crown Prosecution Service (CPS).

That a sequence of actions constituting an incident can overlap different offences is well recognised (Devlin, 1970; Shea, 1974; Ashworth, 2010; Owusu-Bempah, 2015) meaning that a defendant could be charged with different offences for the same actus reus and mens rea (Devlin, 1970; Shea, 1974; Ashworth, 2010; Owusu-Bempah, 2015). This also means that two defendants who have committed a similar 'actus reus' (Herring, 2014; Connor, 2009; Allen, 2011; Herring, 2014) under a similar 'mens rea' (Connor, 2009; Allen, 2011; Herring, 2014) can be charged with alternate offences (Devlin, 1970; Shea, 1974). The issue is not unique to the legal system in England and Wales but is also recognised in the United States (Brown, 2008; Chemerinsky, 2009) where significantly the decision as to what charge to lay in a spectrum of applicable offences has been argued to be aribtary (Chemerinsky, 2009).

Within England and Wales except for a range of less serious offences the decision of which charge to lay against a defendant rests with the CPS (Ashworth, 2010; Owusu-Bempah, 2015) notwithstanding an influence being present from the police as the cases are brought to the CPS by them. There is however no clear and absolute guidance as to what offence should be charged in circumstances where multiple offences apply to the same incident (Ashworth, 2010), with the end decision resting with the CPS and later at trial with the judge themselves (Ashworth, 2010; Owusu-Bempah, 2015).

For police forces, the procedure or rules under what offence a set of circumstances is classified under is set by criteria outlined in the Home Office Counting Rules for Recorded Crime (HOCR) (Home Office, 2016). Three rules are particularly significant to this research. The first is the 'one crime per victim rule'. This dictates that if the circumstances of the incident

fall under multiple crime definitions, then only one crime is recorded, this being the most serious one. The most serious crime is one either judged to be the most serious by the individual recording the crime or incurring the greatestest penalty on sentencing. The second is the 'principal crime rule'. This dictates that if there is a series of crimes contained within an incident, then one crime will be recorded, this being the most serious crime. The third is the 'finished incident rule'. This dictates that if a series of different crimes are reported to the police by one victim at the same time where the victim and offender(s) are the same, then one offence will be recorded, this being the most serious one.The analysis of the data showed that these three rules could mask the way in which social media impacted upon the investigation, which is evidenced in the following chapter.

These rules can be broadly, although not uniformly, related to the behaviour of prosecutors when deciding what charge to bring against a suspect. As described above when applying the 'one crime per victim' rule one aspect of the decision with what offence should be recorded against a set of circumstances, is the gravity of sentence that such an offence would carry on conviction. This is also borne in mind by prosecutors when they are assessing what offence to charge a defendant with (Ashworth, 2010).

It is accepted that the official statistics of crime that the HOCR provide do not reflect the actual levels of crime that are present in society (MacDonald, 2002). The cause of this includes police not recording crimes that are reported to them (Maxfield, Lewis, & Szoc, 1980) and crimes that are committed but are not reported to the police (Hough & Mayhew, 1983; Levitt, 1998). Both of these causes become evident when Home Office statistics are compared against other crime surveys such as the British Crime Survey (Brand & Price, 2000; MacDonald, 2002). Reasons for police not applying or recording crimes uniformly even when they are reported is not only due to the different ways in which an incident can be defined as exemplified above, but also due: to the discretion of officers (MacDonald, 2002), differing levels of proof required before an incident is deemed to have happened (Simmons, Legg, & Hosking, 2003), political motivation (MacDonald, 2002), and an unwillingness by individual officers to take on investigations when crimes are

reported (Maxfield, Lewis, & Szoc, 1980) in order to control their workload. When analysing the data, the issues of officer discretion and differing levels of proof required before an incident is recorded as a crime were evident.. Nevertheless, the HOCR criteria were used initially when detailing the type of offences where social media incidence is present, the reasons for this being fourfold.

First, the focus of the research is on the strategies adopted in investigations and the decision making process behind them. The crime that is not reported to the police, but recognised as taking place in surveys such as the British Crime Survey is not investigated, and so does not fall within the parameters of this research. Secondly, the rules and criteria set out in the HOCR are universally used by the Police in England and Wales (Home Office, 2016) and are well understood. Even if there is a lack of uniformity between how different police areas record crime, there is no other method of crime recording that police forces use that could be analysed. Using the same rules for crime classifications in this research as police use allows for it to be analysed by practitioners in the field of criminal justice with greater ease than were the research to rely on a set of new crime recording rules or a case by case decision by the researcher on each set of circumstances examined. Consideration was given to the way in which charges are brought against defendants as a way of classifying incidents, but again, as discussed above, this process is subjective and does not follow specific guidance that can be uniformly applied. Thirdly, one of the reasons for standardising the crime recording decisions is that the decision of what crime a set of circumstances constitutes is often a subjective one. As discussed above even with the HOCR in place, Her Majesty's Inspector of Constabularies (HMIC) acknowledges that there will be a degree of subjectivity present (HMIC, 2012). As such, whether the researcher looked at each crime report on a case by case basis to determine the crime classification or devised their own crime classification rules,it would be a process or decision that could easily be challenged and thus undermine the validity of the research. Finally, the researcher is an 'insider', which brings with it an additional risk of preconceptions influencing the research (Brannick & Coghlan, 2007; Drake

& Heath, 2011) in what is already noted as being an area of subjectivity. By removing the classification process from the researcher and using a process that has been put in place by a third party, it prevented the influence of the insider from affecting the research in this area.

Once reports had been identified that contained incidence of social media, then how social media was approached by the officer or investigator in the case and their supervisor was recorded and subsequently coded.

4. The choice of interviews as a method of collecting data

It was anticipated that data present in crime reports would not be able to effectively answer the third research question. The limitations of crime reports in providing data identified within literature was discussed above. Those limitations were confirmed and became evident when the crime reports were analysed and although strategies that have been used by investigators are noted in crime reports, the rationale behind the decision to use a specific strategy was not explicit. When the data from the crime reports was coded a correlation was noted between the variation and frequency of strategies and tactics used and whether social media formed critical evidence, evidence or relevant material in an investigation. The reason behind this however could only be implied and cannot be confirmed solely on the information contained within the crime reports. To be able to find the rationale for this and other strategies noted, a second set of data was collected in the form of semi-structured interviews. It was envisaged that, in an interview, the rationale for using a certain strategy could be ascertained.

A semi-structured format was used to conduct the interviews. When using the term 'semi-structured' interview, it was understood to have several characteristics (Gillham, 2005; Crow & Semmens, 2008; May, 2011). First, the same topic areas were explored with each interviewee (Gillham, 2005; Crow & Semmens, 2008; May, 2011). If an area of interest was not covered by the interviewee then they were prompted with a question (Gillham, 2005; Crow & Semmens, 2008) in order for that topic area to be delved into. This

structure was sought in the interviews first to ensure that the topics which addressed the research questions posed were discussed and secondly because it allowed for testing of the reliability (Thornberry & Krohn, 2000) of the data against that obtained from the crime reports.

An interview schedule was constructed to assist the researcher in keeping a semi-structured format. This interview structure was shaped by a preliminary study undertaken prior to this research, a process that is noted as being typical of semi structured interviews (Gillham, 2005; Crow & Semmens, 2008). The interview schedule was divided into six separate parts. The first section asked interviewees to: describe their investigator experience; define social media; describe in what proportion of investigations social media featured and finally the types of investigation that it appeared in. This enabled the cross-referencing of the data obtained from the crime reports for the purposes of testing its reliability (Thornberry & Krohn, 2000).

The second section asked interviewees to provide an example of: a case involving social media that had not resulted in a prosecution; the investigative strategy that was pursued, other strategies that were considered but not used; the reasons for considering those strategies and considerations of ACPO guidelines. The third section concerned questions about investigative approaches that were used by the interviewee that had resulted in successful prosecutions and the reasons for considering those strategies. Specific cases were not asked for. These two sections sought most obviously to answer the second and third research questions posed, to ascertain the strategies used by investigators and the decision-making process behind those strategies.

The fourth section asked interviewees about factors that had had an impact on the way they dealt with social media and pivotal moments in their careers that affected their approach. The literature review undertaken prior to the data collection phase indicated that previous experiences would likely significantly influence decision-making (Adhami & Brown, 1996; Smith & Flanagan, 2000; Youngs & Canter, 2006; Stelfox, 2009; Rossmo, 2009; Zalman & Carrano, 2014; Smith & Tilley, 2015). The questions in this section

looked to identify the past experiences that investigators themselves were aware of as impacting on their decisions.

The fifth section asked interviewees to consider social media and how the police deal with it; what they envisage as best and worst-case scenarios for the future for police investigations and social media; and constraints that they currently face.

Finally, an open scenario was put to the interviewees that included an element of social media with several strategies and tactics available to pick from in response to the scenario. The choice of strategy made by the interviewee was noted and explored. This section is discussed in more detail below.

Structure in the interview was seen to assist the research for the two reasons given above (Thornberry & Krohn, 2000; Gillham, 2005; Crow & Semmens, 2008). Furthermore non-structured interviewing carries with it the risk that the interaction between interviewer and interviewee will affect the data that is being collected. This may take place for a number of reasons including: the interviewees' response changing in order to please the interviewer and provide a socially desirable response; the charectaristics of the interviewer affecting the relationship with the interviewee and in turn the responses provided; and non-standardisation of questions affecting the responses (Fontana & Prokos, 2007). As each interview can have its own unique interaction between interviewer and interviewee, so the parameters of the questions will differ between each interview and the questions put to the interviewee will not be of a standardised nature. This may make any subsequent analysis of the data more difficult as the data obtained will be non-uniform in its nature.

Nevertheless, the choice of using semi-structured in opposition to fully structured interviews were threefold: First, semi structured interviews are noted as being able to give depth to data that is being collected (Crow & Semmens, 2008). The interviews were conducted in order to strengthen and build upon the first data collection method and followed on naturally from it. As discussed above the first method of data collection, examining crime

reports was likely to only fulfil the first two objectives of the research. To identify the decision-making process that explains why investigators have pursued a certain strategy and obtain an in depth understanding of their reasoning, it required that it be explored with them, which the rigidity of a fully structured interview may not have accomplished. A characteristic of semi-structured interviews is that the interviewer is free to probe any answers given further, or explore topics that have been brought up by the interviewee (Gillham, 2005; Crow & Semmens, 2008; May, 2011).

Secondly, semi structured interviews allow some flexibility as to the direction and information that is being sought (May, 2011). Answers given by interviewees can be both clarified and elaborated upon. The flexibility to alter the direction of the interview as a study progresses and theory begins to emerge is critically important to the grounded theory methodology that was used in this research (Schreiber, 2001). This flexibility is not present in fully structured interviews.

Finally, in an interview process the interviewee can dynamically challenge viewpoints that are held by the researcher in a way that a survey or data from a crime report is not able to do. The interviewees may be able to make sense of data in a way that is not obvious or apparent to the researcher (Mason, 2002). The information held within crime reports was coded and analysed, however there exists a risk that the hypotheses made, such as the reason for the correlation between the importance of the material gathered pertaining to social media and the variety and incidence of actions used is misinterpreted or connections between other pieces of data are not made by the researcher. Semi structured interviews allow a dialogue between researcher and interviewee where these connections can be explored or views held by the researcher challenged. This additional benefit that semi structured interviews hold is vitally important if theory is to be constructed. Indeed, grounded theory practitioners, advise obtaining data through different methods because of this: *"by seeking different perspectives on a topic, the researcher is challenged to develop explanations for the variation in the data and to unify them at a more abstract level into a theory"* (Schreiber, 2001, p.26).

There are two characteristcs of semi-structured interviews that assist in this. First, the pre-planned questions that are asked are largely of an open type (Gillham, 2005; Crow & Semmens, 2008). Secondly, the questions that are asked need not be phrased in the same way, nor asked in the same order (Crow & Semmens, 2008).

It is for this reason also that interviews were sought with an additional department other to those from whom the crime reports were taken from. This department was the 'authorities' bureau' which does not generate crime reports nor investigate crime. They do however act as a point of reference and act as a resource for officers when advice is sought around communications data as was identified through the crime reports. There was an anticipation that persons from this department would be able to cast a different perspective on data collected from the crime reports and officers interviewed from the CAIU, DAIU and CID.

The question could be posed as to why the research used the first data collection method if it does not realise all the objectives of the research, instead of relying solely on interviews. First, as stated above the more data sources examined, the more robustly the researcher can build theory. Secondly, interviews place a significant demand in terms of time and resources on both the researcher and the interviewee (Gillham, 2005; Crow & Semmens, 2008). Through the examination of crime reports the research had the opportunity to identify trends, themes and issues that could be further explore through interviews, at a relatively low cost in comparison to obtaining all the data by conducting interviews.

4.1 Sample size of interviewees

As mentioned above in relation to crime reports, sample size in grounded theory is determined by the data collected. (Schreiber, 2001; Day, 2002). Initially 15 interviewees were sought with a view of expanding this as necessary. 15 interviewees were anticipated to be a manageable number of interviews to conduct and analyse based on the time required to conduct the interview, transcribing and subsequent analysis. In total, however only 14

interviews were conducted, with 13 interviewees originating from TVP and one from ASC. More interviewees were sought in both police areas without success. It is well documented that access to the criminal justice domain is difficult to obtain (Jupp, 1989) and particularly to police officers (Horn, 1996; Barrett, 2005).

The gatekeepers that provided the access to both organisations were willing to do so and enthusiastic in their support. However, even though senior managers in both police areas had agreed access, the provision for this in line with the ethical guidance was that participation had to be voluntary. In the course of normal duty, detectives will often work overtime (Innes, 2003) in order to be able to complete their work. In addition to this, there is a reported national shortage of detectives (HMIC, 2015). This means that even though investigators may be willing to participate in research, the pressures of work prevent them from doing so. The invitations for participation in the study were distributed via e-mail and encompassed the whole of both the police areas. In all, 16 participants responded, with two being unable to conduct interviews due to ongoing work commitments. The number of respondents was heavily skewed towards TVP. A possible reason for this was highlighted by one of the ASC gatekeepers as to the current workload that investigators were experiencing in that police area. A second possible reason for officers from TVP being more willing to participate in interviews is due to the researcher working within the same organisation.

4.2 Method of conducting interviews

The interviews barring one were conducted whilst being recorded by a digital recorder (in agreement with the ethical guidelines). Although recording interviews in an audio format is not seen as a necessity by grounded theory theorists (Morse, 2001; Stern & Covan, 2001), there are two key benefits. The first is that information which may not be noted during the interview, either because it is missed or does not seem as important at the time is preserved for the researcher to re-examine (Schreiber, 2001). Secondly, by

not needing to make detailed notes, it affords the interviewer extra mental capacity with which to focus on the interviewee (Schreiber, 2001).

During the course of the interviews advantage was taken of its semi-structured nature in the three ways outlined above. First, strategies and tactics that were outlined by interviewees as being used in relation to social media were elaborated on and crucially the decision-making process behind them was probed. This was key as often the initial disclosure around the decision-making process by the interviewees was quite limited. Secondly, as themes emerged from the interviews they were considered in subsequent interviews that were conducted, particularly around the issue of safeguarding victims. Finally, variation in verbal cues was used to confirm the researcher's understanding of the data. By repeating what the interviewees had said in answer to a question, the response of the interviewee then confirmed or altered the researchers understanding of the meaning of the interviewees' view- point.

The remaining four sections of the interview schedule were constructed to elicit both strategies and the decision-making process behind them from interviewees. Whilst investigators could be asked about specific cases that *had not* resulted in successful prosecution, the same was not true of cases that *had* resulted in a successful prosecution. The reason for this was that if cases were discussed that had secured a conviction at court, but it became clear during the interview that evidence has not been gathered correctly, then there exists an ongoing duty of disclosure in relation to this evidence. Should this disclosure of evidence not being collected appropriately then undermine a prosecution or conviction, then the ethical impact could be significant. However, if only cases were discussed that were unsuccessful or did not result in a prosecution, then the possibility exists that the data collected would be biased. This bias would exist if there is a correlation between these two variables of non-successful prosecution and strategies used. In other words, if the prosecutions at court were not successful because of the decisions made and strategies pursued by investigators with regard to social media. A second issue that arose, which may have distorted the data is that the cases mentioned during the interviews would be historic

71

and as such not reflect current working practices and decision-making strategies employed by officers.

To address these two potential biases in the data collected, two strategies were employed. First, investigators were asked about strategies that they used that have resulted in successful prosecutions. This discussion however was generic and the interviewees were not asked for case specific examples. Secondly, a hypothetical scenario was presented to the investigators in the final section of the interview. This presented the interviewees with the ability to choose strategies and tactics that they would employ at the time that the interviews were conducted and not solely provide examples of historic choices. The hypothetical scenario put to interviewees in the final part of the interview involved an investigation featuring social media and investigators were asked for their proposed choice of strategies in dealing with this case. The purpose of presenting this scenario was to elicit a response from the interviewees which could be evaluated through process tracing methods to ascertain a decision-making process. Process tracing uses the information on the search itself rather than on the input variable and the final output (Harte & Koele, 1997). There are two major process-tracing techniques, verbal protocols and information boards (Gideon, 1996; Harte & Koele, 1997) and both were used to attempt to determine the rationale behind the strategies and tactics that the interviewees choose in the scenario.

The hypothetical scenario was based upon a number of cases that had been noted in the crime reports and was provided to the interviewee through a short verbal narrative. The scenario placed the interviewee as an investigator in a case where a child had been sexually groomed through Facebook with the suspect being in custody. The interviewees were then presented with choices of strategies and tactics that they could use in relation to social media and the scenario presented to them. These choices were shown to the interviewees on cards laid out before them. As with the scenario itself, the strategies chosen for responding to this scenario were identified as used by investigators in the data collected from the crime reports. Behind the strategies and tactics listed on each card there was

another card with further information about the implications of choosing that option. In some cases, this information was fairly detailed in others quite generic. The choices for investigators were framed in two distinct areas. The first was a list of strategies that officers could pursue, specifically of how to access the suspect's social media. The second detailed options for recording the content of the social media of the suspect or tactics that they could employ. Interviewees were asked to examine the strategies and tactics present in each of the two distinct areas and to select those that they would be inclined to use.

As detailed above there are two main techniques of using process tracing - verbal protocols and information boards (Woods, 1993; Gideon, 1996; Harte & Koele, 1997). The information board in this case consisted of the cards detailing possible strategies and tactics laid out in front of the interviewees for them to choose from. Interviewee interaction with the board formed part of the data collected and the behaviour of the interviewees in relation to it was used to ascertain the decision-making process. Where any of the choices elicited a reaction that the interviewer could see, this reaction was recorded. The reactions included picking up cards, verbal comments, obvious changes in facial expression; interviewees spending time looking at a particular option; or returning to an option that they had previously seen. To make interviewee interaction with the information board more visible to the researcher, interviewees were additionally informed that there was information under each choice offered that may inform their decision. This was done to better identify the choices that the interviewees were interested in by tempting them to find out the content of the further information listed behind each option. In order to find out this information, the interviewees would have to physically pick up the card with the strategy or tactic listed on it to reveal it, thereby making their interest known to the researcher. This technique to elicit a response has been labelled 'withheld information' (Woods, 1993).

In order to employ verbal protocols, the interviewees were also asked to think aloud and verbalise their thought process as they picked options from the two columns. Furthermore, for each of the behavioural reactions noted

above interviewees were questioned as to their thought process. This verbalisation of thoughts falls under the term 'verbal reports' in process tracing techniques (Woods, 1993). Verbal protocols have been criticized for not having the rigour of controlled experiments where a specific hypothesis is being tested (Nisbett & Wilson, 1977; Wilson, 1994). However, this research relies on grounded theory methodology (Strauss and Corbin, 1990) where no clear starting hypothesis has been identified, and as such the inclusion of verbal protocols is seen as beneficial. It has been suggested that the use of information boards in conjunction with verbal protocols provides more information than using either in separation (Westenberg & Koele, 1994; Svenson, 1996).

With regard to coding and analysing the data, in the previous small-scale research undertaken to date themes emerged naturally. It was anticipated that, as this research builds upon those studies themes would emerge, which occurred.

4.3. Using a qualitative methodology and process tracing as means of collecting data

Using qualitative methods to understand cognition is not commonplace (Kingstone, Smilek, & Eastwood, 2008). Cognitive Ethology (Kingstone, Smilek, & Eastwood, 2008) was coined as a term to describe the study of the real world with a view to identifying key features of the cognitive process used by individuals. Subsequently, once a theory is identified through real-world observations, then its features can be tested in laboratory conditions. This is in opposition to traditional research, which relies on strict conditions in what is usually termed a 'laboratory'. Findings from the laboratory are then extrapolated to the real world.

It is argued however that laboratory findings have fragility and that the results will not necessarily be reproduced outside of the specific research environment in which the research was conducted (Berry & Klein, 1993; Kingstone, Smilek, & Eastwood, 2008). The reason for this is that the stability of decision making and processes is tied to the situation in which

individuals find themselves in (Duncan & Owen, 2000). Furthermore it may be that strict laboratory conditions cannot ever mirror real world situations precisely due to the lack of variables in a laboratory setting (Woods, 1993; Kingstone, Smilek, & Eastwood, 2008). Conversely, it is argued that real world observations contain too much varience for any particular process that is noted to be directly attributed to a specific factor (Woods, 1993; Kingstone, Smilek, & Eastwood, 2008).

In using a hypothetical scenario with identical choices available to each participant and then observing their choices using verbal protocols and information boards a 'laboratory' setting was created. It is however noted that the use of semi structured interviews reduced the rigidity of this laboratory scenario. Specifically, the interviewees were questioned about their physical responses to the options available to them. Due to the differences in physical response between interviewees, in order to be appropriate different questions were put to different interviewees in different ways and not phrased identically. As such, a risk arises that the interviewees see the question differently and the parameters of the scenario are altered.

In order to mitigate weaknesses identifed above of using a controlled setting, the hypothetical scenario was combined with the interviewees previous views and decision making process behind strategies used and considered with regard to social media in their investigations. This constituted parts 2, 3,4 and 5 of the interview as set out above. These views encompass previous experiences of the interviewees with regard to social media, their subjective views on them and introspection on why strategies were chosen by them. This data can be described as subjective reports defined as '*first person measures of personal experiences and beliefs*' (Kingstone, Smilek, & Eastwood, 2008, p329). Subjective reports are however argued to be unreliable for a number of reasons. First it is thought that introspection of an experience may change the subjective views of the individual about the experience (Lutz & Thompson, 2003). Secondly significant cognitive processes occur beneath concsious awareness which concious introspection does not capture. Finally, subjective reports on behaviour and decision

making may be inconsistent with actual behaviour seen in the real world (Hurlbert & Heavey, 2001).

Both of the above methods in isolation contain shortcomings in their approaches. However, the use of different approaches to collecting data on human cognition including laboratory settings combined with observation and subjective reports have been suggested as a more robust framework than using any one method in isolation (Kingstone, Smilek, & Eastwood, 2008). For this reason both methods of subjective reporting and process tracing were employed within the context of the interview.

5. Insider research

Being an insider researcher brings with it the danger of the researcher's subjective opinion influencing the research process and analysis of data (Brannick & Coghlan, 2007; Drake & Heath, 2011). This is particulary significant when using grounded theory, as the researcher is central to the theory building process (Goulding, 2002; Mruck & Mey, 2007). It was noted in the introductory chapter that preconceptions that were held by the researcher became evident during small scale projects prior to this research being undertaken. As a result self reflection was employed throughout the data analysis and coding process to minimise this impact. Brown (1996) evaluated the benefits and weaknesses of being an insider researcher when carrying out research with the police. A list of 4 separate categories of researcher was identified:

Insider – insider: Police officers or other police staff conducting research within the police

Outsider – insider: Former employees of the police conducing research within the police

Insider – outsider: Researchers who have no background in the police but work within the police or criminal justice system conducting research.

Outsider – outsider: researchers who have no background in the police and who work outside of the police service conducting research of it.

Under this classification the researcher falls into the category of an 'insider – insider'. The possible effects of being an insider researcher when conducting interviews becomes even more pertinent than when examining and coding crime reports. Even without the issue of the researcher being an 'insider', as discussed above, non structured interviews allow for the interviewee to interact with the researcher and as a consequence alter their responses (Fontana & Prokos, 2007). Added to the interaction between researcher and interviewee influencing the data is that the researcher is an insider. The researcher themselves will likely have views on the research being conducted as a result of being an insider and these views may in turn impact on the interview. The researcher may for example unconciously give positive verbal or non verbal cues to the interviewee on views that are consistent with the researcher's own, in turn affecting what the interviewee says. Thus in this type of data collection, not only is the process of categorising data and its analysis capable of being influenced by the researcher, but the actual information that is collected may also be influenced. With regard to the benefits identified of being in this category the following two apply. First, there is an element of credibility that the researcher carries when conducting research as a police officer with other police officers and investigators (Reiner & Newburn, 2007). This credibility is also linked to a measure of trust in that the researcher is less likely to be critical of the interviewees and of the police as a whole. Investigators and officers who are being interviewed may as a consequence be more willing to be candid about their experiences and views as they believe that these views are shared by the researcher.

Secondly, police work is complex with knowledge of criminal legisltation, procedures, practices and professional knowledge likely forming a necessary part of any research that is conducted, which an insider researcher may already posses (Reiner & Newburn, 2007). This was very evident in this research. During the analysis of the crime reports, the researcher's knowledge of: legislation inlcuding RIPA 2000, PACE 1984, SOA 2003; the structure and purpose of different units within the police such as HTCUs, Authorities Bureau, CAIU, DAIU and CID and the type and scope of equipment used, such as stand alone computers and machines to download

and obtain data from electronic devices, all assisted in analysing the data. This knowledge is of course available to outsiders but at a cost of time and further research to ascertain what they involve.

Conversely, there are disadvantages to being an insider researcher. These involve being less willing to be critical in any research findings of the police and interviewees for reasons of wanting to make a favourable impact in the work place and professional allegience. Secondly, an outsider is likely to carry a fresher and more objective perspective than an insider. When conducting the interviews the researcher was acutely aware of their position as an 'insider – insider' and attempted to minimise any views carried impacting on the interviews through verbal or non verbal cues. An attempt was made to base avenues of exploration and topics of questioning not present in the interview schedule to be structured on the data collected from the crime reports and preceding interviews rather than on the views of the researcher. Regular introspection was employed in order to minimise the impact of any bias developing due to allegience to both TVP and work colleagues.

6. Conclusion

An important aspect of presenting qualitative data analysis is to show the method in which the data was collected and subsequently analysed clearly and transparently (Miles & Huberman, 1994). This chapter has articulated the rationale for using crime reports to provide data to answer the first three research questions posed and why crime reports have been selected from the three departments of CAIU, DAIU and CID across two separate police areas . It also makes clear the limitations that have previously been recognised in academic literature in the data that crime reports can provide. This in turn provides the rationale for using interviews to collect data to answer the third research question effectively and for the purposes of testing reliability.

The way in which to categorise the types of crime in which social media was noted was discussed. This involved highlighting the difficulty of applying one crime category type to any particular set of circumstances due to the possibility

that any one particular set of circumstances reported to the police may fit the points to prove for different offences. It was explained that the police crime recording system was chosen due to its uniformity of classification rules and use across all of the police forces in England and Wales. However, the weaknesses of such a categorisation were also outlined, which highlighted that these categories may hide the nature of the social media involvement. Difficulties encountered in obtaining the crime reports were described. This included not only one police force withdrawing from participating in the research but also both police areas which did provide crime reports being unable to provide the necessary resources to anonymise the data. It was explained that this issue was overcome by obtaining agreement from the University Ethics Committee for the researcher to anonymise the reports themselves.

The choice and benefits of using semi-structured interviews in the context of using a grounded theory methodology were then discussed. This included probing investigators' reasons for choosing strategies around social media, allowing issues to be clarified as they emerge in the research and finally to challenge views that might be held by the researcher. The limitations of semi-structured interviews were also acknowledged, which centre on the impact that the researcher has in altering the data that is collected from the interviewee. The method of conducting the interviews and the interview schedule was outlined. The first part of the interview schedule posed questions that cross-reference data collected from crime reports and test its reliability. The second part of the interview sought to obtain a subjective self-reflective account on the part of the interviewees as to why strategies were chosen by them in previous cases that they have dealt with. The final part of the interview puts a hypothetical scenario to the interviewees and uses process tracing methods to identify the decision-making process behind strategies chosen. Each method in isolation, the first being the self-reflective account and the second using process tracing has shortcomings in determining the cognitive process behind decisions. It is argued however that taken together they offer a more robust framework for obtaining data. Sample size was discussed as were the obstacles to obtaining access to

investigators for the purpose of research interviews. Finally, consideration was given to the impact of insider research and the need for the researcher to be conscious of their status as an insider throughout the course of the research.

The following chapter examines and analyses the data obtained from the crime reports and does so whilst comparing them against the ACPO (2012) guidelines reviewed in Chapter 2.

1. Introduction

In this chapter, data found in the crime reports is presented and then analysed. To begin with, the way in which crime reports containing social media were coded is outlined. This includes an explanation of using the categories of relevant material, evidence and critical evidence to do so. The offences found to contain social media are then presented by offence classification against the two police and three investigative areas from which the reports were collected. Through a more detailed analysis of the circumstances of the reports containing social media it is evidenced that the actual role of social media in an incident or offence was often masked by the offence classification. Next strategies and tactics that were identified in the crime reports that investigators used to deal with social media are presented forming a total of 19 separate categories. The crime reports containing social media in each police area are then grouped into those in which social media forms relevant material, evidence or critical evidence. The strategies / tactics used by investigators for each of those groups are then identified.

.

2. Establishing the impact of social media on an investigation

Crime reports taken from each force were examined separately in order to compare whether there were any differences between the two. Each department was also examined separately again with a view to ascertaining whether there were differences between investigative areas. The process for examining the reports was as follows:

1. The different crime types that featured in all the crime reports examined were recorded for each department and police area.
2. Out of those, crime types that contained mention of social media were noted.
3. Where social media did feature in an investigation, that investigation was categorised in terms of the impact that the social media had on it. This was done in the following three categories: 1) Relevant material;

2) Evidence in the investigation; 3) Evidence critical to the outcome of the investigation.

The decision as to the level of impact that social media had in an investigation and where it would sit in regard to the first two of these three groups was made by the researcher on the basis of the definitions found within the Criminal Procedure and Investigations Act 1996 (CPIA 1996). However, even with set definitions available, whether a piece of social media content forms relevant material, or evidence is a subjective one and open to challenge, as the act places the decision as to how material is defined in the hands of individuals. In relation to relevant material, it states that material is relevant if:

 "*it appears to an investigator, or the officer in charge of the investigation or the disclosure officer to have some bearing or on the surrounding circumstances unless it is incapable of having any impact on the case*" (Crown Prosecution Service, 2005, p.36).

Furthermore, the instruction for investigators is that a wide view should be taken and that material be considered irrelevant only after careful consideration (Crown Prosecution Service, 2005; Hannibal & Mountford, 2015). The retention of relevant material in an investigation is crucial to fair outcomes (Roberts & Zuckerman, 2010; Knoops, 2013) in the criminal justice system and has been put in place for two reasons. The first is in an effort to prevent miscarriages of justice that have previously been seen to occur (Choo, 2009; Knoops, 2013) and the second is to increase the efficiency of the criminal justice process (Choo, 2009; Moissidis, 2008). So, whilst social media that falls into this category would not form part of a prosecution case, there is a duty in law for it to be retained by investigators and treated in a certain way (CPIA, 1996; Choo, 2009; Roberts & Zuckerman, 2010; Knoops, 2013; Hannibal & Mountford, 2015). Furthermore, it may not always be clear at the point in which material is collected, whether it will form part of evidence at a later stage or not (Crown Prosecution Service, 2005). As such it forms an important part of the investigative process.

Evidence is defined within the 'core investigative doctrine' as material that is:

*"[…]sufficiently relevant to the facts in issue is admissible, subject to the exclusionary rules. The test for relevance is: 'evidence which makes the matter which requires proof more or less probable' (Lord Simon of Glaisdale in DPP v Kilbourne (1973) AC 729, at p 756. The 'facts in issue' are those facts which the prosecution must prove in order to establish the guilt of a defendant" (*ACPO, 2005a, p.26).

Evidence Critical to the outcome of an investigation is not a category that is defined within professional literature. It was deemed as important for inclusion in this research for two reasons. First, although social media may form evidence within an investigation, if it is not critical to its outcome, then the possibility remains that other evidence can be collected in lieu of it and investigators may choose to do so as part of their investigative strategy. Where it is critical, this option is not available. Secondly, where social media forms evidence that is critical, it may be treated differently by investigators than in cases where it supports other evidence. Investigators for example may focus more on the quality of the collected evidence, because without it a prosecution is not viable. The definition that was used in the research was as follows: Evidence as per the definition used above, without which a successful resolution of a case could not be reached. The test as to whether a resolution is successful or not is whether the CPS deem that a charge can be brought against a suspect based on the evidence, or whether an investigator or supervisor can make a decision that no crime has taken place.

3. The data collected

With regard to crime categories, the data is presented below in a similar format to that in which it was collected. To begin with each police area (starting with ASC and then TVP) and each of the three areas of investigation (Domestic Abuse, Child Investigation and Criminal Investigation) were examined separately for crime categories and frequency of social media appearance. The same areas of investigation in ASC and

TVP were then compared against one another for crime categories and frequency of social media appearance. Next each police area taken as a whole was compared against the other for crime categories and frequency of social media appearance.

Subsequently, strategies / tactics were identified that were used in relation to social media. The strategies / tactics used to deal with social media were identified in each crime report. They were coded into 19 separate categories employed by investigators. In their open codes they were then noted within the context of the impact that social media had on those investigations, so whether it provided critical evidence, evidence or relevant material. These three categories gave a frame work or a level of coding in itself. Relationships between the open codes were sought first within and then outside of those categories.

4. Avon and Somerset Crime reports

4.1 Domestic Abuse Investigations

There were 22 different offence types recorded in 100 crime reports:

Arson endangering life	Common assault	Assault ABH:
Assault GBH section	Attempt to pervert the course of justice	Blackmail
Breach of restraining order	Cruelty to / Child neglect	Criminal damage
False imprisonment	Harassment	Kidnap
Public Order Section 4	Putting people in fear of violence	Sexual assault

Sexual assault on a child under 13	Sexual activity with a child	Sexual assault by penetration
Stalking	Rape	Theft in a dwelling
Threats to kill		

Table 1 - Avon and Somerset Constabulary Domestic Abuse Investigation offence types

Of those 22 offence categories social media featured in seven, which are highlighted in red above. In total, 20 investigations involved a social media element. In five of those, the evidence that social media had to offer was critical to the case outcome. In seven it formed evidence in the investigation and in the remaining eight it formed relevant material.

Although there are seven offence categories with the crime type varying quite significantly between them, there was a predominant way in how social media featured. In 14 of the 20 crime reports, the nature of the social media involvement was in messages being sent between the suspect and the aggrieved or witnesses that caused them some harassment, however there were only four offences of harassment recorded. As such, this is an example of the 'Principal Crime Rule' masking the harassment offences which is the predominant involvement of social media in these cases.

4.2 Child Abuse Investigations

There were 14 different offence types recorded in 100 crime reports.

Cause incite a child under 13 to engage in a sexual activity	Cause a person to engage in sexual activity without their consent	Causing or inciting child prostitution or pornography
Cause a child under 13 years to watch / look at sexual activity	Cruelty neglect to children	Engage in a sexual act in the presence of a child

Meeting a female child following sexual grooming	Possession of an indecent or pseudo photo of a child	Rape of child under 13
Safeguarding a child	Sexual activity involving a child	Sexual assault on a child under 13
Sexual assault by penetration on a child under 13	Take / make indecent photograph pseudo photograph of a child	

Table 2 - - Avon and Somerset Constabulary Child Abuse Investigation offence types

Of those 14 offence categories social media featured in seven which are highlighted in red above. In total, 22 investigations involved a social media element. In nine of those the evidence that social media had to offer was critical to the case outcome. In six it formed evidence in the investigation and in the remaining seven it formed relevant material.

In five of those investigations the nature of social media involvement was in messages being sent between suspect and the aggrieved or witnesses that caused them some sort of harassment. In this set of data there are no offences recorded under the heading of or related to harassment, and so again the HOCR were seen to mask the involvement of social media in the offence. In another 12 of those investigations the social media involvement constituted either the grooming of a victim or interaction between suspect and aggrieved, which in turn was a precursor to a more serious sexual offence.

4.3 Criminal Investigations

There were 11 different offence types recorded in 100 crime reports:

Arson endangering life	Assault GBH section 18	Causing a person to engage in a sexual activity without their consent
Cause or incite a child to engage sexual activity	Kidnap	False imprisonment
Rape	Rape of child under 13	Sexual activity involving a child
Sexual assault	Sexual assault by penetration	Sexual assault by penetration on a child under 13
Threats to kill		

Table 3 - Avon and Somerset Constabulary Criminal Investigation offence types

Of those 11 offence categories, social media featured in five, which are highlighted in red above. In total 15 investigations involved a social media element. In three of those the evidence that social media had to offer was critical to the case outcome. In eight it formed evidence in the investigation and in the remaining four it formed relevant material.

In three of those investigations the nature of social media involvement was in messages being sent between suspect and the aggrieved or witnesses that caused them some sort of harassment. One of these offences falls under the heading of 'Threats to Kill'. However, the threat to kill was made through other means and not via social media, the content of which in this case was less seriously harassing. Although constituting only three investigations and so smaller in both total and proportion in comparison to the data from Domestic and Child Abuse Investigation departments, again the HOCR were seen to mask the actual involvement of social media. In another seven of

those investigations the social media involvement constituted either the grooming of a victim or interaction between suspect and aggrieved, which in turn was a precursor to a more serious sexual offence.

5. Thames Valley Police Crime Reports

5.1 Domestic Abuse Investigations

There were 23 different offence types recorded in 100 crime reports:

Abuse of trust	Adult protection	Any other indictable offence
Assault GBH	Assault with injury	Breach of restraining order
Child protection non-crime incident	Common assault	Criminal damage
Domestic incident non-crime incident	Domestic violence disclosure scheme	Drug supply
False imprisonment	Harassment	MAPPA risk assessment of the aggrieved
Perverting the course of justice	Rape	Robbery of business property
Sexual assault	Sexual assault on a child under 13	Threats to kill
Unexplained death	Violent disorder	

Table 4 - Thames Valley Police Domestic Abuse Investigation offence types

Of those 23 offence categories social media featured in eight, which are highlighted in red above. In total 17 investigations involved a social media

element. In ten of those the evidence that social media had to offer was critical to the case outcome. In two it formed evidence in the investigation and in the remaining five it formed relevant material.

In ten of those investigations the nature of social media involvement was in messages being sent between suspect and the aggrieved or witnesses that caused them some sort of harassment. However, nine of these offences were recorded under the heading of harassment and so the HOCR masked the involvement of social media in only one offence.

5.2 Child Abuse Investigations

There were 13 different offence types recorded in 100 crime reports:

Assault with injury	Assault without injury	Child abduction
Child protection non-crime incident	Cruelty to children and young persons	Domestic non-crime incident
Domestic non-crime incident	Harassment all offences	Sexual assault
Sexual assault on a child under 13	Sexual activity with a child	Rape
Rape of a child under 13		

Table 5 - Thames Valley Police Child Abuse Investigation offence types

Of those 13 offence categories social media featured in five, which are highlighted in red above. In total 13 investigations involved a social media element. In two of those the evidence that social media had to offer was critical to the case outcome. In ten it formed evidence in the investigation and in the remaining one it formed relevant material.

In four of those investigations the nature of social media involvement was in messages being sent between suspect and the aggrieved or witnesses that caused them some sort of harassment. Two of those offences were recorded under the offence heading of harassment, with the HOCR masking the involvement of social media in two offences. In another two of those investigations the social media involvement constituted either the grooming of a victim or interaction between suspect and aggrieved, which in turn was a precursor to a more serious sexual offence.

5.3 Criminal Investigations

There were 22 different offence types recorded in 100 crime reports:

Action Fraud	Adult protection non-crime incident	Arson with intent to endanger life
Assault with injury	Assault GBH section 18	Attempted murder
Burglary other than in a dwelling	Child protection non-crime incident	Domestic incident
Drug possession	Drug possession excluding cannabis	Drug supply
Obscene publications	Perverting the course of justice	Possession of firearms
Possession of other weapons	Rape	Rape of a child under 13
Robbery	Sexual activity involving a child	Sexual assault

Unexplained death		

Table 6 - Thames Valley Police Criminal Investigation offence types

Of those 22 offence categories social media featured in seven, which are highlighted in red above. In total 20 investigations involved a social media element. In five of those the evidence that social media had to offer was critical to the case outcome. In eight it formed evidence in the investigation and in the remaining seven it formed relevant material.

In one of those investigations the nature of social media involvement was in messages being sent between suspect and the aggrieved or witnesses that caused them some sort of harassment. With this offence not being one of harassment the HOCR masked the nature of the social media involvement in this one case. In another nine of those investigations the social media involvement constituted either the grooming of a victim or interaction between suspect and aggrieved, which in turn was a precursor to a more serious sexual offence.

6. Comparison of crime types featuring social media between TVP and ASC

The cross over on specific crime types between TVP and Avon and Somerset Constabulary appeared initially to be fairly limited. Within general Criminal Investigations the overlap was limited to three offence types: rape; sexual assault and assault occasioning GBH. Within Child Abuse Investigation there was an overlap of only two offences: Sexual Assault on a child under 13 and Sexual activity with a child. And finally, within Domestic Abuse investigations there was an overlap again of only two offences: harassment and rape.

In total, the offence types that were common to both TVP and ASC when comparing across all departments numbered eight:

Rape	Sexual assault	Sexual activity involving a child

Sexual assault on a child under 13	Assault with injury / Assault ABH	Assault GBH section 18
Harassment all offences	Obscene publications	

Table 7 - Common offence types to both Avon and Somerset Constabulary and Thames Valley Police featuring social media

This was a total of eight different crime categories out of a total of 15 category types that mentioned social media in TVP and out of a total of 18 crime categories mentioning social media in ASC. Three of those crimes categories: Harassment, Rape, and Sexual activity with a child featured in more than two crime reports, and between them formed the vast majority of the crime reports, 31 crimes out of a total of 49 within TVP and out a total of 57 for ASC. By taking a broader classification approach to create three categories to encompass: sexual offences, physical non-sexual assaults and harassment, these three categories encompassed 35 out of 48 offence types in the TVP crime reports and 51 out of 57 offence types in Avon and Somerset that featured social media. This observation could be useful in alerting officers to crime types where social media is more likely to feature and in the construction of standard operating procedures created to assist officers in dealing with such crimes. Such standard operating procedures are common in assisting investigators in their cases (Rowley, 2010; Yexley & Horvath, 2012; Veigas & Lum, 2013). The ACPO (2012) guidelines only refer to indecent images of children when discussing offences other than those where the cyberelement fully constitutes the crime as being offences where digital evidence might feature. These findings show however that digital evidence, specifically social media is prominently present in a number of other offences categories.

7. Crime classifications masking offences

Officer discretion and proof required prior to an offence being recorded were evident as playing a role in the child and adult protection incidents not being recorded as full offences in both ASC and TVP. This was highlighted as a cause of crimes not being recorded uniformly by police forces in chapter two (Simmons, Legg, & Hosking, 2003). An example of officer discretion affecting crime recording was a 'child protection incident' recorded in a TVP crime report. In this report, the mother of a child believed that the father was sexually abusing the child based on what the three-year-old child had said. Other than two comments made by the child, which did not clearly indicate sexual abuse there was no other evidence that constituted the basis of the belief that this offence took place. No further evidence could be collected from the child as the mother was reluctant for the child to have contact with the police. This incident was recorded as a 'child protection incident' rather than an offence that would detail a sexual assault on a child. In this case the level of proof required to evidence an offence taking place was not present and discretion was exercised by the officer in the case in not recording an offence as having taken place.

In a crime recorded by ASC investigated by the criminal investigations department under the heading of 'causing or inciting a child under 13 to engage in sexual activity' the 'one crime per victim' and 'finished incident' rules were both seen to be applied. The circumstances recorded indicate that the offender requested on more than one occasion that a child under 13 send them pictures of themselves that were indecent and asked the victim to engage in a sexual activity over webcam via social media. The offender also did sexual acts on webcam which the aggrieved saw. The offender and the aggrieved both exchanged indecent images of themselves on several occasions.

This case was reported to the police once this interaction had finished. The offender made admissions to the circumstances outlined above. Only one incident or crime report was created. Clearly a series of crimes were committed as indecent images were sent on a number of occasions and the offender made requests of the aggrieved to perform sexual acts on more

93

than one occasion. However, as these offences were reported to the police at the same time, the 'finished incident rule' applied. Furthermore, these circumstances could constitute a number of offences, including 'causing a child to watch a sex act' as set out in s.12 of the Sexual Offences Act 2003 (SOA 2003), 'causing or inciting a child under 13 to engage in a sexual activity' as set out in s.8, 2003 and possession and distribution of indecent images of children as set out in s.1 of the Protection of Children Act 1978. However as per the 'one crime per victim' rule only one offence is recorded.

These two findings are important as although the number of recorded investigations that contain social media can be seen to total 49 of the 300 examined within TVP and 57 of the 300 examined within ASC, these figures mask the greater total number offences that feature social media due to the crime recording rules. As such the proportions of crimes that feature social media (16% of those examined from TVP and 19% of those examined from ASC) may also not be an accurate representation. The combination of differing levels of proof, officer discretion and HOCR counting rules affecting the way in which incidents were recorded, required that the crime reports were examined in the detail of what occurred within each incident rather than relying on the overall recorded category of offence to assess how social media featured in and impacted upon different crime types. This more detailed analysis is presented in the following section.

8. Factors affecting investigator decision making

There was a wide and diverse range of strategies and tactics that investigators used and or considered when approaching social media in their investigations. The range of actions that were noted as being used in crime reports were coded into open categories. These categories are displayed in tables below separately for ASC and TVP crime reports and for the three ways set out above in which social media can be classified within an investigation (forming critical evidence, evidence or relevant material). Under each category is listed in how many investigations the strategy or tactic was noted as being used in. The categories are numbered from one to 19, with

consistency across the tables as to the category type that each number refers to for ease of comparison. Within these 19 categories are evident a number factors that were identified during the literature review as affecting decision making within the police including knowledge and structural organisation. A more detailed overview of these factors is given below and subsequently highlighted in the 19 categories of strategies and tactics identified as being used by officers.

Knowledge available to an investigator enables or constrains their ability to make a decision. It has previously been suggested that the police lack the knowledge and skills to effectively deal with digital evidence (Jewkes & Andrews, 2007; Jewkes & Yar, 2008; Nicol, Innes, Gee, & Feist, 2004) or a new scenario that they have previously not dealt with (Stelfox & Pease, 2013). Knowledge as a term can be subdivided in further categories: knowledge of local policy; a working knowledge of the legal framework in relation to the collection of evidence; professional knowledge which includes the management of case work and principles of investigation; and a detailed knowledge of the legal framework (Stelfox, 2009). Each of these categories, although overlapping and ultimately necessary to some degree to be able to conduct an investigation, carry a slightly different emphasis.

Local policies which will be in line with legislation, but may be skewed towards the effective use of resources and their proportionate deployment within the constraints of the police force or department. A murder investigation would for example warrant a greater resoure allocation than a theft from a vehicle due to the the greater gravity of the offence. Local procedures including the provision of gatekeepers for forensic submissions (including digital submissions) will determine what an investigator is able to do and the outcomes available for them in any particular case (Stelfox, 2009).

A working knowledge of the legal framework is critical to officers collecting evidence. Decisions in relation to the collection of evidence can be required immediately, without the ability for officers to consult with reference material (Stelfox, 2009). So for example an investigator has to be aware when he is within the limits of the law to seize a physical piece of evidence, such as a

computer, otherwise he will run the risk of the computer being excluded as evidence in any ensuing court case. With regard to digital evidence, a working knowledge of the Regulation of Investigatory Powers Act (RIPA, 2000) is crucial as it regulates how digital data can be obtained if it constitutes communciations data or involves the interception of communications.

The management of case work can be deemed as professional knowledge (Schon, 1983; Usher & Bryant, 1987; Eraut, 1994) and carries with it the need to balance the expenditure of the investigator as a resource against potentially a number of competing investigations and lines of enquiry. Principles of investigation also constitute professional knowledge when understood as standard operating procedures and have the ability as described above, to signpost the investigator and direct him as to the decisions that can be taken. Such standard operating procedures have been created with social media directly in mind (ACPO, 2012) as discussed in chapter two. However in an investigator's absence of knowledge about this specific guidance there are various investigative techiniques (Stelfox 2007) which also constitute professional knowledge and allow social media to be evidenced in a number of different ways. These forms of 'evidencing' are part of the professional knowledge of an investigator. For example, the content of a social media message can be recorded in the form of a witness statement, a photograph, a digital download or a screen capture to name a few methods.

Finally a detailed legal knowledge may constrain or signpost the investigator as to the decisions that have been previously taken and are in turn expected and what is required of them. Stated cases with regard to evidence collection require the police to take specific action when they encounter specific circumstances, thus simplifying the decision making process. One of the best known examples of such a stated case is that of *R v Turnball* (1977) 1 QB 224 which stipulates the factors that require consideration when a witness makes an identification.

Organisational structure and supervision will have a substantial impact on the individual investigators (Nicol, Innes, Gee, & Feist, 2004; Youngs &

Canter, 2006; Stelfox, 2009). Supervisors will assign cases to an invistigator, thereby affecting the amount of time that they have to pursue enquiries. They will also assign investigative actions, thereby removing some of the decision making choices from the investigator and offer professional advice and direction, which may frame the choices and subsequent decisions that an investigator will have and make. How open an organisation is to change will impact on how quickly investigators will adapt to dealing with new forms of evidence such as social media. For example, it has been noted in the past that the police is generally resistant to dealing with cybercrime for a variety of reasons (Jewkes & Yar, 2008; Awan & Blakemore, 2016). These include: a culture among police of not viewining cybercrime as actual crime; a lack of previous exposure to cybercrime for senior officers; and it being low on down on public priorities (Jewkes & Yar, 2008; Awan & Blakemore, 2016). Whilst as discussed in the methodology chapter, not all social media incidence in a case will entail a 'cybercrime', a proportion for example where social media has been used to groom a child so that sexual offences can be committed, undoubtly will (Wall, 2001; Broadhurst, 2006; Gordon & Ford, 2006; Ajala, 2007; Jewkes & Yar, 2008; Clough, 2011; Gilespie, 2015).

Finally, police forces have very different structures between themselves of where the expertise in cybercrime sits, that being dedicated High Tech Crime Units, Peadophile online investigation teams, intelligence departments, Crime Scene Investigation units or a mixture of the above (Jewkes & Yar, 2008; Hunton, 2009; Awan & Blakemore, 2016). The ease of access for investigators to these areas of cybercrime expertise will likely impact on how they will approach social media as evidenced below.

9. Strategies employed in investigations

9.1 Avon and Somerset Constabulary

All the below strategies and tactics were noted in cases where social media offered evidence that was critical to the investigation. There were 17 investigations in total:

1) Interviewing the suspect (5 investigations)	2) De briefing the suspect (4 investigations)	3) Summarising the social media involvement (17 investigations)
4) Using the RIPA* to obtain social media information (4 investigations)	5) Seizure and download of information stored on devices (6 investigations)	6) Obtaining passwords and usernames of social media accounts (5 investigations)
7) Researching how to obtain information from social media providers (3 investigations)	8) Assessing the social media involvement (1 investigation)	9) Obtaining statements (6 investigations)
10) De briefing 11) witnesses (8 investigations)	12) De briefing the victim (11 investigations)	13) Considering safeguarding (2 investigations)
14) Considering the use of undercover officers (1 investigation)	15) Obtaining supervisory advice (7 investigations)	16) Using specialist resources for research purposes (1 investigation)
17) Evidence being provided by aggrieved or suspect (4 investigations)	18) Attempt to identify / information sought about suspect / witness or victim through social media	19) CPS advice sought (0 investigations)

	other than subscriber checks (7 investigations)	
20) Accessing social media account (0 investigations)		

Table 8 - Strategies / tactics noted in Avon and Somerset Constabulary investigations where social media evidence was critical

*RIPA refers to the Regulation of Investigatory Powers Act 2000 (RIPA, 2000)

At a basic level, the ability of investigators to interview suspects (category one) demonstrates knowledge of the law in how to do so as set out in The Police and Criminal Evidence Act 1984 (PACE 1984) and local knowledge of policies and procedures of how to undertake such interviews whether that be inside or outside of custody. The use of the Regulation of Investigatory Powers Act 2000 (category four) further demonstrates knowledge of more complex legal frameworks and the application for material covered by this act as well as knowledge of local policy of how to do so. More evidence lies in the seizure of devices (category five) and completion of statements (category nine) the processes for doing so which are also covered by criminal law including different sections of PACE 1984. This demonstrates a knowledge of the relevant legal framework when dealing with social media which is identified above (Stelfox, 2009) as a component of knowledge that affects investigator decision making.

Working knowledge of digital evidence is demonstrated by investigators in categories 5 and 7. The researching of how to obtain information from social media providers shows a growth in this knowledge for those individual investigators conducting this research. Furthermore, the information was also obtained from other departments within ASC and TVP demonstrating that this knowledge was already present and available to be accessed. Although police expertise in digital evidence has been recognised (Sommer, 2004;) this contrasts with the typical suggestion noted in the literature that officers do not have the capabilities to deal with digital evidence (Nicol,

Innes, Gee, & Feist, 2004; Jewkes & Andrews, 2007; Metcalfe, 2007; Jewkes & Yar, 2008; Hunton, 2009).

Category 14 - obtaining supervisory advice demonstrates the ability for investigators to obtain guidance from their line managers about their investigations. This reflects on the organisational structure of ASC and TVP in either facilitating this, allowing it or actively making it happen - a factor identified above as influencing decision making (Nicol, Innes, Gee, & Feist, 2004; Youngs & Canter, 2006; Stelfox, 2009). Investigators' working knowledge with regard to digital evidence and effects or organisation structure on decision making are explored in more detail below.

There were 21 investigations in total where social media constituted evidence. The following strategies / tactics were noted in those investigations:

1) Interviewing the suspect (6 investigations)	2) De briefing the suspect (0 investigations)	3) Summarising the social media involvement (20 investigations)
4) Using the RIPA to obtain social media information (1 investigation)	5) Seizure and download of information stored on devices (6 investigations)	6) Obtaining passwords and usernames of social media accounts (1 investigation)
7) Researching on how to obtain information from social media providers (0 investigations)	8) Assessing the social media involvement (4 investigations)	9) Obtaining statements (7 investigations)
10) De briefing witnesses (4 investigations)	11) De briefing the victim (13 investigations)	12) Considering safeguarding

		(1 investigation)
13) Considering the use of undercover officers (0 investigations)	14) Obtaining supervisory advice (5 investigations)	15) Using specialist resources for research purposes (1 investigation)
16) Evidence being provided by aggrieved or suspect (4 investigations)	17) Attempt to identify / information sought about suspect / witness or victim through social media other than subscriber checks (4 investigations)	18) CPS advice sought (0 investigations)
19) Accessing social media account (0 investigations)		

Table 9 – Strategies / tactics noted in Avon and Somerset Constabulary investigations where social media provided evidence

In total, there were 18 investigations where social media constituted relevant material and the variety of investigative actions used fell further:

1) Interviewing the suspect (4 investigations)	2) De briefing the suspect (1 investigation)	3) Summarising the social media involvement (15 investigations)
4) Using the RIPA to	5) Seizure and download	6) Obtaining passwords

obtain social media information (1 investigation)	of information stored on devices (2 investigations)	and usernames of social media accounts (0 investigations)
7) Researching on how to obtain information from social media providers (0 investigations)	8) Assessing the social media involvement (2 investigations)	9) Obtaining statements (2 investigations)
10) De briefing witnesses (2 investigations)	11) De briefing the victim (7 investigations)	12) Considering safeguarding (0 investigations)
13) Considering the use of undercover officers (0 investigations)	14) Obtaining supervisory advice (2 investigations)	15) Using specialist resources for research purposes (1 investigation)
16) Evidence being provided by aggrieved or suspect (2 investigations)	17) Attempt to identify / information sought about suspect / witness or victim through social media other than subscriber checks (4 investigations)	18) CPS advice sought (0 investigations)
19) Accessing social media account (0 investigations)		

Table 10 – Strategies / tactics noted in Avon and Somerset Constabulary investigations where social media constituted relevant material

As the importance of the social media present in the investigation decreased from forming critical evidence to evidence and finally relevant material so too there was a fall in both the type but also the incidence of strategies and tactics used. With regard to types of strategy where social media formed evidence that was critical, 17 different strategies and tactics were used. Where it constituted evidence 14 different types of strategy and tactic were seen and where it was relevant material 13 separate strategies and tactics were noted.

With regard to the frequency with which strategies and tactics were used, where social media constituted critical evidence in total strategies and tactics relating to social media appeared 92 times (a mean of 5.4 in each investigation). Where social media constituted evidence, strategies and tactics appeared on 77 occasions (a mean of 3.7 used in each investigation) and where it was relevant on 45 occasions (a mean of 2.5 used in each investigation).

 As such there is a correlation with what investigators were either doing or recording what they were doing and the importance of the social media material. This correlation becomes even more pronounced when it is noted that there were only 17 investigations where social media formed evidence that was critical to the investigation as compared to 21 where it formed evidence and 18 where it formed relevant material. The more important the social media was to the case, the greater the frequency and variety of actions performed. There is no rationale recorded for this correlation within the crime reports themselves. However, one explanation is that this is due to investigators' application of case management, a factor noted as affecting investigator decision making above (Schon, 1983; Usher & Bryant, 1987; Eraut, 1994). There is a finite amount of time that investigators have to dedicate to their investigations and a finite amount of resources that each police area has to expend. As such, lines of enquiry that are judged to be less important may not be pursued. The correlation on its own could also be explained in another way, in that the more enquiries that were conducted in relation to social media the more important evidence it uncovered. However, in almost all the investigations there was an initial summary of the social

media involvement. The content of these summaries and the importance that they attached to social media changed little as further strategies and tactics were pursued and material collected in relation to the social media. This suggests that the initial appraisal of how relevant the social media was, was made correctly and it was on this basis that different strategies / tactics and their frequency were pursued.

9.2 Thames Valley Police

This pattern repeated itself through with the strategies and tactics that were employed in the TVP crime reports. In relation to cases where social media formed critical evidence in the investigation there were 16 cases in total. The range of actions were coded into the following open categories:

1) Interviewing the suspect (9 investigations)	2) De briefing the suspect (2 investigations)	3) Summarising the social media involvement (12 investigations)
4) Using the RIPA to obtain social media information (3 investigations)	5) Seizure and download of information stored on devices (10 investigations)	6) Obtaining passwords and usernames of social media accounts (1 investigation)
7) Researching on how to obtain information from social media providers (3 investigations)	8) Assessing the social media involvement (4 investigations)	9) Obtaining statements (5 investigations)
10) De briefing witnesses (3 investigations)	11) De briefing the victim (9 investigations)	12) Considering safeguarding (2 investigations)

13) Considering the use of undercover officers (0 investigations)	14) Obtaining supervisory advice (3 investigations)	15) Using specialist resources for research purposes (0 investigations)
16) Evidence being provided by aggrieved or suspect (2 investigations)	17) Attempt to identify / information sought about suspect / witness or victim through social media other than subscriber checks (1 investigation)	18) CPS advice sought (0 investigations)
19) Accessing social media account (1 investigation)		

Table 11 – Strategies / tactics noted in Thames Valley Police investigations where social media evidence was critical

In relation to cases where social media formed evidence in the investigation there were 17 investigations in total. The range of actions were coded into the following open categories:

1) Interviewing the suspect (6 investigations)	2) De briefing the suspect (0 investigations)	3) Summarising the social media involvement (13 investigations)
4) Using the RIPA to obtain social media information	5) Seizure and download of information stored on devices	6) Obtaining passwords and usernames of social media accounts

(1 investigation)	(10 investigations)	(5 investigations)
7) Researching on how to obtain information from social media providers (1 investigation)	8) Assessing the social media involvement (4 investigations)	9) Obtaining statements (5 investigations)
10) De briefing witnesses (3 investigations)	11) De briefing the victim (7 investigations)	12) Considering safeguarding (0 investigations)
13) Considering the use of undercover officers (0 investigations)	14) Obtaining supervisory advice (6 investigations)	15) Using specialist resources for research purposes (0 investigations)
16) Evidence being provided by aggrieved or suspect (5 investigations)	17) Attempt to identify suspect / witness or victim through social media other than subscriber checks (4 investigations)	18) CPS advice sought (2 investigations)
19) Accessing suspect or victim social media account (3 investigations)		

Table 12 - Strategies / tactics noted in Thames Valley Police investigations where social media provided evidence

In relation to cases where social media formed relevant material in the investigation there were a total of 14:

1) Interviewing the suspect (1 investigation)	2) De briefing the suspect (0 investigations)	3) Summarising the social media involvement (10 investigations)
4) Using the RIPA* to obtain social media information (0 investigations)	5) Seizure and download of information stored on devices (2 investigations)	6) Obtaining passwords and usernames of social media accounts (1 investigation)
7) Researching on how to obtain information from social media providers (1 investigation)	8) Assessing the social media involvement (3 investigations)	9) Obtaining statements (3 investigations)
10) De briefing witnesses (2 investigations)	11) De briefing the victim (6 investigations)	12) Considering safeguarding (0 investigations)
13) Considering the use of undercover officers (0 investigations)	14) Obtaining supervisory advice (3 investigations)	15) Using specialist resources for research purposes (0 investigations)
16) Evidence being provided by aggrieved or suspect (0 investigations)	17) Attempt to identify suspect / witness or victim through social media other than subscriber checks	18) CPS advice obtained (0 investigations)

	(0 investigations)	
19) Accessing social media account (0 investigations)		

Table 13 – Strategies / tactics noted in Thames Valley Police investigations where social media constituted relevant material

Aside from the categories 13 and 15, the strategies and tactics used by investigators in TVP repeated those that were seen in ASC, which demonstrated a consistency of options being adopted across the two police areas. This supports the idea that there are accepted customs and practices that have developed to collect digital evidence that can effectively be presented to a jury in a court setting (Bryant, 2016). Furthermore, the total frequency in which categories 13 and 15 were used by investigators in ASC was only on 3 occasions. As with ASC as the importance of the social media present in the investigation decreased, so too there was a fall in the type of strategies / tactics used.

With regard to types of strategy and tactics where social media formed evidence that was critical, 16 different options were used. Where it constituted evidence, 15 different types options were seen and where it was relevant material 10 separate options were noted. With regard to the frequency with which strategies and tactics were used, where social media constituted critical evidence in total strategies and tactics relating to social media appeared 70 times (a mean of 4.4 used in each investigation). Where social media constituted evidence, strategies and tactics appeared on 75 occasions (a mean of 4.4 used in each investigation) and where it was relevant on 32 occasions (a mean of 2.3 used in each investigation). The correlation with what investigators were either doing or recording what they were doing and the importance of the social media material was not as strong as it was with the reports from ASC, but still present. Again, in the majority of the investigations there was an initial summary around the social media involvement, and the importance attributed to social media changed little as the investigation progressed and further strategies / tactics were pursued.

Of the four strategies / tactics outlined by the ACPO (2012) guidelines to deal with social media two of them are noted as being used in the crime reports and subsumed in the categories above. The first of these is to contact the authorities' bureau if the data that is being sought is deemed to be in transit. These actions fell under the codes of 'seeking specialist resources for advice' and 'using RIPA (2000) to obtain information' on social media accounts. The second was the catchall strategy of securing a copy of what can be seen. This can be seen in the coded categories of 'Obtaining passwords and usernames of social media accounts'' and then 'accessing social media account'. Whilst there is no mention of printing out the social media logs (the second suggestion put forward in the guidelines) within the strategies / tactics seen in the crime reports, there is mention of victims and witnesses making screen shots of logs and sending them electronically to investigators. This would be the necessary precursor to these screen shots then being printed out by investigators. There is no reference in the crime reports to investigators making use of a specific facility to save chat logs (the first suggestion put forward in the guidelines). However, officers were seen to be submitting electronic devices for the extraction of information to HTCUs or using specialist equipment to do so in line with first part of the guidelines referring to seizure of electronic devices, and in so doing obtaining information pertaining to social media through this process.

10 Social media and investigators access to knowledge and information

As noted above, the action of researching how to obtain information from the provider of the social media appearing in the case was identified in eight investigations (out of a total of 106 that featured social media) across both ASC and TVP crime reports. Six out of the eight investigations where this occurred was where the evidence offered by social media was critical to the case outcome. With the exception of one case, the advice obtained appeared to be consistent.

There are however four further pieces of evidence that show investigators seeking specialist knowledge that was outside of their own knowledge base,

but present within the two police organisations and in so doing progressing their investigations. First, the crime reports evidenced officers submitting devices for examination and download, either to an operator who through a connection to a device can download the contents of a phone or to their HTCUs. This was seen in 36 investigations spread across both ASC and TVP and is in line with guidance provided in the ACPO (2012) guidelines around seizure of electronic devices. Secondly, in obtaining supervisory advice either from their line managers. It was seen that often as a result of this consultation further investigative actions were set by the supervisors. Thirdly, on three occasions, specialist resources within ASC were asked to conduct research on the investigators' behalf to progress the investigation. Finally, CPS advice was obtained on three occasions.

Aside from one case where the investigator was given lines of enquiry to pursue by their supervisor there was no evidence to suggest that lack of knowledge in how to deal with social media was negatively affecting investigators ability to progress their investigations, which has been suggested in some of the literature as to what happens when officers deal with digital evidence (Nicol, Innes, Gee, & Feist, 2004; Jewkes & Andrews, 2007; Jewkes & Yar, 2008; Williams, 2008; Hunton, 2009; Awan & Blakemore, 2016). In almost all of the situations, the opposite appeared to be the case. When investigators were faced with a lack of knowledge they approached others to obtain that knowledge or to facilitate their case moving forwards. Not only does this demonstrate an ability to obtain knowledge with regard to digital evidence, but it also demonstrates legal knowledge in relation to RIPA 2000 and submission for checks on social media accounts and PACE 1984 with regard to seizure of electronic items for subsequent examination.

11. Social media and organisational structure and resources

The ability for investigators to seek advice from a variety of persons and departments reflects on local policy, resources and organisational structure (Groeneveld, 2005). The crime reports do not contain the organisational

structure and policy with regard to the management structure, the way in which supervisory reviews are conducted, their frequency, the policy in relation to contacting High Tech Crime Units, submitting digital items for analysis or how investigators can make applications under RIPA 2000 for information relating to indivdual social media accounts.

As discussed in chapter two, there is no possibility to explore further this information without using other types of data. However the crime reports did evidence that these actions were taking place. Given that the crime reports show that supervisory reviews have taken place, the organsiation structure and policy either allows reviews to be conducted by supervisors and this is utilised by them, or it is an expected aspect to their role that is actively followed. Either way, the interaction between supervisor and investigator takes place and this interaction is recorded in the crime reports.

The crime reports showed that there were three departments who had expertise of digital evidence and specifically social media. These departments were the HTCU, Intelligence Units and units dealing with applications for communications data. These have been identified previously as having expertise in the area of cybercrime within the police (Jewkes & Yar, 2008; Hunton, 2009; Awan & Blakemore, 2016). These three departments were contacted by investigators on a regular basis in both TVP and ASC. Given that the crime reports did not contain any reference about other departments that investigators turned to for information, it would suggest that these three departments are known for their expertise in social media and hence they were being asked for advice. Not only were these departments approached for guidance, but technical expertise was provided, either in the form of downloading devices or in the information provided by them about the social media applications. There was no evidence in any of the crime reports that there was uncertainty about where to submit devices for examination, there was simply a record of investigators doing so.

It has been argued that there has been a resistance by the police in considering cybercrime offences as actual crime (Jewkes & Yar, 2008; Awan & Blakemore, 2016). There was however no evidence in terms of the language used of resistance to investigating any of the crimes that involved

social media. It is of course possible that the resistance to investigation may have manifested itself in crime reports not being created, which in turn would not be evident in the crime reports examined.

12. Problem Solving, Heuristics, prescriptive and descriptive models of decision making

Heuristics, prescriptive and descriptive models of decision making have been identified in the literature review as models of decision making that may impact or describe the decision-making process behind the investigative strategies and tactics chosen by investigators. However, due to the static nature of the information collected in the crime reports it is not possible to expand or explore further the reasons why the strategies identified above were selected. There are strategies and tactics present in the tables that show established ways of collecting evidence and how this process is influenced. These include obtaining statements (Gozna & Horvath, 2009), seeking or obtaining supervisory advice (Groeneveld, 2005) and interviewing suspects (Sanders & Young, 2012). There is a lack of evidence in the crime reports to ascertain whether investigators weighed up different ways of obtaining evidence and as a result of this process made a decision to use them or whether investigators used these techniques automatically as a consequence of previously employing them. Other strategies and tactics are present that may have been adapted for social media. This would include seeking specialist advice, seizing electronic devices and making communications data applications using RIPA 2000.

There is some limited support to show that investigators were mirroring the steps identified as being followed by individuals when they encounter a new issue in problem solving models (Getzels, 1982; Simonton, 1999; Pretz, Naples, & Sternberg, 2003). First, officers were seeking advice on how to deal with social media. This offers support to the proposition that they were encountering and recognising social media as a new problem and in so doing seeking advice on how to deal with it. Secondly, strategies and tactics are present that show investigative enquiries that are unique to social media.

112

This includes the seeking information around suspects, witnesses and victims through social media and accessing social media directly. This again offers support to the idea that officers were seeing social media in a unique light and in so doing approaching it distinctively to other forms of evidence that they deal with.

It may have been expected as detailed towards the beginning of chapter 3 that the NDM would feature within the crime reports as a framework for decision making. However, whilst envisaged by ACPO (2012) and the National College of Policing as being prescriptive in nature, the NDM is very similar to and overlays onto models of professional learning cycles (Dewey, 1933; Argyris & Schön, 1978; Kolb, 1984; Gibbs, 1988; Johns, 1995; Brookfield, 1998; Thompson, 2000; White, Fook, & Garnder, 2006). These models are descriptive in nature rather than prescriptive, having been constructed following observations of how professionals in different fields make decisions. Whilst there was evidence of professional learning cycles utilised within the research, there was no direct evidence of the NDM and it's individual steps being employed by investigators. The NDM assumes however in it's first step that there is a concious extrapolation of a problem by the decision maker. In contrast this research has found that social media was being approached as a problem in a 'fuzzy scenario' where the issue and it's facets are not particulalry well defined (Pretz, Naples, & Sternberg, 2003). In such a scenario the problem requires first of all recognition by the individual that a 'problem' exists and then the subsequent defining of the problem's facets (Bransford & Stein, 1984; Sternberg, 1985; Pretz, Naples, & Sternberg, 2003). These steps are not present within the NDM. This is in contrast to a situation where the issue is distinct and decisions can be applied within clear parameters (Pretz, Naples, & Sternberg, 2003). Furthermore, the research found that a significant portion of the decisions made in relation to social media were driven by heuristcs which can allow an unconcious process. This may offer an explanaiton as to the NDM's lack of mention, although there are other possible explanations for it not being utilised including that it may not be well suited to making decisions within

complex investigations and as such is not utilised by detectives. To ascertain this is an area for further research.

In order to ascertain the reasons why strategies detailed above have been used, the decision-making process behind them, and to evidence that officers were indeed seeing social media as a distinct and new problem, interviews were conducted with investigators. This forms the second part of this research and is addressed in the following chapter.

13. Conclusion

When an overall view of the data was presented showing the types of crime that have had social media involvement and the way in which social media affected these investigations, the arguments supporting the weaknesses of using the original police classifications to identify which investigations social media was affecting were highlighted. The conclusion was drawn that the next step in the data analysis would be to examine the social media involvement in the incidents in more detail. It was shown that the majority of investigations featuring social media occurred in the following three offence types: sexual; physical non-sexual assaults; and harassment cases. This allows for signposting investigators to the potential of social media material being present in certain investgations, expanding the scope of those mentioned within the ACPO (2012) guidelines and the construction of standard operating procedures to assist officers in dealing with social media in such crimes. Such procedures are widespread in signposting investigators in areas other than social media in their cases (Rowley, 2010; Yexley & Horvath, 2012; Veigas & Lum, 2013).

Strategies and tactics were then presented that were visible in the data and 19 separate categories were found that aside from two repeated themselves across both police areas. These strategies / tactics reflected established factors that affect investigative decision making identified in academic literature. These include different forms of knowledge, organisational structure and resources. The strategies evidenced around social media however challenge the notion that police lack the knowledge and skills to

deal with digital evidence or the impetus to deal with offences where it is present (Jewkes & Yar, 2008; Awan & Blakemore, 2016). It was shown in the crime reports that three out of the four suggested tactics in the ACPO (2012) guidelines were being utilised.

The limitations of crime reports have prevented an analysis as to why decisions are taken, whether officers behave in a way described by problem solving models when tackling social and a deeper exploration of the organisational structure and resources present (Jewkes & Yar, 2008; Hunton, 2009; Awan & Blakemore, 2016). The next chapter examines the data collected through interviews with investigators, which had the potential to overcome the constraints that crime reports present.

1.   Introduction

This chapter begins by identifying the strategies / tactics that were noted as being used by investigators during their interviews. A comparison is then made with these against those that were identified in the examination of crime reports. Next, the first part of the analysis of the interviews is presented. In this analysis four aims are identified that investigators have when dealing with social media. The way in which the ordering of these goals was achieved from the data is described and data from the interviews presented to that effect. The decision-making models seen in the literature review are shown not to adequately explain how officers approach social media when they encounter it in their investigations. Problem solving as a concept is revealed to more accurately describe the situation faced by investigators when encountering social media. The four aims identified are portrayed as an evolved understanding of what drives the decisions of investigators.

How investigators frame social media as a problem is then presented with 10 separate facets distinguished by officers. This describes the first three stages of the problem-solving model as presented by Pretz, Naples, & Sternberg (2003) namely, identifying social media as a problem, defining it and ordering goals that the individual faced with the problem wants to achieve.

The chapter then goes on to describe the fourth stage of the model, that being developing strategies to achieve the identified goals. It breaks this stage however further into those steps presented by the decision making model of Frauenknecht & Black (2010). It describes the choices made by investigators using the stages in this decision-making model with reference to the four identified goals of investigators of: collecting evidence in a way that it would be accepted by a court; identifying suspects; maintaining the engagement of the victim; and safeguarding individuals. The greatest

116

amount of information available around decision making rules obtained from the interviews was around the aim of obtaining evidence for court and as such the main body of the analysis focuses on this goal. There was much less information pertaining to the remaining three goals and the options that investigators identified in relation to achieving them. Finally the ACPO (2012) guidelines are compared against the actual behaviour of investigators.

2. Strategies used when social media is encountered

Data collection through the process of semi-structured interviews with investigators sought to answer the second and third questions posed in this research. The second question looked to identify investigative strategies deployed by investigators when they encounter social media. Data obtained from crime reports identified a number of strategies and tactics used and coded them into 19 separate categories. These were used during the hypothetical scenario presented to investigators at the end of the interview. However, prior to the hypothetical scenario strategies and tactics used in previous cases encountered by the investigators were discussed. In total 14 investigators were interviewed and two cases discussed with each investigator during their interview. Although this meant that only a total of 28 cases that involved social media were explored in comparison to the 106 cases identified in the crime reports, the same categories of strategies and tactics employed or considered were noted in the interviews as in the crime reports barring one, which was consideration of using undercover officers. Furthermore, the use of undercover officers was only considered in only one of the 106 crime reports containing social media. Although no statistical analysis has been conducted, the mention of this strategy in only one report out of 106 may be considered to be out of the boundaries of normal considerations made by investigators. No further strategies or tactics were noted during the interviews additional to the ones seen deployed in the crime reports. Although it is difficult to make a direct comparison of the frequency options used between both sets of data, that the same options were identified defends the reliability of the results found in each (Thornberry & Krohn, 2000). The following table shows the same categories as identified in

the analysis of the crime reports. Below each category is listed the number of interviewees that mentioned or considered this strategy or tactic during their interviews when discussing previous cases that they have dealt with:

1) Interviewing the suspect (mentioned as being employed or considered by 14 interviewees)	2) De briefing the suspect (mentioned as being employed or considered by 1 interviewee)	3) Summarising the social media involvement (mentioned as being employed or considered by 14 interviewees)
4) Using the RIPA to obtain social media information (mentioned as being employed or considered by 5 interviewees)	5) Seizure and download of information stored on devices (mentioned as being employed or considered by 10 interviewees)	6) Obtaining passwords and usernames of social media accounts (mentioned as being employed or considered by 6 interviewees)
7) Researching on how to obtain information from social media providers (mentioned as being employed or considered by 3 interviewee)	8) Assessing the social media involvement (mentioned as being employed or considered by 14 interviewees)	9) Obtaining statements (mentioned as being employed or considered by 12 interviewees)
10) De briefing witnesses (mentioned as being employed or considered by 7 interviewees)	11) De briefing the victim (mentioned as being employed or considered by 6 interviewees)	12) Considering safeguarding (mentioned as being employed or

		considered by 12 interviewees)
13) Considering the use of undercover officers	14) Obtaining supervisory advice (mentioned as being employed or considered by 3 interviewees)	15) Using specialist resources for research purposes (mentioned as being employed or considered by 10 interviewees)
16) Evidence being provided by aggrieved or suspect (mentioned as being employed or considered by 8 interviewees)	17) Attempt to identify / information sought about suspect / witness or victim through social media other than subscriber checks (mentioned as being employed or considered by 8 interviewees)	18) CPS advice sought (mentioned as being employed or considered by 7 interviewees)
19) Accessing social media account (mentioned as being employed by or considered 11 interviewees)		

Table 14 – Strategies / tactics noted as being used by investigators in the data obtained from interviews

3. The identification of four goals

During the course of the interviews, it became clear, that the parameters of the decisions that investigators were encountering were not clearly defined. The strict boundaries of experiments from which heuristics have been identified and prescriptive / normative and descriptive / positive models have been derived from, were not present. Whilst elements of models identified in decision making literature were present in the data, they failed to adequately describe the initial situation that faced investigators when they encountered social media. There was no single set of parameters that investigators were describing during the interviews against which to overlay a model of decision making as defined in the literature review. What was clear however was that investigators were identifying social media as a problem. The following statements were made by different investigators in the initial stage of the interviews when investigators were asked to define social media:

Participant 8: "Massive pitfalls and I think we are lacking hugely on social media. Well behind"

Participant 9: "I think there needs to be a lot of work around assisting police around social media".

Participant 11: "Hard work. I think it causes problems rather than solves problems".

Participant 13: "It's the bane of my life at the minute with some of the jobs that I have".

As the interviews progressed it became clear that all the investigators had been at a point during their professional careers where social media had featured in an investigation and presented an unknown element to them. As the above statements show, social media was being identified as an issue, but it was not immediately obvious what that issue was or the parameters of the problem that it presented. Rather than revealing strict parameters in

which a decision was being made, the coding process revealed four separate goals that investigators strove towards. These were as follows:

1.   Safeguarding individuals

2.   Maintaining the engagement of the victim.

3.   Identifying the suspect for the purposes of the investigation.

4.   Collecting evidence in such a way that it would be accepted in court.

The aims were clearly identified by investigators through statements that they made during the interviews. However, not all 14 interviewees mentioned each of the four aims. The safeguarding of individuals was mentioned by 12, reference to maintaining the engagement of the victim was mentioned by 11, identification of the suspect by 7 and collecting evidence that would be accepted in court by 7. The order in which these goals are listed is reflective of the importance assigned to them by investigators. The importance that investigators assigned to a goal was ascertained through comments made by them when considering one goal against another and where a clear choice had to be made of satisfying one over another. In other words, in a situation where only one goal out of two being considered could be achieved. Although not all investigators ranked each of the four aims, when they did make comments that placed aims relative to each other they were always ranked in the above order. The evidence for this was that in each of the interviews where previous cases were discussed, definitive statements were made in relation to tiering that were not over ruled elsewhere in the interviews.

3.1 Collection of evidence for court

The greatest number of comments, a total of 57, were made with regard to presenting the social media encountered in investigations as evidence for the purpose of it being presented in court. The following comments are typical of the ones made by participants regarding social media and relating it to court:

Participant 9: "*Well court, giving it to CPS, they need it to be evidenced in the right way*"

Participant 10: "*Make sure whatever product they get can stand up evidentially in court*"

Participant 12: "*Eventually everything will be questioned in court*"

The main concern in presenting social media as evidence in court was that it would not be excluded as evidence because of a challenge by the defence or scrutiny by the court. The following comments provide some insight into this:

Participant 6: "*you rely on it in a decent case in court and falls down because you haven't id'ed somebody correctly or collected the evidence correctly.*"

Participant 3: "*doing things the right way by going through authorities, and getting things produced in a manner we know if it's questioned in court we obtained this through the right channels.*"

Participant 5: "*That would have to come from the defence and or the suspect should there be one….. All we need is that element of doubt don't we. That's all we need from the defence.*"

As these goals became apparent during the coding procedure, literature was sought that had examined detective work to establish whether these goals had previously been explicitly acknowledged as was seen in the literature review.

3.2 Identification of the suspect for the purpose of the investigation

Identification of the suspect as an aim was commented on a total of 13 times. This was the lowest number of comments with respect of the four overarching goals identified. The following comments are examples of the

ones made by participants with regard to social media and relating it to identifying a suspect for the purpose of the investigation:

Participant 10: "*So we've had to identify who that person was, initially. It was an absolute priority, then have a look at the content of his Facebook contacts*"

Participant 1: "*Essentially it was our only way of progressing this investigation. We had the complaint with the victim but in order to do anything about that whatsoever we had to try and identify who it was that was asking her for these images*"

Participant 5: "*we want to identify them*"

There is an implicit ordering that places the identification of a suspect in an investigation over recording social media as evidence for court. This is because if there is no suspect who has been identified then there can be no case which can be heard in court (Connor, 2009). Furthermore, the following comments show that when looking to identify a suspect through social media that was present in a case, investigators were not concerned with presenting it as evidence unless there was a prospect of the case going to court, which shows that these two aims are separate and distinct:

Participant 6: "*Yeah. I probably use it more as an intel tool rather than, yeah an evidential ID through Facebook.*"

Participant 9: "*Once I'd found him you know he's then consensual. So it becomes irrelevant really to me I found the right person, he's admitting his presence, he's saying its consensual so the investigation takes another, now I'm trying to prove consent or whatever, that becomes irrelevant. Obviously if he has said no I've never been there then I would have to look at my evidence chain really.*"

Participant 6 was talking about a robbery investigation where the identification of a suspect took place through social media that presented itself during the case. The investigator's use of the social media to identify the suspect rather than use it as evidence is very clear as it is described as an 'intel tool' rather than 'an evidential ID'. Participant 9 was discussing their investigation into a rape. The aggrieved in this case could not name the suspect, but the suspect was identified through the social media present in the case. The investigator explains that once the suspect had been identified and arrested, during the subsequent interview he placed himself at the incident when it occurred. As such, there was no need to evidence how he was identified as a suspect because he did so himself. The issue in the case was now consent. Had he not identified himself as being present, then it may have been necessary to evidence how social media had identified him as the suspect. In these two comments, the two investigators demonstrate that identifying the suspect through social media was a separate and distinct goal to evidencing the social media and furthermore it was an objective that was sought prior to considering whether to present social media as evidence.

3.3 Maintaining victim engagement

In total 26 comments were made on the subject of maintaining victim engagement with the following being typical of the strength of feeling expressed on the importance of the victim:

Participant 2: "*Yeah and it was all very victim focused if you like*"

Participant 1: "*I mean we are here to try and provide a service to the victim*"

Participant 12: "*because long term if there is stuff going to court I want a much better relationship with victim*"

The ordering of the victim as a goal above that of identifying the suspect and gathering evidence for court was also very clear.

Participant 3: "*the most important thing here isn't about me getting a quick conviction or a quick detection. It's about the victim and sometimes we lose sight of that*"

Participant 12: "*I probably wouldn't. Just because I'm thinking long term if I want to keep her on board for a prosecution if I could build a good rapport with her, a good relationship with her. It would only be this my personal gain to see it then and there.*"

Participant 13: *"Because I had to make a decision, do I arrest a vulnerable CSE girl for some petty shit, well it's not petty it's quite, and risk damaging a relationship with the police, or do I get her in voluntarily. So I got her in voluntarily."*

Participant 3 in the statement above clearly places the victim above the quick conviction of the suspect and the actions that would lead to and enable a quick conviction to happen. Participant 12 was discussing whether to seize a victim's phone against their will from them in order to be able see and record social media messages visible on the phone as evidence. Again, the investigator makes a decision not to seize the phone in preference to preserving or maintaining a better relationship with the victim. Participant 13 describes a situation where the suspect in the case they are investigating is a victim in another case. In order to maintain the relationship with the victim, they alter the way in which they approach her as a suspect and make a decision not to arrest her but rather deal with her voluntarily. This last example places maintaining a relationship with the victim above that of dealing with them as a suspect and collecting evidence which an arrest would facilitate in this case by giving the investigator powers to seize their phone.

Out of the 26 comments made regarding maintaining a relationship with victims, 14 described the process of obtaining evidence relating to social media consensually from the victim, specifically by having access to their phones or electronic devices that had social media content stored on them.

Although consideration was given to seizing these devices against the wishes of the victim, none of the investigators described making this choice, preferring instead to try and obtain the evidence another way or to persuade the victim to allow access to their device. This was done to maintain a relationship with the aggrieved. The seizure of such devices is done to obtain intelligence, evidence for the case or to identify the suspect. Three investigators explicitly describe making a choice not to seize devices from their victim if they will not provide access to their social media even if it impedes identifying the suspect in the case.

3.4   Safeguarding

In total, 39 statements were made regarding safeguarding. In some cases, the word 'safeguarding' was specifically mentioned whilst in other cases the risk to victim(s) and the safety of the victim was considered. Comments containing reference to risk and safety of victims were included as these elements are present in literature and government agency direction concerning safeguarding reviewed in Chapter 2. This highlighted that safeguarding of children, vulnerable adults, victims of rape and domestic violence had over the last 20 years become a statutory requirement for the police to fulfil (Adoption and Children Act 2002; Children Act 2004; Laming, 2009). The following comments are typical of the ones made by participants regarding social media and relating it to safeguarding:

Participant 3: "*If the child is in a safe place. If the child has been assaulted and the child has phoned mum and mum doesn't know where he is then yeah. That would be quite a priority to get just for safeguarding issues and welfare.*"

Participant 5: "*First and foremost if you're dealing with victims, how can we protect them from this happening again. What can they put in on their own self-awareness, self-protection around stopping this happening.*"

Participant 7: "*In terms of managing the risk to other people, because its social media, if you've got an idea, if you know who your suspect is, you can probably determine if you've got other potential victims that are at risk.*"

Participant 9: "*these girls need safeguarding it could be their images. We had a real concern about this lad and all the relationships he was having.*"

With regard to ordering the Safeguarding above the other three objectives identified in total there were nine comments made. Two comments ordered safeguarding above maintaining victim engagement. The remaining seven comments ordered safeguarding above organisational guidelines with regard to the action undertaken having a negative or questionable impact on the case at court.

Participant 4 considered the risk that the suspect posed to the aggrieved and stated that this would influence their decision making. If the risk was significant enough they would break with protocols and access the suspects Facebook directly over normal work computers.

Participant 5: "*If police officers encourage victims to stay on those Facebook twitter accounts it will obtain further information then that goes against the ethical approach to why are we putting victims not saying they have to we are encouraging them to stay there to see if it will generate more evidence. And that is an issue for me.*"

Participant 7: "*Yeah, I think it's always a little bit, a grey area in terms of whether you have got the power to seize it as evidence of the case, bearing in mind that it's your victim and I suppose it's the case really I suppose if we're talking life and death, I would quite happily stand up in court and say that I've seized it.*"

Participant 9: "*Yeah. And because we need to justify it. And justification is protecting children or vulnerable people then that ups the ante.*"

Participant 11: "*Like those guidelines are there to make sure that we don't do something wrongly. But if I was doing it for the right reasons and it was to protect somebody, especially with that Facebook thing, checking to make*

sure with the intel that we had and everything else. You know I was doing it
for the right treasons. As long as I can justify it."

Participant 4 discusses the hypothetical scenario presented in the final part of the interview. They explain that if the suspect posed a significant enough risk to the victim or other victims then they would break protocols and access the suspect's facebook directly on work computers even though this would break organisation guidelines and may subsequently impact on the admissibility of evidence. Participant 5 was using a hypothetical example to emphasize the importance of the victim to them when dealing with social media. In the scenario that they outline, the victim is being harassed by a suspect via social media. Instead of officers advising the victim to block the suspect, they advise the victim to not block the suspect so that any further messages sent by the suspect can be collected as evidence for the case. The investigator explains that a scenario such as this would be an issue for them ethically as they would rather protect the victim than obtain evidence.

 Participant 7 discusses the risk posed by the suspect in a hypothetical scenario. Their comment is in relation to seizing the victim's electronic devices in order to identify the risk posed and that if it was a 'life and death' scenario then they would be happy to do so. Given that the victim in this scenario does not wish to surrender her electronic devices, the intended consequence would likely be to damage the relationship with the victim. The investigator may also forsee a potential issue in court in taking this course of action as they reference standing up in court and explaining their action. As such they can be seen to order safeguarding above maintaining a relationship with the victim and potentially the collection of evidence for the purposes of court. This example shows safeguarding as a goal to be distinct from the goal of maintaining and engaging the victim in that what is seen as being in the best interests of the victim may alienate the victim from the police and other public agencies. Other examples where these two aims conflict could include the arrest of an offender in a domestic violence situation to whom the victim is emotionally attached and protective of or the

decision to remove a child from their parents from whom they do not wish to be separated from.

Participant 9 refers to a case where she was challenged by a solicitor acting on behalf of the suspect as to their attempts to obtain access to the suspect's computer and that this course of action was outside the scope of the investigation. The investigator justifies her enquiries not in terms of collecting evidence for the case or that they have a legal basis to pursue those enquiries but rather on the basis of safeguarding. The safeguarding in this case centres around identifying the other victims of the suspect who are at risk from him.

Participant 11 speaks about breaking guidelines and rules which prevent officers from doing the wrong thing in relation to social media and its collection if it is in order to protect an individual. Although not specifically mentioning collection of evidence for court the guidelines that the investigator is refering to are the ACPO guidelines whose concern is the gathering of electronic evidence including social media.

4. The ranking of investigator goals

The four aims discussed above presented themselves clearly in the data during the coding process. The most commonly mentioned aim regarding social media was to collect it to use as evidence in court. This was the lowest in terms of priority however. There were no cases where the interviewees placed the collection of social media to use as evidence in court above the other three aims identified. The second identified aim in terms of importance for investigators was that of suspect identification. This had the lowest incidence of mention out of the four aims. This can be explained by the suspect being known in the majority of the cases discussed to the victim or identified through other means prior to the social media evidence being known to the investigator. Identification of the suspect and collection of evidence for court are closely intertwined. Without a suspect, there can be no prosecution and so no court case for evidence to be collected for. Criminal law requires first an act that constitutes the offence (actus reus) and

secondly a guilty mind (mens rea) which precipitated the act (Connor, 2009) before a criminal offence can be considered to have taken place. The 'guilty mind' necessitates a suspect. As such in order for a case to be heard in court a suspect is required. The collection of evidence can lead to the identification of a suspect. However, the identification of a suspect does not necessitate a court case or collection of the material that identified the suspect as evidence for court. This was shown in the examples where officers identified suspects using social media, but did not subsequently use that material for the purposes of evidence for court once the suspect had been identified. There exists the possibility that investigators would rather not identify the suspect if this were to compromise evidence collected for court, however this type of preference was not expressed during the interviews.

The third identified aim was to maintain victim engagement. Investigators were clear that the relationship with the victim was more important than the collection of evidence and in three cases more important that identifying the suspect. The primary aim identified was that of safeguarding. This aim is intertwined with the other three in that prevention of harm to the victim and others may entail maintaining a relationship with the victim, identifying the suspect and collecting evidence for court in order to convict an offender. Investigators expressed a willingness to damage the relationship with the victim and circumvent rules around the collection of evidence in order to identify other victims and the suspect in a case for the purpose of safeguarding. In this way a distinction is made between the aims of identifying the suspect for the purpose of the investigation and identifying the suspect for the purpose of safeguarding. The preferences as they are ordered from one to four are done so in an ordinal way with no measure of strength of preference of one choice of aim over another. I failed to find an explicit ordering of these 4 objectives during the literature review.

ACPO (2012) guidelines only address one of the investigator aims that being the collection of evidence for court. The other three aims identified above are not recognised in the guidelines nor is any guidance given as to where strategies could be found to address them.

5. Identifying the facets of social media as a unique problem

Investigators were seen across all 14 interviewees to recognise that a problem existed when coming across social media in their investigations as in the first step of Pretz, Naples, & Sternberg's (2003) model. Investigators also defined the problem that they were facing with ten separate facets being identified from the data. These were coded into the following categories: 1) failure of social media providers to engage with the police; 2) the lack of legislation granting police powers in relation to it; 3) the changing nature of social media; 4) an increased workload associated with social media; 5) restrictive guidelines; 6) lack of specialist support; 7) difficulty in accessing social media accounts; 8) a lack of training; 9) inadequate technical resources; 10) loss of evidence. These 10 coded categories reflect how investigators framed the problem of social media in the cases that they dealt with. All of the difficulties identified by investigators during the interviews have previously been acknowledged (Barnes, 2006; Kardasz, 2012; Trottier, 2012; Etzioni, 2016) and were referred to in the litearture review.

The table below shows the aspects of social media that caused them issue and which participants identified each issue:

1. Failure of social media providers to engage with the police Participants: 1, 2, 3, 5, 9, 10, 11	2. The lack of legislation granting police powers in relation to it Participants: 1, 5, 9, 10, 11	3. The changing nature of social media Participants: 3, 6, 10, 11, 12, 13
4. An increased work load associated	5. Restrictive guidelines Participants: 3, 5, 8, 9, 10, 11, 13,	6. Lack of specialist support Participants: 1, 2, 4, 6, 7, 9, 11, 12

with social media Participants: 1, 3, 5, 6, 7, 8, 9, 10, 12, 13, 14		
7. Difficulty of accessing social media accounts Participants: 1, 5, 9, 13, 14,	8. A lack of training Participants: 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	9. Inadequate technical resources Participants: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 14
10. Loss of evidence Participants: 1, 3, 4, 5, 9, 13,		

Table 15 - Facets of social media that cause issue for investigators

Categories, one, two, three, four, seven and ten are ones that are unique to social media and these facets have been noted previously and discussed in the literature review. During the interviews three of the five investigators who mentioned a lack of legislation as an aspect of social media that caused them issue expanded further on the cause of this. Their focus was on social media as communications data and how current legislation on communciation, namely RIPA 2000 did not easily encompass it. The issue of the right to privacy was raised, whether there is an expectation of privacy when communications are sent via social media and how communications are retrieved when investigators access suspects' and victims' social media accounts.

The first, second and seventh categories as listed above combine to form the 10th category in the table which pertains to loss of evidence. If social media providers fail to engage with the police then evidence cannot be collected from them. If there is a lack of legislation to force them to engage then again evidence cannot be obtained. The same is also true if

132

investigators cannot access pertinent social media accounts to collect evidence directly. Further to this, investigators were concerned about data being ereased from social media accounts by suspects, victims and witnesses, if not secured quickly enough.

The remaining categories (five, six, eight and nine) as posing an issue to them are not unique to social media. Investigators desired more knowledge around social media through training (category eight) and specialist resources in terms of personnel (category six). A lack of training has been identified as an issue by investigators in computer based crime (Goodman, 1996; Jewkes & Yar, 2008; Williams, 2008; Hunton, 2009; Awan & Blakemore, 2016), but also a wide range of other fields in policing including mental health (Lamb, Weinberger, & DeCuir Jr, 2002), family crisis intervention (Bard & Berkowitz, 1967), pursuit driving (Hill, 2002) and dealing with youth offenders (Pilavin & Briar, 1964). Similarly the need for specialist resources to support different areas of police work is noted in computer related crime (Hunton, 2009), cybercrime (Jewkes, 2013), fraud investigations (Button, Frimpong, Smith, & Johnston, 2007), mental health triage (The Police Foundation, 2016) and serious sexual assault investigations (Hester & Lilley, 2015). Restrictive guidelines have been widely acknowledged as having a significant impact on police work not only in relation to computer based evidence (Biggs & Vidalis, 2009) but more generally affecting officers ability to exercise discretion in all aspects of their work (Chakrabarti, 2008) and their ability to perfrom 'frontline' duties (Sindall & Sturgis, 2013). Finally it has been noted that technical resources at the disposal of the police to deal with computer based and internet crime are inadequate (Sommer, 2004; Hunton, 2009; Jewkes, 2013; Bryant & Stephens, 2014).

Previous studies (Chase & Simon, 1973; Simon & Simon, 1978; Glaser, 1999) have suggested that the greater the expertise in a particular field the clearer the individual is able to identify the pertinent factors in an encountered problem. The correlation between the number of factors identified in the issue and so the framing of the problem was compared

against investigator time working in a detective role. This is seen in the table below.

Participant number	Years working as a detective	Categories identified by participants as causing issue in relation to social media
Participant 10	28 years	1, 2 ,3, 4, 5, 8, 9
Participant 5	18 years	2, 3, 4, 5, 7, 8, 9, 10
Participant 9	12 years	2, 3, 4, 5, 6, 7, 8, 9, 10
Participant 1	10 years	2, 3, 4, 6, 7, 8, 9, 10
Participant 14	7 years	4, 7, 9
Participant 3	5 years	1, 3, 4, 5, 8, 9, 10
Participant 2	4 years	3, 4, 5, 8, 9, 10
Participant 11	3 years	1, 2, 3, 5, 6, 8
Participant 8	3 years	4, 5, 8, 9,
Participant 6	3 years	1, 4, 6, 8, 9
Participant 7	2 years	4, 6, 8
Participant 4	1 year	6, 8, 9, 10
Participant 13	1 year	1, 4, 5, 7, 8, 9, 10
Participant 12	1 year	1, 4, 6, 8, 9

Table 16 - Facets of social media that cause issue for investigators as identified by each interviewee

There was as can be seen no clear correlation. This was also the case when the total amount of time investigators had served in the police was compared against factors identified that framed the problem. Significantly, the studies (Chase & Simon, 1973; Simon & Simon, 1978; Lesgold, et al., 1988; Glaser, 1999) which identified that domain specific knowledge assisted in the identification of the factors that comprised a problem were conducted in 'laboratory' conditions. In those studies the participants did not have the opportunity to seek advice or knowledge from other sources when tackling the problems presented to them. During the coding process it became apparent however that investigators would activily seek knowledge to supplement their own when they encountered social media and were unable

to identify strategies to achieve their stated aims. Investigators sought knowledge from colleagues, supervisors, specialist departments and expressed a desire for additional training in relation to social media. The below table shows strategies to obtain information against the number of participants that selected each strategy:

1. Consulting with supervisor for advice (3 investigators)	2. Expressing a desire for additional training (13 investigators)	3. Sharing of professional knowledge (13 investigators)
4. Approaching specialist resources for advice (10 investigators)		

Table 17 - Strategies used by investigators to obtain further information about social media

The 'real world' which allows the transfer of knowledge during these interactions appears to have negated the difference between the knowledge that individuals hold with reference to the subsequent framing of a problem that is noted during 'laboratory' conditions. This significantly shows a willingness on the part of investigators to search for knowledge when they come across a problem that they do have the domain specific knowledge to frame. This was noted in chapter three during the examination of the crime reports where investigators were seen to approach specialist departments, their supervisors and the CPS as well as conducting their own research when they were coming across social media platforms that were new to them.

The ACPO (2012) guidelines do not explicitly define social media as forming a new and unique problem, although by mentioning it and providing four strategies / tactics to deal with it there is an inferred acknowledgement of it forming a separate issue. This absence is noticeable given that the

identification of a problem and defining its facets are articulated as the first two steps within problem solving (Pretz, Naples, & Sternberg, 2003) models.

Having recognised social media as a new 'problem' with distinctive facets and identified officer aims and goals the next stage of problem solving models is to identify decision making rules used by individuals. This is addressed in the next section.

6. Decision making rules

The first three steps that investigators were seen to undertake when approaching social media as put forward in the model of problem solving by Pretz, Naples, & Sternberg (2003) are described above. This includes first recognising that social media is a problem. Secondly, defining or framing the problem in terms of 10 separate facets and thirdly identifying four hieracrhical goals that investigators were pursuing. Investigators were also seen to conform to the last two stages of the problem solving model, these two stages being developing a strategy to reach those goals and evaluating the actions taken. These two steps as discussed in the literature review are further expanded upon in the decision making model proposed by Frauenknecht & Black (2010) into 5 separate stages. The first stage is for the decision maker to identify possible options. The second is to identify the consequences of those possible options being acted upon with the third being to identify how desireable each of those consequences is. The fourth is to assign a likelihood of those consequences occuring. The final stage is to utilise a rule by which to choose an option out of those identified. Rules that decide on which option is chosen are encompassed by the decision-making literature that concerns Heuristics (Elio, 2002; Gigerenzer, 2008),

Normative / prescriptive models (Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011) and Positive or descriptive models (Einhorn & Hogarth, 1981; Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011) described in the literature review.

To begin with, the options considered by investigators in relation to collecting evidence for court are examined. These options are further separated into three separate issues: the overall strategy to achieve the collection of evidence, the tools or tactic to enact a chosen strategy and the physical way to secure evidence. For each of those options the consequences that investigators envisaged happening are ascertained. The desirability of the options was weighed by investigators. In identifying the consequences and desirability of options, decision rules used by investigators to make a choice were identified. These are examined in the subsections below.

7. Obtaining evidence for the purpose of court

7.1 Investigators' strategies for collecting evidence

The following options were considered by investigators when looking to obtain evidence for court:

Option 1	Option 2	Option 3	Option 4	Option 5	Option 6
Gaining access to a social media profile by obtaining a username and password with the user's consent	Requesting the victim, suspect or witness to provide evidence from their profiles not in the presence of the investigator	Requesting the victim, suspect or witness to provide evidence from their profiles in the presence of the investigator	Requesting content directly from the social media provider	Seizing electronic devices	Seeking advice on how to obtain evidence
Using a work computer	Using a work computer	Using a work computer	Contacting the social media provider directly	Using equipment to download the device.	Approaching specialist departments
Using a standalone computer	Using a standalone computer	Using a standalone computer	Contacting the social media provider through the authorities' bureau	Using HTCU to download the device.	Approaching the CPS
Using a personal device	Using a personal device	Using a personal device			Obtaining supervisory advice

	Using the victim / suspect / witness device	Using the victim / suspect / witness device			Obtaining advice from colleagues
Using statements to describe social media content	Using statements to describe social media content	Using statements to describe social media content	Obtaining a report from the social media provider	Obtaining a report from HTCU	
Screen shooting images of social media content	Screen shooting images of social media content	Screen shooting images of social media content		Obtaining a report from equipment used to download the device	
Taking photographs of social media content	Taking photographs of social media content	Taking photographs of social media content			
Printing off images of social media content	Printing off images of social media content	Printing off images of social media content			
Using software to record investigator actions when viewing the profile	Using software to record investigator actions when viewing the profile	Using software to record investigator actions when viewing the profile			
Downloading the entire profile to an e mail account	Downloading the entire profile to an e mail account	Downloading the entire profile to an e mail account			

Table 18 - options used by investigators when looking to obtain evidence for court

Investigators identified three separate issues to consider when choosing options to deal with social media. The first (in black in the table above) was the overall strategy considered for accessing social media content. The second is seen in the subsequent rows which are green in colour. These identify the tools with which to fulfil each strategy for gaining access to social media content. The third is seen in the remaining rows in red. These pertain to the physical way in which the evidence would be secured. For each of these three options different decision rules were found as being used by investigators.

The ACPO (2012) guidelines identified three specific tactics for dealing with social media that were discussed in the literature review. The fourth strategy

was a catchall to 'always secure a copy of what is seen' without specifying how to do so.

The three specific tactics that it offers however are seen to be covered by those identified by officers to deal with evidence in the table above: Downloading the entire social media profile to an e mail account, the printing out of social media content and approaching the authorities' bureau for advice. As can be seen from the table above there were several other specific strategies and tactics identified by officers that are not identified, mentioned or discounted by the guidelines (ACPO, 2012).

7.2 Investigators view of the consequences of choosing overall strategies in obtaining evidence for court

Investigators identified the following consequences of choosing an overall strategy with regard to accessing social media content:

Option 1	Option 2	Option 3	Option 4	Option 5	Option 6
Gaining access to a social media profile by obtaining a username and password with the user's consent	Requesting the victim, suspect or witness to provide evidence from their profiles not in the presence of the investigator	Requesting the victim, suspect or witness to provide evidence from their profiles in the presence of the investigator	Requesting content directly from the social media provider	Seizing electronic devices	Seeking advice on how to obtain evidence
The ability to see all the content and not that just selected by the user	Minimised collateral intrusion on other persons	Minimised collateral intrusion on other persons	An independent third party providing evidence that cannot be challenged in court	An independent report providing evidence that cannot be challenged in court.	Ascertaining the correct way of obtaining social media evidence
Ease of access to the account	No ability to see the entire content of the social media profile.	Ease of access to the account	Time taken to have access to the content	Some social media content being missed.	Those persons approached not being able to provide adequate advice
Collateral intrusion on other persons		The ability to see all the content and not	The social media provider not		

		that just selected by the user	affording the content		
Inadvertent changes made to someone's account that they did not wish to happen					
The accusation could be levelled that evidence had been changed / deleted by investigators					
Contravening RIPA 2000 due to accessing live telecommunications data					

Table 19 - Consequences identified by investigators for choosing overall strategies for accessing social media content

The first line of the table above depicted in black writing details the overall strategy identified in the first table seen above. Under each of these six options are then shown investigators views of the possible consequences of undertaking each specific strategy. The rows in green show what investigators perceived to be positive outcomes and the conversely the rows in red show what officers perceived to be a negative outcome.

As described in the model by Frauenknecht & Black (2010) investigators used rules to decide which options to choose. Although the term 'rule' is used this is not to suggest that investigators were using one single or simple guideline to inform their decisions. As will be discussed below the 'rules' involved multiple strands, were complex in nature and applied differently to the separate aspects of how to approach social media.

The questions asked of investigators during the interviews did not probe the weighting of desireability as to the consequence of each of the options. What did not materialise also was a coherent or obvious weighing of the likelihood of outcomes in relation to each strategy. That is not to say that this consideration did not take place on the part of the investigators, rather that

the interview structure and questions did not address this explicitly. Decision making rules however did appear quite clearly and did so for each of the three separate issues identified in the first table above those being: choosing an overall strategy to access social media content; identifying the tools to do so; and finally how to secure the physical evidence. Investigators decision making rules with regard to physically securing evidence are examined first. This is then followed by the rules engaged to decide which tools were used, before finally examining the how the overall strategy is chosen.

7.3. Decision rules used by investigators when choosing how to physically secure evidence for court

When considering how to physically secure social media evidence detailed in red in the first table), investigators relied on their previous experiences. They directly transposed their experience from past events pertaining to the collection of non social media evidence and applied it to social media. The following comments exemplify this:

Participant 1: "*I think it just boils down to established and traditional methods of presenting evidence. So, it literally it is as simple as writing a statement to say I logged on to this site at this date at this time and this is what I saw and here's a photograph of it and hoping it will be good enough for the courts.*"

Participant 1: "*if I had you know a filing cabinet with a large amount of data in it, how would I present a single document or single page of a document or a paragraph of that page and I'm simply using the same principles to present something that's written on a screen or an image*"

Participant 3: "*It's like the old lady walking down the street and bringing in a blood-stained knife. Ultimately, she'll be the one who is questioned about where it was found in the circumstances, the person in the SDO (front counter) who has just accepted it and given to forensics to look at. Yeah. It's the same for anything, it is evidence. Its information. Tangible or not.*"

Participant 6: "*So when I go to a crime scene and see a bloody knife on the floor, I take a photo of it and exhibit that photo. I see evidence on social media I take a photo of it and exhibit that photo.*"

A total of nine investigators made a direct identification with other forms of evidence collection as influencing how they collected evidence around social media. This pertained to taking statements, photographing, obtain screen shots of and printing off social media content. The ability of an individual to associate a new situation with a past one is well documented (Orasanu, Martin, & Davison, 2001; Moriarty, 2015; Cookson, 2017). A prefect match is not required with a previous situation for the individual to make use of the rules that they used in the previous incident (Orasanu, Martin, & Davison, 2001; Moriarty, 2015; Cookson, 2017). This is true of the use of previous situations by investigators to inform their behaviour around social media because as has been shown above social media poses a new problem for investigators with facets that make it unique and different from previous problems encountered by them.

Participant 9: "*I've done it myself and it's worked for me in the past.*"

Participant 6: "*I've used it evidentially a few times. It's never been challenged the way I've done it. So far.*"

Both investigators were providing reasons for why they were content with the tactics that they were using for collecting social media evidence. They did so by seeking confirmation from past experiences that showed that the tactic that they were using was adequate and correct. This demonstrates both confirmation bias and the availability heuristics. Confirmation bias as they sought information to confirm that their choice of how to physically secure social media evidence is correct and the availability heuristic, as they were picking out a choice of physically securing evidence that they used previously and so is easily available for them to implement. Looking at past experiences however, and specifically when they apply to collecting other types of material and evidence, does not guarantee success for that strategy or tactic in the future or in relation to social media.

Representativeness heuristic is closely aligned to confirmation bias. It describes how individuals attribute beliefs to a certain set of events biased on their experience from similar sets of events in the past. With regard to the police, it has been noted that investigators rely on their professional knowledge to make decisions, a great deal of which is acquired from their own personal experience (Adhami & Brown, 1996; Smith & Flanagan, 2000; Stelfox, 2009). Again, this allows for the quicker formation of a hypothesis and plan as to how to deal with a situation, including collection of evidence. It may however also lead to errors, as the current situation may differ significantly to the ones encountered previously by the officer and lead to an erroneous hypothesis or identification of a suspect (Stelfox, 2009; Moriarty, 2015).

This engagement of the representative heuristic can be seen through the following investigator comments:

Participant 12: "*Only because I've had it in court and it's slightly different but this is my thinking towards it*"

Participant 6: "*That was never scrutinised or criticised at court*"

Both investigators were making comments about investigations that they had taken to court and strategies and tactics that were used not with regard to social media material but other electronic evidence. They then applied those same strategies and tactics to social media based on their positive experience in court.

The following comments allude to the availability heuristic (Ask & Granhag, 2005; Rossmo, 2009; Stelfox, 2009; Rassin, Eerland, & Kuijpers, 2010; Moriarty, 2015) being engaged:

Participant 4: Explained that it was natural to take a statement and exhibit Facebook posts in the way that the above example was given. That this was the way that evidence was exhibited and she had been taught.

Participant 7: "*I think it probably stems from harassment legislation way way way back, cause 10, 12 years ago, when we didn't have ACESO[1] machines, we would have to evidence, we would have to write verbatim the messages, even if there were a hundred messages, we would have to write them verbatim. And put it in a duty statement*"

The majority of investigators identified that their strategy or tactic of dealing with social media originated from previous experiences when asked directly for an explanation as to the approach that they were pursuing. For the reasons detailed above it is argued that these decisions are based on heuristics. In contrast three of the officers expressed their inability to identify the reasoning behind their decisions:

Participant 6: "*I think I just that was the best way I could think of dealing with that at that time. Yeah I don't think I've necessarily seen someone do it like that.*"

Participant 12: "*If I'm being honest, I'm not too sure. I suppose, I don't really know.*"

Participant 12: "*I don't know where that came from.*"

Participant 13: *"But I can't remember my thinking behind it.*"

This lack of immediate insight as to where a decision stems from has also been identified as an indicator of heuristics affecting the choices made by an individual and is discussed in more depth during the literature review.

---

[1] ACESO refers to equipment that is able to form a mirror image of data held on a mobile phone or SIM card. A limited number of officers have a licence and access to this equipment.

8. Investigators decision rules for choosing the tools with which to fulfill a chosen strategy.

8.1 The use of a personal device, standalone or normal work computer to access social media profiles

When making a choice between the tools with which to fulfil a given strategy from the choices of standalone, work, personal computers, victim and suspect computers, contacting social media providers directly in order to access social media accounts or using HTCU or equipment present in police stations to download electronic devices, heuristics were again seen to be employed. Specifically, this involved the availability heuristic (Ask & Granhag, 2005; Rossmo, 2009; Stelfox, 2009; Rassin, Eerland, & Kuijpers, 2010).

Investigators stated that personal devices, had previously been used by them to access social media, when it had first surfaced within investigations, however they no longer considered it a viable tool. The reason for this was the potential visibility of the investigators' personal profiles by suspects or witnesses, if personal devices were used. When determining whether to use a standalone computer or a normal work computer, the determining factor appeared to be the ease of access or availability of equipment:

Participant 1: "*At the moment we are introducing standalone computers where we can long onto Facebook anonymously but you are talking one computer per county and you are expecting people who work at one police station to travel down to another police station which is the best part of 60 miles so they can log onto a Facebook account.*"

Participant 6: "*I'm not saying it doesn't exist. But when you're rushed and you're juggling all these investigations.*"

Participant 8: "*Which was probably wrong. I don't know. I know we have a standalone in the ACESO room. I guess you're sat at your desk it's easier.*"

Participant 9: "*The lack of available computers. So, we've got that one, but as CID we probably don't have one in our office.*"

Participant 13: "*If you are looking up someone, that's the AIT standalone machine that's recording equipment that shows you what you did to find out what's circumstances for a job, look through Facebook, I can see behind it I suppose in court as in to prove that you haven't made it up if that makes sense. But that is there is a lot of reluctance from my colleagues to use that – oh for fucks sake, more time consuming, more faff, its more exhibits, whereas we are at our desk top, we've got the technology at our hands, let's just research people, find it, screen shot it*"

Investigators believed that the use of a 'stand-alone' computer with a distinct IP address not related to their police network was a preferable way to access social media profiles. Two investigators identified the reason for this probably stemmed from shielding their police IP address from suspects when intelligence work was being conducted on suspects' social media profiles. This reasoning may however be redundant when applying it to a suspect or victim social media profile that the suspect and victim were aware that police would be looking at. A further two investigators stated that the stand-alone computer had software installed that could record the investigator actions when looking at social media profiles. Aside from this the other investigators were unable to explain the reason for this preference other than to refer to guidelines or training courses.

Nevertheless 12 out of the 14 investigators expressed an inclination to use their own work computers rather than accessing a standalone due to the availability of their work computer in comparison to the standalone. Reasons for the lack of availability varied from someone else using the 'stand-alone' computer, it being in a different office, being in an inaccessible room to being in a different police station. Thus, the hurdle of unavailability could be as low as a walk along a corridor from the investigators office to the room where the 'stand-alone' was with the specific case files pertaining to the case. This was a conscious decision as officers were aware of guidelines or reasons for using a stand-alone computer but chose not to use this option due to what appeared to be the engagement of the availability heuristic.

8.2 Use of equipment at the police station or the HTCU to download electronic data from devices

Similarly, when investigators were considering whether to use equipment present at the police station to download the content of an electronic device or to submit the device to the HTCU, the ease of availability of the results and the time taken to obtain those results featured heavily. This was the case even though investigators believed that evidence provided by HTCU would be preferable to that gained from equipment available at the police station. The comments below are typical of those made:

Participant 6: "*We have a 5, 6 months turn around for phones so I wasn't about to, we have to deal with stuff expeditiously don't we, I wasn't going to submit all that stuff and leave him hanging for 6 months.*"

Participant 9: "*I mean ACESO is only a couple of years old. When it was just HTCU you were seizing and then sending phones off for you'd think a lot more before you think I'm going to download this person's phone. But definitely me nowadays, knowing that I've got people and we've got CSI that do it and people in our office that can ACESO download a phone if it's an option and someone's willing to sign a consent then I can give it back to them the same day you know and I've captured that evidence so, it's the systems available to us*"

Participant 10: "*I mean I think it was always viewed the best practice would be for example to seize the device or you wanted to go into an account that HTCU would video it and put their preamble on their initially and then you would get a very professional sort of package. But then when certainly I know their work is now sort of backed up probably 9 or 10 months.*"

Participant 14: "*if you are sending something off to the HTCU you are going to be waiting around 6 months for something to come back.*"

There appeared to be a choice between three weighted factors for investigators in relation to choosing whether to submit an item to the HTCU for examination. On the one side, there was the quality of evidence that

would be obtained by submitting a device to the HTCU. This was balanced against the speed with which this evidence would be returned and whether a device would be accepted for examination. The speed with which a device would be examined was identified by investigators as functionally important in gathering evidence for two reasons. First, the quicker a device is examined the more likely the investigation is to progress in a timely manner. Secondly, investigators were more likely to gain access to victims' electronic devices such as phones if they could return those devices back to them promptly. This reflects the strong attachment of individuals to their electronic mobile communications devices and specifically mobile phones (Oksman & Rautiainen, 2003; Rosen, 2004; Campbell, 2007; Green & Haddon, 2009; Vandebosch & Van Cleemput, 2009).

Furthermore there were process barriers to the submission of devices for examination to the HTCU. One officer highlighted that due to the restrictions on their resources the HTCU would only examine one item out of a number seized during an investigation. The investigator stated that it was difficult to make an informed choice around which item to submit. A second officer detailed that the HTCU unit would not examine an item unless there was a belief or suspicion that there was material present that would assist the case. This in the investigators' view was a reasonable procedure as the HTCU has a need to triage items for examination otherwise it would be overwhelmed with submissions that would most likely not hold any relevant material or evidence (Sommer, 2004; Hunton, 2009; Jewkes, 2013; Bryant & Stephens, 2014).

However, they gave the example of a particular case where the mother of a victim had told the officer that she had examined the victim's computer and found no relevant material on it. As such the HTCU would not have accepted the computer. Due to previous experience, the investigator believed that there still may be evidence on the computer that the mother had missed. This is a further example of the representative heuristic (Stelfox, 2009; Moriarty, 2015) being employed and of professional learning (Dewey, 1933; Argyris & Schön, 1978; Kolb, 1984; Gibbs, 1988; Johns, 1995; Brookfield, 1998; Thompson, 2000; White, Fook, & Garnder, 2006) being acted upon.

Although they identified that guidelines instructed that investigators should not examine electronic devices themselves as it was likely to alter data (ACPO, 2012) the choice facing them was to examine it themselves or lose any potential evidence. Having examined the computer, the investigator found evidence relevant to the case and as such, subsequently submitted the computer to the HTCU who examined it and produced a report to detail the evidence found. That police HTCUs are overwhelmed with submissions and work has been commented upon previously (Kshetri, 2009; Yar, 2013; Bregant & Bregant, 2014). However although there is clearly an impact on the amount of devices that can be examined and the time which it takes to do so, the HTCUs as evidenced in chapter 4 were shown to be continuing to function and provide evidence in cases concerning social media.

The use of equipment available at a police station was more widely considered. The reason for this was that a phone or tablet could be examined in a very short time frame. This allowed investigations to progress quickly and the electronic device be returned to the victim in question. Furthermore there was a perceived degree of independence about the report that was produced by the equipment, which made it an attractive option. There were however also impediments that prevented the use of such equipment. When there was a suspicion that indecent images were present on a device then guidelines instructed that they be submitted to HTCU rather than be examined locally. These internal TVP guidelines (Thames Valley Police, 2017) concerning indecent images found on electronic devices appeared to cause genuine frustration in officers. Secondly the examination by HTCU was believed to be more thorough than what was achievable with equipment at the station.

8.3 Approaching the CPS, supervisors or colleagues for advice

Although the CPS was contacted by investigators to apply for social media content from the United States, only three officers reflected upon approaching the CPS for the purposes of advice. The view of two of those

investigators was that the CPS was unable to offer useful advice as to how to deal with social media.

Participant 6: "*That never gets picked up on by CPS because they don't really know if we are doing rightly or wrongly*"

Participant 7: "*Yeah. I mean they wanted me to get. If I'm honest I don't think CPS really understand the whole social media stuff.*"

In both cases the investigators were commenting on previous experiences with the CPS and modelling their choices because of it. As discussed above this is indicative of both the representativeness heuristic (Stelfox, 2009; Moriarty, 2015) and of professional learning cycles (Dewey, 1933; Argyris & Schön, 1978; Kolb, 1984; Gibbs, 1988; Johns, 1995; Brookfield, 1998; Thompson, 2000; White, Fook, & Garnder, 2006) and incorporating past professional experience into present practice.

Professional learning cycles were also extended to knowledge held by investigators' co-workers. When considering colleagues, 12 out of 14 investigators spoke of using knowledge that their direct colleagues with whom they worked had suggested or that they had asked them of. This knowledge appeared to be accepted without much question. The following comments were typical of this:

Participant 6: "*Which I haven't done but my colleagues use them a lot and apparently you can get a link to this persons Facebook account*"

Participant 12: "*They're all pretty experienced in there. So, I've got no qualms in going to them.*"

Three of the officers made reference to consulting with their supervisors and again accepted the knowledge that they provided. There was no clear discernible reason for this acceptance that was given. The knowledge of direct colleagues was treated as an extension of their own knowledge. The absolute confidence in relation to advice given was also extended to colleagues from some other departments however this was not as universal when compared with direct colleagues. Whilst knowledge sharing between team members appeared to be inherently accepted by investigators this is by no means typical of working team environment (Cabrer & Cabrera, 2002;

150

Zarraga & Bonache, 2003; Cabrera, Collins, & Salgado, 2006). The interaction between supervisors and investigators appeared to be very organic. This and investigators interaction with other team members is reflective of the organisational structure and culture (Cabrer & Cabrera, 2002; Zarraga & Bonache, 2003; Cabrera, Collins, & Salgado, 2006). An example of this behaviour with regard to social media was investigators downloading the profiles of social media users to email addresses (in the case of Facebook). This behaviour was learnt from other colleagues. This particular technique of physically securing the evidence differs from the others used by investigators as it is a new technique not mentioned as being previously used or applied to other forms of evidence gathering.

8.4 Contacting the social media provider directly or via the authorities' bureau

Contacting the social media provider directly was discussed by five investigators. The first provided an example of having tried to obtain information directly from a social media provider based in Canada but being informed that the request would have to be made through the authorities' bureau. The second suggested approaching social media providers' directly as a line of investigative enquiry, but had no experience of doing so themselves. As such these two investigators had made a conscious decision to approach the provider directly at some point in their career. The other three rejected it out of hand stating that social media providers would not provide the information directly to an officer. Two of those investigators were part of the authorities' bureau, which grants authorities under RIPA (2000) and applies under these authorities for communications data. These two investigators took this knowledge from the roles that they were performing.

In addition to the two investigators from the authorities' bureau a further two investigators spoke of obtaining evidence from social media providers via the authorities' bureau. The reason for applying to the authorities' bureau was for two reasons. The first was again the quality and independence of the evidence that would be obtained from the service providers. The second was for obtaining advice as to how to actually obtain material from social media

151

providers. There were three caveats mentioned to obtaining content from user accounts in this way. The first was that regarding Facebook, they would only supply this evidence if the offence was judged under the criteria of being 'serious crime'. This bar is set for crimes that would attract a custodial sentence of 3 years or more on first conviction, include violence, financial gain or conspiracy. The second was the amount of time that would pass between an application being made and the evidence being obtain, which could take up to 12 months. Finally, it was stated that some social media providers would simply not provide the evidence even if requested (Hodge, 2006; Boyd & Ellison, 2007; Ward, 2011; Kardasz, 2012).

9. Decision rules used by investigators when choosing an overall strategy to access the content of a social media account

When deciding which option to choose to access social media content in an account a greater number of rules appeared to be engaged and more conscious consideration given to the decision than with the choices described above. First, the likelihood of a case going to court was considered. Secondly the gravity of a case was reflected upon. The following comments made by investigators illustrate this:

Participant 6: "*Well I would say we have different workloads, we have more serious jobs and less serious jobs, we have limited personal resources and time and effort to put into things, so we have to be proportionate about the seriousness of the offence, the willingness of the victim, the likelihood of trial or is it something that is going to be NFA'ed*"

Participant 6: "*And if the offence is more serious and you've got a willing victim you've got to guess I be proportionate with your investigations and some take more commitment, more, more work than say do others. I think as a police officer you need to think where the job may end up eventually. If you are looking at crown court trial you probably look to do more investigation than if that wasn't going to happen. Inevitably those investigations get more scrutiny.*"

Participant 10: "*So it was a case of look, how pivotal is this information. How serious is this offence we are dealing with.*"

The reason for this consideration was the quality of evidence that would be gathered. The more important the case and the greater likelihood that the case would be heard in court then investigators tended to view evidence that was more independent of them and more complete in nature as preferable. This preference was made as there was a belief that evidence that was independent of them was less likely to be challenged in court (although none of the investigators had actually experienced such a scenario). A victim or a witness providing evidence was seen as being independent of the investigator. Similarly seizing a device to be examined by either HTCU or equipment at the police station was seen as a way of obtaining impartial evidence. The most secure evidence was believed to be that provided by the social media provider themselves. The decision was driven by fear of evidence being excluded or the investigators themselves being criticised over their actions.

Whilst victim and witnesses providing the social media content themselves was perceived to be independent of the police and required smaller resources when compared to submitting items to the HTCU or using police equipment to examine it, investigators were wary of it. The reason for this was a fear that the victim or witness may have altered or not included all the content present and in so doing exposing the prosecution of the case at court to risk. As such although the evidence was independent there was a question as to its completeness.

Obtaining evidence from logging onto individuals' accounts whether they belong to a victim or suspect created several issues for investigators. First, it was identified that this course of action would be against internal guidelines. Secondly there was an ethical issue about collateral intrusion. Thirdly consideration was given whether an application under RIPA 2000 was required. Fourthly how to evidence the content of the account presented issues. Finally, the independence of the evidence could be challenged as

the accusation could be levelled that the content of the account was tampered with.

In contrast to many of the decision rules observed and described above which involved heuristics when considering which tools to use and how to physically evidence the content of social media accounts, this choice was considered. Investigators were clearly weighing up the desirability of options

The first two comments below are examples of investigators referring to the strength of evidence when supplied by the social media provider themselves and the second two comments refer to the strength of evidence when provided by the HTCU:

Participant 3: "*however with authority of authorities and the things that they do, they can produce a proper effectively legal document which again I could do by submitting a statement, however there is more weight to a report from Facebook saying for instance at this time at this place this message was made from this person to this person this is the IP address, that give us locations, it simply rubber seals the fact that it is true and it's not just the investigator colluding with the witness.*"

Participant 5: "*2 elements there, 1 is best evidence, it won't have been tainted, it won't have been in some way changed or there is a potential for the accusation of change*"

Participant 10; "*I mean I think it was always viewed the best practice would be for example to seize the device or you wanted to go into an account that HTCU would video it and put their preamble on their initially and then you would get a very professional sort of package. But then when certainly I know their work is now sort of backed up probably 9 or 10 months.*"

Participant 14: "*Well more professional for want of a better word, but yes because they are a unit that specifically is there to do that kind of thing. Whereas when you're sat with a witness or victim who is going through a computer and showing you certain things then things might get missed off. So, evidence-wise I would suggest its best to go through.*"

This choice of more independent and complete evidence was however tempered by the cost of obtaining that evidence and the value of that

evidence as assigned to it by the investigators. With independence and completeness of the evidence there was also a perceived cost in obtaining it when measured against the time and effort on the part of the investigators. The costs included the time it would take for an electronic device to be examined by HTCU, the process for a submission to be made to examine a device or obtain material from a social media provider directly, and convincing a victim to give their electronic device to the police. The choice considered by investigators was an intertemporal one. The ease of obtaining evidence now set against how that evidence would be perceived in court at a later time. The following comments illustrate this:

Participant 1: "*So I think the courts are mindful to what we can realistically achieve with the technology and the resources available to us with social media.*"

Participant 1: "*it is a question of trying to balance the evidential standard over what can be achieved in a timely manner*"

Three of the options or at least the initial steps were relatively low cost in terms of time and effort. The first was obtaining advice whether that be from colleagues, supervisors or specialist departments. The second was to seize an electronic device in preparation for examination. The third was victims and witnesses providing the social media content themselves to investigators. Whilst investigators obtaining advice from their colleagues was not noted in the crime reports, the seizure of devices was. The popularity of seizing items for examination appears at odds however to the observation that most content of user accounts was held either in a cloud or in external storage rather than on the electronic device of the user. Indeed, this was supported by investigators comments:

Participant 12: "*if you ACESO a phone there is only very limited information that you can get off there and because Facebook and Instagram aren't saved to the hard drive itself it's almost impossible to get it off an ACESO*"

However, the data pertaining to social media accounts that was recorded on these devices however limited still provided important information to investigators as the following comment shows:

155

Participant 9: "*Because WhatsApp when you send an image via WhatsApp it automatically saves depending on your settings but generally can automatically save into your photo albums and she did still have that so I could tell via Facebook that was my man.*"

There was no ranking constructed between the gravity of the case and the likelihood of it appearing in court against which option was used to access social media content as the information needed to do so was not present in the interviews. Although different in nature this observation lends support to the relationship between the importance of the social media material obtained (relevant, evidence or critical evidence to the case) and the number of strategies / tactics employed regarding it noted from the crime reports. This is an example of intertemporal decision-making, which are noted in both descriptive/positive (Einhorn & Hogarth, 1981; Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011) and normative/prescriptive (Crozier & Raynard, 1997; Koksalan, Wallenius, & Zionts, 2011) models of decision making. The intertemporal relationship in this case is balancing the value of the evidence, against the effort made by investigators in relation to it.

Nevertheless, the majority of investigators identified that their strategy or tactic of dealing with social media originated from previous experiences when asked directly for an explanation as to the approach that they were pursuing. For the reasons detailed above it is argued that these decisions are based on heuristics. In contrast three of the officers who were interviewed expressed their inability to identify the reasoning behind their decisions. This lack of immediate insight as to where a decision stems from has also been identified as an indicator of heuristics affecting the choices made by an individual. By taking a course of action that has not been consciously thought out, the implication is that an unconscious thought process has been utilised. It is this unconscious decision-making process that heuristics can describe (De Martino, Kumuran, Seymour, & Dolan, 2004; Dane & Pratt, 2007; Gigerenzer & Gaissmaier, 2011). Individuals' use of heurisics whether concious or unconcious on which to base their decision is driven by contextual cues which identify it as a type of situation in which a

particular response is appropriate (Klein, 1999; Higham & Vokey, 2000; Gigerenzer & Gaissmaier, 2011).

10. Decision making regarding keeping the victim engaged, identifying suspects and safeguarding

When considering the goal of maintaining a relationship with the victim and social media two options were considered. The first was the seizure of electronic devices and the second was obtaining usernames and passwords to victims' accounts. When considering the seizure of electronic devices belonging to victims the main concern of investigators was victims not consenting to the seizure and keeping the device from the victim for an extended period of time. This action was envisaged to alienate the victims from the investigation and from the investigators. As such the use of equipment available at a police station was universally preferred to submission of a device to the HTCU. The reason for this was that a phone or tablet could be examined in a very short timeframe. This allowed for the electronic device to be returned quickly to the victim. One of the investigators stated that if the victim did not provide their device, then it would change their strategy with regard to the victim. It would necessitate them arresting the offender in contrast to dealing with them voluntarily in order that their mobile phone could be seized. Obtaining the username and password to victims' accounts if given was not extrapolated on further.

Information from the interviews regarding options and their consequences pertaining to the goal of suspect identification was the least prolific out of the four identified goals. In the comments made, how the suspect was identified and the evidence presented to court did not become a pertinent issue for investigators. Options that were considered included: seizing victim devices for examination and open source research regarding suspects on the internet. Within these two options the only one further extrapolated was that of seizing victims' devices for examination. The issue of the victims not wishing to give their devices up was raised in the same vein as discussed

with the goal of obtaining evidence for court and maintaining a relationship with the victim.

When considering decision making regarding safeguarding three options were considered which were also identified and used in the goal of obtaining evidence for court. These were requesting information from the social media provider, accessing the victim's account having obtained their username and password and finally seizing the victim's device. However, as the goal changed so did the consequences of the actions considered in contrast to the other three goals. The consequences of not obtaining the social media content were couched by investigators in terms of the level of danger and its immediacy towards victims. Thus, the strategy and the tools with which to achieve the aim were differentiated between by the amount of time it would take to identify suspects and victims. As such investigators stated that they were not concerned with guidelines present that instructed them not to use work computers to access social media profiles as time was of the essence. The only caveat with contacting social media providers directly was that social media providers would provide information immediately only if there was an immediate threat to life present.

11. Conclusion

In the interviews, investigators identified the same strategies and tactics with respect of how they dealt with social media as were found during the examination of the crime reports with the exception of one strategy, which featured in only one crime report out of a total of 106. This finding supported the reliability of the results found (Thornberry & Krohn, 2000) in both sets of data. During the course of the interviews four goals were identified that detectives strive towards when considering social media in their investigations. These four goals were found to be hierarchical in nature. All four aims have been previously identified in literature examining police and more specifically detective work. However, they have been either assumed to form part of detective work by researchers in the case of evidence collection and suspect identification or in relation to all four goals they have

been noted as being prescribed onto the police through legislative changes and governmental pressure. The identification of these aims by investigators themselves and in the hierarchical order described in this chapter is an original way of identifying how investigators approach the issue of social media.

It was found that the approach that was taken when social media was encountered could not be overlaid onto descriptive or normative models of decision making or those that encompassed heuristics. Instead it was suggested that 'problem solving' models (Bransford & Stein, 1984; Sternberg, 1985; Pretz, Naples, & Sternberg 2003) are better equipped to describe how investigators approach social media. The first three steps of 'problem solving' as defined by by Pretz, Naples, & Sternberg (2003) were recognised as being acted out by investigators. The first of these steps is a recognition that social media presents a problem, which was identified by all the interviewees. The second step is to identify the facets of the problem that social media presents. Ten were found and categorised. It was suggested that a lack of domain-specific knowledge did not hinder the ability of investigators to identify the facets of the problem that social media poses due to the ability of investigators being able to seek and obtain knowledge from various sources. This was also supported by the findings from the examination of the crime reports. This is in contrast to results obtained in studies more generally around the issue of problem framing (Chase & Simon, 1973; Simon & Simon, 1978; Lesgold, et al., 1988; Glaser, 1999) that were conducted under 'laboratory conditions'. A number of these facets that framed social media as a problem were found to be unique in nature. Finally the third step - the identification of the goals of the problem solver was seen as discussed above in terms of four hierarchical aims that investigators pursue. The remaining steps of the 'problem solving' model correlate to the processes noted as occurring within normative, descriptive and heuristic decision-making models (Shogren, et al., 2008; Frauenknecht & Black, 2010).

It was demonstrated that investigators were seen to engage in four out of five of the steps of the decision-making model as put forward by

Frauenknecht & Black (2010) when considering the aim of collecting evidence for court. First this involved identifying options for how to access social media content, the tools appropriate to do so and the physical of way recording this content. Secondly there was a clear consideration by investigators of the implications of choosing a particular strategy and thirdly a recognition that some consequences were desirable whilst others were not. Finally, rules were used by investigators to inform their choice of how to deal with social media. It was commented on that the assessment of the likelihood of an outcome taking place – the remaining step of the decision-making model was not noted, but neither was it explicitly addressed during the course of the interviews.

The rules used to inform investigators' choice of how to physically secure evidence were shown to be driven by heuristics both consciously and unconsciously. Specifically, these were Confirmation Bias, the Availibility Heuristic, and the Representativeness Heuristic. Types of tactics used by investigators to physically secure evidence were transposed from techniques used to collect other types of evidence. These included writing statements, photographing and printing off screen captures.

Within these heuristics, models of professional learning were also noted and a striking feature of this was that knowledge that was transferred or shared between investigators did not appear to be questioned but was accepeted as being correct. One technique of physically securing evidence that was new and not previously employed by investigators in relation to other forms of evidence was the downloading of social media profiles onto an e mail address. A second example of professional learning was that investigators had stopped using personal devices to access social media profiles.

When considering which tools to use to fulfil a particular strategy the Availibility Heuristic was again shown to be engaged. The ease of access or availability of equipment such as standalone computers or ease of submission and time taken for HTCU's to provide evidence featured heavily in guiding investigator decisions. When making a decision however it was not simple the availability of tools that was considered by investigators. How quickly the investigation could progress, the effect on the victim, whether

they would allow their electronic device to be taken from them and the quality of the final evidential product were all considered. This showed that not only was the availability heuristic being engaged but that there were also conscious intertemporal choices being made. In making this decision, investigators were assigning desirability or lack of to the different possible outcomes.

The greatest amount of conscious consideration was given to deciding which option to choose to access social media content and a greater number of rules appeared to be engaged. The gravity of the case and the likelihood that it would appear in court was at the forefront of officers' thinking. Independence and completeness of evidence were seen as desirable. However the more arduous the process to obtain the evidence and the longer it took to do so the less desirable it was seen to be. Accessing social media profiles of victims or suspects by investigators whilst practiced by a number of investigators had a number of drawbacks. These included: it being against internal guidelines; ethical issues around collateral intrusion; how to evidence the content of the account once accessed; that it could draw accusations of tampering by investigators; and finally that it may fall under the auspices of RIPA 2000.

Information relating to the decision making process with regard to keeping the victim engaged, identifying suspects and safeguarding was much less plentiful. The choices made by investigators were less complicated with fewer options to consider.

1.   Evaluation of the study

The research used a grounded theory methodology (Glaser, 1978; Strauss & Corbin, 1994). Significant to this approach is that the researcher plays a key role in the emergence of the theory from the data. As such any prior knowledge that the researcher holds has the potential to impact on the interpretation of the data that is collected (Cutcliffe, 2000). A certain amount of literature was reviewed around decision making processes prior to the collection and analysis of the data and the researcher was acutely aware that this may in turn impact on how the data was viewed by them. However, when the data was examined the theory that had been initially considered was clearly seen not to offer an explanation as to the processes that were observed. As a result, further theoretical concepts were sought to explain the behaviour of investigators and literature on 'problem solving' (Getzels, 1982; Simonton, 1999; Pretz, Naples, & Sternberg, 2003) was found to model what was observed well. Not only was 'problem solving' not reviewed in the initial literature review, but it was also not known to the researcher prior to the data collection phase. This was a significant endorsement first of the impartiality of the researcher in this study as a grounded theory practitioner and secondly for the grounded theory approach used in this research and the emergence of theory from the data collected. The impartiality of the researcher as an 'insider' was also considered as being able to negatively impact on the study. It was shown however that the initial focus of the researcher as treating social media as evidence or being able to have an impact on a case at court was narrow in scope and that three other objectives were identified as being pursued by investigators. Recognition of this in the data provides evidence that the researcher as an insider continued to be open to new ideas outside of their original conception of the issues present.

Two separate sets of data were examined. Crime reports were considered as they offered a way of collecting data suited to the objectives of the study

without the preparation time required to construct a data collection mechanism. They appeared at the outset to offer the advantages of both primary and secondary data (Jupp, 1989; Kothari, 2004). However as has previously been noted in the literature (Alison, Snook, & Stein, 2001; Canter & Alison, 2003; Horvath & Brown, 2006; Feist, Ashe, Lawrence, McPhee, & Wilson, 2007) the reports were found to not contain the rationale for decision making around social media but rather only the strategies and tactics that were used. A total of 19 separate strategies and tactics were identified and a tentative hypothesis drawn that officer decision making around the number of them engaged to deal with social media depended on the importance of social media to a specific case. In other words whether it formed critical evidence, evidence or relevant material in the investigation. This hypothesis around the importance of social media to the investigation and its correlation to what strategy or tactic was pursued to evidence it was later found to be supported by the data from the interviews. There it was seen that there was an evaluation by investigators as to which strategy or tactic they would use depending on whether they believed that it would be relied upon in court and scrutised or not.

The crime reports also highlighted that attempting to show which type of investigations social media featured in was difficult, as government crime classification rules masked the number and types of crimes against which a record was created. Although this was the case, no other system of classification was identified that was superior. By looking more closely at the types of crime it was found however that the social media featured in three main types of offences. These were sexual, physical non-sexual and harassment crime categories. Identifying offence types where social media has a higher chance of featuring in, is useful signposting for investigators within any relevant guidelines.

Both sets of data supported the notion that investigators were not hampered by a lack of knowledge around social media as has been previously proposed (Jewkes & Yar, 2008; Awan & Blakemore, 2016). Rather, the crime reports suggested an organisational structure that facilited knowledge sharing and this was further confirmed in the data from the interviews.

The second data set was obtained from conducting interviews with investigators. This data set provided greater validity to the research (Kirk & Miller, 1986; Winter, 2000; Golafshani, 2003; Gadd, Karstedt, & Messner, 2011) as the findings drawn from the data in the crime reports were repeated in the data found in the interviews. This included challenging the notion that officers did not have sufficient knowledge to deal with social media, strategies and tactics noted for dealing with social media, and a correlation between the perceived importance of social media and how it was approached by investigators. The interviews however provide a much richer source of data for theory generation. This was because processes could be both observed and decision making rationale directly questioned. Problem solving models were found to describe the behaviour of investigators noted in the interviews.

The literature review identified that ACPO (2012) were the most up to date guidelines aimed at investigators rather than forensic scientists describing how to deal with digital evidence and specifically social media. There were four main strategies / tactics identified in these guidelines, three of which were seen to be engaged in the crime reports and all four engaged by investigators in the data obtained from the interviews.

Two police areas consented to participating in the study. Although the two data sets provide validity for each other, they do so only relation to the police areas from which the data was drawn. As such it is difficult to apply the findings universally across all police areas in England and Wales. This was exacerbated by 13 of the 14 participants in the interviews originating from one police area. There is thus an obvious scope for further research in examining data from a greater range of police areas and with a greater number of participants.

2.   Deductions from research

There were a number of original notions found during the course of the research. The overarching theme connecting them was that social media as evidence or relevant material within investigations was a new and unique

issue that officers had not encountered previously. Investigators however, were using heuristics based on their experience of other forms of evidence to manage social media, which did not provide adequate strategies to do so. In so doing they risk evidence being collected that may subsequently be excluded in court. The most current guidelines (ACPO, 2012) were found to not adequately address the issue of social media or provide sufficient advice for investigators. Furthermore, the goals of investigators were found to be wider than that of evidence collection and diverged into suspect identification, victim engagement and safeguarding, objectives not mentioned or covered by current guidelines in relation to social media.

To elaborate on the above, the research supported the conclusion that when faced with social media, interviewees were shown to mirror the steps identified as being followed by individuals when they encounter a new issue in problem solving models (Getzels, 1982; Simonton, 1999; Pretz, Naples, & Sternberg, 2003). This finding has significance and has not previously been noted. First, it identifies social media as a new issue and a new problem that has not been encountered before by investigators. Investigators identified it as a problem by defining ten separate facets to social media of which six are unique to it. Whilst these facets have already been described by academic researchers as differentiating social media from other forms of electronic evidence, these researchers are specialists in their fields and approach the issue from a systemic perspective rather than that of practitioners.

Similarly, detectives themselves identified four goals that they aim to achieve – goal identification being a consequent step in problem solving models to defining the problem. This research confirms the view of earlier academics and academic literature that investigator and detective aims encompass the collection of evidence (Maguire, 2003; Stelfox & Pease, 2005; Tong & Bowling, 2006; Stelfox, 2009) and suspect identification (Isaacs, 1967; Greenwood, 1970; Greenwood, Chaiken, & Petersilia, 1976; Eck 1983). It also shows that the statutory requirements relating to safeguarding (Adoption and Children Act 2002; Children Act 2004; Laming, 2009) and victim engagement (Adler, 1991; Lees & Gregory, 1993; Temkin, 1999; Jordan, 2001; Horvath & Brown, 2009) are being adhered to by officers.

However, these four objectives have previously been identified by researchers or legisators from a top down perspective rather than by practitioners themselves. That practitioners themselves identify with these goals and order them in a particular way is a new finding.

The ranking of these goals has not been noted or observed before. Although these four objectives were identified from the data through the coding process, it did not appear that investigators were consciously explicitly defining all four of them and ranking them in a certain order. There is an implication from this for the training of officers, that being to explicitly identify these objectives so that all four are conciously considered by investigators during the decision making process.

Different strategies and tactics were noted as being employed by officers when coming across social media. These strategies / tactics were found to be more varied in scope than the four put forward in the ACPO (2012) guidelines. Heuristics, specifically the availability, confirmation bias and the representative heuristic were found to be the drivers of officers' decision making rules as to which strategy or tactic they chose to use. The use of heuristics driving evidence collection in this way has not been previously noted. This is important as it shows that officers are relying on previous experiences of dealing with evidence that in many cases are not appropriate to dealing with social media, which is discussed further below.

3. Drawing pedagogical implications

Social media featured in 106 out of 600 crime reports examined. This constitutes just under 1/5 of the investigations examined, which is a notable amount. With the permeation of the internet through society, such numbers are only bound to rise in the future. Although social media features in the appendices to the guidelines (ACPO 2012) on digital evidence, neither the appendices nor the main body of the guidelines provide a clear strategy of how to deal with it and suggestions when instructing how to record it are at odds with the four principles that start and form the basis of the document. This research has shown that social media poses a problem for investigators

and as an issue has unique facets that have not been encountered before. Furthermore, officers are adapting their own solutions and in some cases using heuristics based on previous experiences of evidence collection, which may not be appropriate to social media. As such there is a very clear need to address and clarify in guidelines provided to officers this issue of how investigators first of all view and secondly approach social media in their investigations. Not doing so risks evidence not being collected in line with legislation such as RIPA (2000) and as a consequence being excluded in court.

It was found that social media featured heavily in three crime categories. These were sexual offences, physical non-sexual assaults and harassment. The ACPO (2012) guidelines only refer to indecent images of children when discussing offences other than those where the cyberelement fully constitutes the crime as being offences where digital evidence might feature. These findings show however that social media is prominently present in a number of other offences categories. Making this clear in guidelines relating to social media would better alert officers to the crimes where social media might feature.

There are references in the guidelines that identify some of the unique aspects that social media presents when compared to traditional evidence. These include first of all its transient nature and that evidence can be lost. Secondly, that the data itself is not in the main stored on the electronic device of the user and so cannot be seized and imaged in a traditional way. Thirdly that the provider of the service may be based abroad and furthermore not allow or give access to the data if is requested. Fourthly that the evidence may involve communications data that is in transit) and thus fall under the regulation of RIPA 2000. These features of social media encompass some, but not all of those highlighted by investigators in this research. As was discussed in the previous chapter a critical aspect of problem solving is first recognising that there is a problem and secondly defining the boundaries of that problem (Getzels, 1982; Simonton, 1999; Pretz, Naples, & Sternberg, 2003). Whilst all the investigators interviewed identified multiple facets of social media that made it unique, none of the

167

investigators identified all the facets. Clearly defining all the differences between social media and traditional digital evidence would assist investigators by giving them clarity that it constitutes a unique and new form of evidence to which the four principles at the start of the document are difficult to apply to. This would be crucial to developing guidance in relation to social media that was either part of revised ACPO (2012) guidelines or separate in its own right.

That investigators were utilising the availability (Ask & Granhag, 2005; Rassin, Eerland, & Kuijpers, 2010), representativeness (Garb, 1996; Brannon & Carson, 2003; Moriarty, 2015) and confirmation (Klayman, 1995; Nickerson, 1998; Oswal & Grosjean, 2004) heuristics and previous data collection techniques for social media became very apparent during the research. However, it has been shown that social media forms a new and unique form of evidence, as mentioned in the above paragraph, and that previous data collection techniques are not always successful when utilised with regard to it. For example, the primary technique for securing digital material in the past and advocated by the ACPO (2012) guidelines was seizure and analysis of electronic devices. Due to the majority of social media content being held in servers outside of the jurisdiction of the UK law enforcement agencies (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015), this strategy is unlikely to capture the information sought by investigators. By making this explicit, it would focus investigators on the necessity to approach social media in a different way rather than attempt to use techniques for the collection of other types of evidence.

Having emphasised that social media is different, the differing goals of investigators should be acknowledged. Accessing the content of social media for safeguarding or maintaining victim engagement is not the same as accessing it for obtaining evidence for court or for identifying a suspect. The principles that form the basis of the guidelines are designed so that evidence can be accepted in court. If safeguarding is the principal aim however then these rules may not need not be adhered to. It is accepted of course that laws remain in place (RIPA 2000) that protect peoples' right to privacy and that place constraints on how law enforcement officers act in relation to

communications data. However, there is also legislation present (Adoption and Children Act 2002; Children Act 2004; Laming, 2009) as discussed in the previous chapter that places obligations on the police to protect vulnerable adults and children. The aim of collecting evidence in a way that is acceptable to a court (which entails adherance to RIPA 2000) and that of safeguarding were identified by interviewees in some situations as competing with each other. Indeed, investigators stated that they would be content to explain any actions in court that were in contravention of guidelines if the aim was to ensure children's safety. This is a significant finding as it shows investigators' willingness to be accountable to the courts for their actions contravening guidelines, because of their professional judgement. As highlighted in chapter 2, that the aims of officers are competing has been previously noted in academic literature (Jordan, 2001) and this research supports those findings. Identifying differing aims and how it affects the way in which social media is approached would provide greater clarity for officers. As with the facets of social media it was not clear that investigators were explicitly consciously defining their aims or ordering them. By explicitly outlining them and ordering them, it would undoubtedly assist their decision-making processes.

Guidelines (ACPO, 2012) state that social media providers would provide the best evidence but may also not provide data that is requested. On the other end of the scale they also suggest that investigators secure a copy of what they see as there may not be another opportunity to do so. Rather than leave these two opposites as unexplained they should be expanded on as they appear conflicting. First, the reason why evidence provided by the social media provider would constitute best evidence requires rationalisation. Explicit rationalisation of why a strategy should be pursued will assist officers in deciding whether or not to pursue it based on its merits. Investigators during the interviews stated that this was due to the independence of the evidence and that interference from the investigator could not be levelled at the evidence if presented in court.

Secondly, the circumstances under which evidence is not likely to be provided by them must be explained. Investigators highlighted this as a

169

negative aspect of applying directly to the social media provider for evidence. If officers know the criteria and time frames under which service providers will release information, then they can make an informed decision to pursue or disregard this option on that basis. It is accepted that the criteria under which social media providers will supply content will vary depending on the jurisdiction in which they are based and on the social media provider themselves (Barnes, 2006; Hodge, 2006; Boyd & Ellison, 2007; Ward, 2011; Kardasz, 2012; Etzioni, 2016). A reference data base of social media providers encountered by law enforcement officers could be maintained that contains this information. Where a provider is unlikely to provide this information then a list of alternative strategies that could be employed would be listed. This is important as the investigators interviewed did not have confidence in the actions that they were pursuing.

Two other tactics are put forward by the guidelines. The first is to save information from chat logs onto a removable media device and if this is not available to print off the chat logs. However, a situation could easily be envisaged from the scenarios spoken about during the interviews where this would not be possible. For example, a victim whose access to social media takes place on a smart phone. They victim has no other electronic device such as a computer or laptop from which to access social media. They do not have or are not prepared to provide a removable media device. They have no way to connect their device to a printer. Amongst the tactics used by investigators was that they had asked victims to e mail them files containing such chat logs. Such a tactic appears to afford the same benefits as saving the file to a removable device or printing off the file.

In such a situation investigators, as has been demonstrated in interviews could also decide to access a user's social media account themselves having obtained appropriate permissions from the user. However, the guidelines refer to 'information in transit' and suggest contacting the authorities' bureau if this is the case. Accessing a social media user account where the data pertaining to that account is stored in the United States would mean that the data would have to travel from the data storage system of the social media provider to the computer that the investigator is using.

This has been noted as being telecommunications data that is being requested not only from a different physical location but one that is likely to be in a different legal jurisdiction (Taylor, Haggerty, Gresty, & Hegarty, 2010; Mason & George, 2011; Taylor, Haggerty, Gresty, & Lamb, 2011; Chung, Park, Lee, & Kang, 2012). If that is the case, then it may fall under the auspices of RIPA 2000. However, this is not clear in the guidelines. If that is what the guidelines are referring to, then it should be made explicitly clear to deter officers from accessing such accounts themselves. If it is not, then investigators should be given the freedom to access suspect and victims' profiles if their consent is obtained.

From the guidelines it was not clear in how many different ways evidence should be captured. Furthermore, investigators offered additional strategies and tactics for evidencing social media than the four put forward in the guidelines. By legitimising different forms of data gathering it may save police forces and investigators time and resources by not requiring evidence to be duplicated. For example, if it was made clear that a chat log from a social media account downloaded to an email account formed adequate evidence, it may be unnecessary to then also obtain that chat log from the social media provider themselves. Each such suggestion would need to be made in conjunction with persons who are experts in the field of digital cloud computing forensics. (Biggs & Vidalis, 2009; Damshenas, Dehghantanha, Mahmoud, & Solahuddin, 2012) with the technical implications of evidence collection techniques being considered.

Another tactic offered by investigators that were not identified in the ACPO (2012) guidelines was for the victim to access the social media account in their presence on a computer that is capable of recording images on a media device or that is capable of printing. In order for this to happen that equipment needs to be readily available for investigators to use. One of the more noticeable complaints by investigators was that standalone computer to access social media were not easily accessible. For investigators to use them, such standalone computers would have to be readily available not only in intelligence offices where witnesses would not be able to be brought to but in dedicated rooms for witnesses. Stretched resources (Sommer,

171

2004; Hunton, 2009; Jewkes, 2013; Bryant & Stephens, 2014) mean that the availability of a strategy or tactic as found in this research, has a significant impact on whether it will be used.

As a consequence of devices being triaged before being accepted for examination by HTCUs, there are circumstances as seen during the course of the interviews that mean that devices that may contain evidence will not be accepted by them. Investigators have a choice in those circumstances to either disregard these devices or examine them themselves, to ascertain whether there is evidence present on them. Rather than not acknowledge this or risk the loss of evidence a process could be put in place that formalises investigators ability to examine devices that are not accepted by HTCU.

Two solutions could be considered. At the most inexpensive, investigators could examine devices themselves, maintaining their own audit trail until such a moment that they find evidence, at which point the device could be submitted to the HTCU. The success of these tactics would depend on whether the initial examination by investigators would be challenged at court for altering the evidence held on the device and the computer literacy of the investigator conducting the examination. On the other end of the scale equipment could be provided and a number of investigators could be trained to image the memory of electronic devices. These images could then be examined for evidence. The option would incur a cost both in equipment and training but may be prove more robust to challenge at court. Consideration could be given to extending this process to circumstances where the devices require more immediate examination than HTCU resources allow for (Kshetri, 2009; Yar, 2013; Bregant & Bregant, 2014).

4.   Conclusion

This study set out to ascertain the types of investigation that social media features in, the strategies that detectives use when they encounter social media in an investigation, to understand the decision-making process behind the choice of strategy and compare it against the most up to date guidelines available for investigators. It found that social media appeared in a

significant amount of investigations and across a broad spectrum of complex case types investigated by detectives. Further to this however, the data examined found these research questions to be incomplete in trying to understand how officers deal with social media. The initial focus of the research concentrated on social media as evidence or having the potential to impact on a case as relevant material. During the interviews this focus on social media as evidence was shown to be only one aspect of investigators' goals. These goals also prominently included suspect identification, victim engagement and safeguarding with the collection of social media as evidence ranked the least important of the four.

Where the initial research questions sought to simply identify strategies and why they were chosen, the data showed that there were further initial steps in investigators appraisal of social media. First, there was a recognition that it presented a problem and secondly defining its facets as an issue. These first two steps then assisted in informing strategies that would be chosen to deal with social media. The strategies and tactics that were used by officers were wider in scope than suggested in the guidelines. It was found that the decision rules on which the choice of strategy or tactic used was driven by heuristics. Ascertaining how social media is approached by investigators is crucial to providing advice and guidelines. The most up to date guidelines in the form of the ACPO (2012) guidelines were found to be lacking in both options and explanation of preferred choice of strategy or tactic. A number of recommendations are made based on the findings of this research on how to improve the guidelines. These focus on increasing investigators' cognition of why social media forms a new and unique problem, formalising the aims that they have, and identifying strategies and tactics to deal with social media together with an explanation of the strengths and weaknesses of each. Finally, a number of practical observations are noted around submissions of digital evidence to HTCUs and the availability of digital forensic equipment at the disposal of detectives.

ACPO: The Association of Chief Police Officers (ACPO) or in full 'The Association of Chief Police Officers of England, Wales and Northern Ireland', was an organisation that was established in 1948 and for a significant period of time led the development of policing practices in England, Wales, and Northern Ireland (ACPO, 2005c; Parker, 2013). Following the Parker Review into ACPO, it was replaced in 2015 by a new body, the National Police Chiefs' Council. ACPO did not have any powers to enforce its recommendations or any mandate to do so. However, in practice it allowed and facilitated national policy to be formed rather than individual police areas replicating work in the same fields (ACPO, 2005c; Parker, 2013).

Aims: This thesis refers to 'aims' in three different settings. First, the aims of the research. Secondly, the aims noted within the ACPO guidelines for investigators and thirdly the four aims of detectives identified from investigator interviews. In all three cases, the use of the word aim is used interchangeably with the words 'goal' and 'objective', They are seen to represent an idea or desired possibility that can be attained through a course of action (Latham & Yukl, 1975; Hsiaw, 2010 Locke & Latham, 2013). It is noted that a distinction can be made between the word 'goal', 'aim' and 'objective'. This sees a sliding scale. On one end a goal can be understood to be a general statement of intent over a longer term. On the other an objective may be more specific and relate to a shorter time span in terms of achievement (Lindvall, 1964, Saylor & Alexander, 1974; Wise, 1976), with an 'aim' sitting between the two (Taylor, 1997). Whilst noted, not uniquely (Percy, 1973; Hoffman, 1980) this distinction is not used in this research between the three terms.

ASC: Refers to Avon and Somerset Constabulary. In 2017 ASC employed 2759 police officers (Home Office, 2018). It is one of 43 separate semi autonomously administered police areas within England and Wales. It encompasses the counties of Somerset and South Gloucestershire, which includes within it the cities of Bath and Bristol as well as the towns of Weston-Super-Mare, Taunton and Yeovil. It is one of the largest police forces in England and Wales covering both urban and rural areas (HMICFRS, 2018b). Between the 1 October 2015 and the 31 March 2016 there were 131, 226 crimes reported to the force (HMICFRS, 2018b)**.** The area covered by the force is 1,844 square miles in which there are approximately 1.65 million residents mainly centred in the urban areas of Bristol and Bath (HMICFRS, 2018b). A

significant proportion of the population originates from an ethnic minority background (HMICFRS, 2018).

Basic Command Unit: This is the largest organisational sub structure that police areas are divided into. It was introduced into policing and replaced the previous two-tier structure of 'divisions' and 'sub divisions' (Loveday, 2006).

CAIU: Refers to 'Child Abuse Investigation Unit'. This is a specialist department of investigators and detectives concerned with investigation of crimes committed against children and child protection. Such units are present across forces in England and Wales (National College of Policing, 2015).

CID: Refers to the 'Criminal Investigation Department'. This was the successor to the Detective Branch in the Metropolitan Police and has become a term used for plain-clothes police detectives in the UK (Newburn, 2007). The work of the unit encompasses the investigation of serious and complex crime (Maguire, 2003).

Correlation: The word correlation has been used in this thesis specifically with regard to three variables and an association between them. The first two variables are that of frequencey and variation of strategies used by investigators in an investigation. An association is implied between these two variables and the third variable, that being importance of social media to the investigation. In other words whether it forms critical evidence, evidence or relevant material in an investigation. In using the term 'correlation', it is not used in the mathematical sense of there being a calculated correlation co-efficient and a linear relationship between two variables. There is no statistical dependance that has been calculated between these two variables and so what is noted is an association between variables that has not been quantified (Chen & Popovich, 2002; Liebetrau, 2018). What is meant by the term correlation in this research is that there is a tendency towards a concomitant or associated variation between two variables, where there is a causative connection. In other words where one variable causes a variation in another indirectly (Mari & Kotz, 2001; Chen & Popovich, 2002; Shevlyakov & Oja, 2016).

CPS: Refers to the 'Crime Prosecution Service'. This is an agency that is independent of the police and prosecutes criminal cases in England and Wales that have been investigated by the police and other agencies (Crown Prosecution Service, 2017).

Cloud Storage Systems: A repository or storage system for digital material that can be rented, bought or is provided by a third party (Garfinkel, 2010; Ward, 2011; DeSousa, 2013).

DAIU: Refers to 'Domestic Abuse Investigation Unit'. This is a specialist department of investigators and detectives concerned with investigation of crimes committed within a domestic setting. Such units are present across forces in England and Wales (National College of Policing, 2016)

Decision Making: Decision Making for the purpose of this research is defined with five distinct and separate stages:

"*a process used to make choices among contending courses of actions and includes the following steps: (1) identify possible options, (2) identify possible consequences for each option, (3) evaluate desirability of each consequence, (4) assess likelihood of consequences, and (5) use a "decision rule" that identifies the best option and maximizes well-being based on current beliefs and knowledge*" (Frauenknecht & Black, 2010, p113).

Detective: a warranted officer who has undergone and completed the second tier of the 'professionalising investigation programme'. This includes completing the National Investigators Examination, attending a five-week course and undergoing a work-based assessment (National College of Policing, 2017a).

Evidence in the investigation: Evidence is defined within the 'core investigative doctrine' as material that is:

"*[…]sufficiently relevant to the facts in issue is admissible, subject to the exclusionary rules. The test for relevance is: 'evidence which makes the matter which requires proof more or less probable' (Lord Simon of Glaisdale in DPP v Kilbourne (1973) AC 729, at p 756. The 'facts in issue' are those facts which the prosecution must prove in order to establish the guilt of a defendant"* (ACPO, 2005, p.26).

Evidence critical to the outcome of the investigation: This is not a category that is defined within professional literature. It is defined in this research as evidence as per the definition used above, without which a successful resolution of a case could not be reached. The test as to whether a resolution is successful or not is whether the CPS deem that a charge can be brought against a suspect based on the

evidence, or whether an investigator or supervisor can make a decision that no crime has taken place.

GBH: refers to 'Grievous Bodily Harm'. There are two offences created in which Grievous Bodily Harm can be inflicted or sustained both detailed under the Offences Against the Person Act 1861 (s.18 and s.20). Under the act 'grievous bodily harm' is defined as 'serious' or really 'serious bodily harm'.

Goal: A goal represents an idea or desired possibility that requires a course of action in order to achieve it and commitment in doing so (Latham & Yukl, 1975; Hsiaw, 2010 Locke & Latham, 2013). As such the achievement of a goal necessitates a process (Fried & Slowik, 2004) and when the term is used in this research it refers to an individual consciously setting it (Hsiaw, 2010; Locke & Latham, 2013). Within this research the term 'goal' refers to the four issues that investigators wish to achieve of: Safeguarding, Victim engagement, Suspect Identification and Collection of Evidence. It is noted that there are alternative ways of defining and viewing a goal from other academic fields including economics (Suvorov & van de Ven, 2008), engineering (Miller & Pribram, 1960) and education (Urdan & Maehr, 1995), which remove the concious element of goal setting by individuals.

Grounded Theory: Grounded theory was adopted to analyse the primary data collected. This methodology is well-suited to building theory in a relatively unexplored field (Glaser, 1978; Schreiber, 2001; Goulding, 2002). The approach adopted in this research as to when a literature review was undertaken was that advocated by Strauss and Corbin (1990) and this extended to the coding approach used in examining the crime reports. Strauss and Corbin (1990) argued for the use of 'axial codes'. These codes are theoretical codes that offer a structure or 'skeleton' for further codes that emerge from the data to be built around (Kelle, 2007). In coding data from the crime reports such axial codes were used. These codes centered around the importance of social media to a case, specifically whether the social media content formed 'relevant material', 'evidence in the case' or was 'evidence critical to the outcome of the case'. It was these codes that provided the framework for the inference drawn in chapter four, that the more important social media was to an investigation, the greater the frequency and variety of actions performed in relation to it. The 19 categories that emerged in the crime reports detailed in tables 8 through to 13 originated from what was written by investigators

and supervisors in the investigative logs contained in the crime reports. Each crime report that had a mention of social media in the three axial categories was anonymised and saved. They were then examined line by line by the researcher. Sentences, part sentences or words that appeared to the researcher as significant or forming concepts were recorded on a separate coding document. In practice this entailed the recording of any mention of social media and placing it in or creating a category for it. Practical text books on using grounded theory often suggest the use of 'post it' notes (Bringer, Johnston, & Brackenridge, 2004; Gabbay & Le May, 2004) and the physical writing of 'memos' (Holton, 2007; Lempert, 2007; Reichertz, 2007) to assist in the formulation of categories and dependency between them. Although post it notes were initially tried, the researcher found 'microsoft word' a much easier tool to use. Eventually the initial categories that were created were collapsed into larger more encompassing categories that formed the 19 seen in the 6 tables. The axial codes (Strauss and Corbin, 1990; Goulding, 2002; Reichertz, 2007) then allowed the formation of an inferred link between the 19 categories and a process the investigators employed. As discussed in the literature review when the data from the interviews was coded, the technique became more in line with that advocated by Glaser (1992). Each interview barring one was recorded. The recording was then typed into a transcript by the researcher. As each transcript was created, sentences, part sentences and words were taken form it and grouped into categories on a separate 'microsoft word' document. As before the initial categories that formed were collapsed into larger ones. The categories that formed were so distintinct and strong that the 'axial framework' that was used to assist the coding process in the examination of crime reports was deemed to be constrictive rather than assisting in identifying links between categories.

Heuristics: Heuristics describe rules that individuals fall upon when asked to make decisions often when faced with an inability to process all the information at their disposal. They explain some decision making, offering a quicker way for an individual to make a decision with less information whilst offering a degree of optimisation (Simon, 1955; Elio, 2002; Gilovich & Griffin, 2002; Snook & Cullen, 2008).

HOCR: Refers to 'Home Office Counting Rules'. These are provided by the Home Office to give consistency in crime recording across England and Wales and detail where there is statutory obligation to implement them (Home Office, 2014).

HMIC: Refers to 'HM Inspectorate of Constabulary'. This is an agency independent of the police that assesses individual police forces on a wide range of competencies and publish publicly available reports (HMIC, 2017).

HTCU: Refers to 'High Tech Crime Units'. These are specialised units within law enforcement agencies that deal with digital and technical aspects of policing and tackling technology related crime (Jewkes & Yar, 2008; Hunton, 2009; Awan & Blakemore, 2016).

Inductive Reasoning: This is a method of reasoning or reaching conclusions based on the expanding of a particular observed set of circumstances into a generalisation (Sloman & Lagnado, 2005; Bryct, 2009a, Keane & Eysenck, 2010). As such an inductive argument (in contrast to a deductive one) cannot alone achieve certainty even if all the premises are true (Copi, Cohen, & Flage, 2007; Keane & Eysenck, 2010). Rather an inductive argument can be classed along a scale from 'strong' to 'weak'. Inductive reasoning encompasses heuristics within it in that it can describe how individuals come to conclusions on limited experiences and make predictions based on current knowledge (Keane & Eysenck, 2010). It does not however completely overlap the concept of heuristics. Whilst heuristics describe the decision making of individuals based on previous experience, they may not include all of the individual's current knowledge and experience. As such heuristics may distort an individual's inductive reasoning by for example only identifying readily available knowledge to support a conclusion (availability heuristic) or identifying knowledge that confirms a conclusion that the individual is seeking to confirm (confirmation bias). Furthermore, heuristics need not require a conscious process of reasoning. Professional Learning cycles (Dewey, 1933; Argyris & Schön, 1978; Kolb, 1984; Gibbs, 1988; Johns, 1995; Brookfield, 1998; Thomspon, 2000; White, Fook, & Garnder, 2006) can also be seen to really upon inductive reasoning in that individuals learn from their experience and alter their predictions and choices based on their professional knowledge gained. The closeness of various models describing human thought processes, in this case inductive reasoning (Sloman & Lagnado, 2005; Bryant, 2009a, Keane & Eysenck, 2010), heuristics, reasoning by analogy

(Holyoak, 2005; Bryant, 2009a) and professional learning models has been identified as showing that such models are somewhat arbitrary in delineating and camouflaging what are similar forms of thinking (Keane & Eysenck, 2010). Other theories of reasoning which are deductive in nature include 'Rule', 'Evolutionary' and 'Semantic' models (Leighton & Sternberg, 2013). Rule models suggest that individuals have certain mental commands that are followed in reaching a decision. Evolutionary models propose that humans have evolved patterns of reasoning that have allowed them to meet specific needs during the evolutionary process, for example in constructing social contracts. In line with this, heuristics can also be seen to provide 'rules of thumb' which individuals follow in reaching an outcome. All of these models fall under the umbrella of 'positive' or 'descriptive' that seek to describe, understand and model the actual choices that are made by individuals (Einhorn & Hogarth, 1981; Crozier & Raynard, 1997; Koksalan, 2011). Whilst not excluding the validity of these models or their potential application to decision rules employed by investigators during the problem-solving process, clearly identifiable examples of such rules were not visible in the data.

Investigation: The two definitions of 'investigation' as detailed within CPIA (1996) have been adopted in this research:

"*For the purposes of this Part a criminal investigation is an investigation conducted by police officers with a view to it being ascertained—*

(a)whether a person should be charged with an offence, or

(b)whether a person charged with an offence is guilty of it"

Art. 22, CPIA (1996)

Investigative actions: Investigative actions when referred to fall into the definition as put forward by the National College of Policing (National College of Police, 2018) Authorised Professional Practice:

"any activity which, if pursued, is likely to establish significant facts, preserve material or lead to the resolution of the investigation. The volume of actions should be proportionate to the type of investigation"

(National College of Police, 2018)

Investigative Strategy: An investigative strategy is referred to by the National College of Policing (National College of Policing, 2018) in the following way:

"*The purpose of an investigative strategy is to:*

- *identify the most appropriate line(s) of enquiry to pursue*

- *determine the objective of pursuing particular lines of enquiry*

- *identify the investigative action(s) necessary to efficiently achieve the objectives, taking into account resources, priorities, necessity and proportionality*

- *direct and conduct investigative actions to gather the maximum amount of material which may generate further lines of enquiry*

- *understand and manage community impact.*"

and within the Murder Manual (ACPO, 2006) it is defined as:

"*the principal aim of the investigative strategy is to locate and gather*

Material"

(ACPO, 2006, p.56)

Both of these definitions identify with the strategies found during investigator interviews as shown in table 19 on page 136. These strategies determine the objective of obtaining access to social media content, take into account resources, the ability to gather the maximum amount of material and understanding community impact (shown in red and green within the table).

Multi Agency Safeguarding Hub: A hub of public sector agencies located in the same physical location, sharing information and decision making with the aim of safeguarding vulnerable individuals (Home Office, 2014a).

NDM: Refers to the 'National Decision Model'. This is a framework put forward by the National College of Policing for officers to use when making decisions (National College of Policing, 2014a). The model was initially developed by the National Police Improvement Agency on behalf of ACPO (NPIA, 2012). The model is purported to be suiteable for all decision making in a police setting including operational and non operational situations. As such there may be an expectation that this model would have featured in investigators' decision making and been either visible in the crime

reports examined or discussed during the interviews. Whilst envisaged by ACPO (2012) and the National College of Policing as being prescriptive in nature, the NDM is very similar to and overlays onto models of professional learning cycles (Dewey, 1933; Argyris & Schön, 1978; Kolb, 1984; Gibbs, 1988; Johns, 1995; Brookfield, 1998; Thomspon, 2000; White, Fook, & Garnder, 2006). These models are descriptive in nature rather than prescriptive, having been constructed following observations of how professionals in different fields make decisions. Whilst there was evidence of professional learning cycles utilised within the research, there was no direct evidence of the NDM being employed by investigators. It was not within the scope of this research to identify why this was the case. However that the NDM was not noted as being used is in line with the findings of the research, where social media was noted as being approached as a 'fuzzy scenario' (Pretz, Naples, & Sternberg, 2003), In such a scenario the problem is not clearly defined to the decision maker and requires first of all recognition that a 'problem' exists and then the subsequent defining of the problem's facets (Bransford & Stein, 1984; Sternberg, 1985; Pretz, Naples, & Sternberg, 2003). These steps are not present within the NDM. This is in contrast to a situation where the issue is distinct and decisions can be applied within clear parameters (Pretz, Naples, & Sternberg, 2003).

National College of Policing: The National College of Policing was created in 2012 as a professional body for the police service in England and Wales. It states that it's functions are to develop knowledge, provide education and to set standards (National College of Policing, 2017).

Normative / prescriptive models of decision making: These models of decision making look to identify the optimal decision given a certain set of circumstances (Crozier & Raynard, 1997; Camerer & Loewenstein, 2003). Such models can assist decision makers to identify this optimal choice where a decision is required.

Objectives: This thesis refers to 'objectives' in three different settings. These are: the objectives of the research, the objectives noted within the ACPO guidelines for investigators and the four objectives of detectives identified from investigator interviews. In all three cases, the use of the word objective is used interchangeably with the words 'goal' and 'aim', Goals are seen to represent an idea or desired possibility that can be attained through a course of action (Latham & Yukl, 1975; Hsiaw, 2010 Locke & Latham, 2013) and is detailed above in the glossary. It is noted

that a distinction can be made between the word 'goal', 'aim' and 'objective'. This sees a sliding scale. On one end a goal can be understood to be a general statement of intent over a longer term. On the other an objective may be more specific and relate to a shorter time span in terms of achievement (Lindvall, 1964, Saylor & Alexander, 1974; Wise, 1976), with an 'aim' sitting between the two (Taylor, 1997). Whilst noted, not uniquely (Percy, 1973; Hoffman, 1980) this distinction is not used in this research between the three terms.

Positive / Descriptive models of decision making: Positive or descriptive models seek to describe, understand and model the actual choices that are made by individuals (Einhorn & Hogarth, 1981; Crozier & Raynard, 1997; Koksalan, 2011).

Principles: In this thesis the term 'principle' refers firstly to the knowledge that investigators have as to the 'principles of an investigation' and secondly to the 'principles of digital investigation' as set out in the ACPO (2012) guidance on digital evidence. The 'principles of an investigation' are set out by the National College of Policing (2018) in their authorised professional practice. The ACPO (2012) guidance on digital evidence describes 'principles of digital investigation' as 'laws' and 'rules' to be adhered to by an investigator when dealing with digital evidence. It describes these principles as being in place in order for investigators to show objectivity in court (ACPO, 2012).

Problem Solving: The definition of problem solving as put forward by Pretz, Naples, & Sternberg (2003) was adopted. This model is represented in five clear and separate stages that an individual progresses through when encountering an unidentified problem, the model being cyclical in nature. These stages are as follows: a) Recognition that a problem exists, b) Defining or framing the problem, c) Identification of the goals, d) Developing a strategy to reach goals, e) Evaluation of actions in relation to the goals. In this definition, decision making is seen as being subsumed within the problem solving process but not fully constituting it (Wehmeyer and Shogre, 2008; Frauenknecht & Black, 2010).

Ranked Aims: Refers to the ordering or aggregating of items by their importance through individual preference (Brams, 2008; Balinksi & Laraki, 2011; Langville & Meyer, 2012). Specifically in this thesis it is used as a term with regard to the four

aims of detectives when dealing with social media identified from investigator interviews. No conflict in ordering was noted between investigators.

Relevant Material: The definition within Criminal Procedure and Investigations Act 1996 (CPIA 1996) is used within this research:

"*it appears to an investigator, or the officer in charge of the investigation or the disclosure officer to have some bearing or on the surrounding circumstances unless it is incapable of having any impact on the case*" (CPS, 2005, p36).

Sampling: The sampling technique in this research falls under that of 'systemic random sampling' (Acharya, Prakash, & Nigam, 2013) or 'consecutive sampling' (Schuster & Powers, 2005; Bowers, House, & Owens, 2011; Sharma, 2017). In this type of sampling the first date is selected at random and then 'k' number of samples are selected from this point onwards (Schuster & Powers, 2005; Bowers, House, & Owens, 2011; Acharya, Prakash, & Nigam, 2013; Sharma, 2017). The advantage of this system is that the cost is low in that the process of selecting a 'probability sample' is not incurred, either in design or in its implementation. It also has high internal and external validity and is better that convenience or snowball sampling in controlling sample bias. It is often considered as the best non-probability sampling method (Sharma, 2017). The disadvantage is that it is not a true probability or random sample and that it may be time or seasonally affected (Schuster & Powers, 2005; Bowers, House, & Owens, 2011; Acharya, Prakash, & Nigam, 2013; Sharma, 2017).

Strategy: Strategy as a concept has been defined in various different ways (Gray & Williamson, 2002; Jarzabkowski, 2005) with many authors describing the difficulty in precisely characterising the term (Jarzabkowski, 2005; Dolman, 2005; Slack & Lewis, 2008) or eschewing doing so (Mills, Platts, Bourne, & Richards, 2002; Ayson, 2004). The interchangeable nature of the meaning assigned to 'strategy' creates potential for any analysis of data against theoretical concepts to become confused (Frauenknecht & Black, 2010). To avoid confusion, as with 'problem-solving' a set definition of strategy was used in this research. The intention again was not to give preference to a particular definition of strategy over another, but rather set out the definition for the purpose of clarity. Freedman (2003) provides a detailed examination of the concept of a strategy and his observations on what constitutes a

strategy are adopted. Freedman (2003) argues that a strategy is more than simply a plan, but involves an objective whose attainment may involve an element of conflict. Without conflict, a strategy is simply a plan to achieve an objective. He describes two broad types of strategic planning. He first talks about innate decision making, skill or flair as a way of formulating strategy. This neatly describes heuristics (Elio, 2002; Gigerenzer, 2008) as a way humans navigate complex scenarios in a short period of time. He then describes a second method that involves a conscious analysis of the situation to achieve an objective where the situation is particularly complex. As is seen in the data, both situations are noted. Furthermore Freedman (2003) lays an emphasis on the means available to an individual to achieve his objective. This is clearly very pertinent in the decision-making processes that investigators go through, whether it is their consideration of the physical equipment at hand or their ability to obtain information from foreign jurisdictions. Freedman's (2003) view on strategy sees it as a process that moves through various states. This characterisation can see strategy as compatible with the different stages of problem solving (Pretz, Naples, & Sternberg, 2003) that individuals move through.

Tactics: As with strategy, the term 'tactic' has been described in many different ways and fields (Freedman, 2003; Gross, 2016). There is a delineation between tactics and strategy at the level at which an action or process is implemented. The term tactic was initially set and described in doctrines of war (Freedman, 2003; Gross, 2016). In such doctrines where strategy concerns itself with the setting of overall objectives and pursuit of power, tactics are implemented in individual situations that cumulatively seek to achieve the strategy (Freedman, 2003; Gross, 2016). The term 'tactic' in this thesis is used interchangeably with the term 'tool'. They describe the way investigators achieve the overall strategy that is set and the physical way in which evidence is secured (as shown on table 18 on page 134).

Tools: The term tool within this thesis is used interchangeably with the term 'tactic' as defined above. It is used to describe the way investigators achieve the overall strategy that is set and the physical way in which social media evidence is secured (as shown on table 18 on page 134).

TVP: Refers to 'Thames Valley Police. This is one of 43 separate semi autonomously administered police areas within England and Wales. It is the largest non-metropolitan police force in England and Wales and encompasses the counties

185

of Berkshire, Buckinghamshire and Oxfordshire. It is divided into 12 local policing areas (Thames Valley Police, 2018). Between the 1st of April 2016 and the 31st of March 2017 there were 138, 710 crimes reported to the force (Thames Valley Police, 2017)**.** The area covered by the force is 2,216 square miles in which there are approximately 2.4 million residents mainly centered in the urban areas of Oxford, Milton Keynes, Aylesbury, Maidenhead and Slough. Around 15% of the population originate from an ethnic minority (HMICFRS, 2018c). In 2017 TVP employed 4186 police officers (Gov, 2018).

Victims' Charter: This lays out the obligations that are incumbent on criminal justice agencies including the police to victims of crime. Key aspects of the code include defined entitlements for victims separated into different categories including children, young people, parents and businesses (Victims' Commissioner, 2018).

Bibliography

Acharya, A., Prakash, A. S., & Nigam, A. (2013). Sampling: Why and How of it? . *Indian Journal of Medical Specialities*, 4(2): 330-333.

ACPO. (2000). *The murder investigation manual.* London: National Policing Improvment Agency.

ACPO. (2005). *Guidance on Investigating Serious Sexual Offences.* London: Assocation of Chief Police Officers.

ACPO. (2005). *Practice Advice on Core Investigative Doctrine.* Cambourne: National Centre for Policing Excellence.

ACPO. (2005, July 02). *The Purpose of ACPO.* Retrieved from ACPO: http://www.acpo.police.uk:80/about/about.html

ACPO. (2006). *Murder Investigation Manual.* London: Assocation of Chief Police Officers.

ACPO. (2012). *ACPO Good Practice Guide for Digital Evidence.* London: Association of Chief Police Officers of England, Wales & Northern Ireland.

Adhami, E., & Brown, D. P. (1996). *Major Crime Enquiries: Improving Expert Support for Detectives.* London: Home Office Police Research Group Special Interest Series Paper 9.

Adler, Z. (1991). Picking up the pieces: a survey of victims of rape. *Police Review*, 1114-1115.

Ajala, E. (2007). Cybercafes, Cybercrime Detection and Prevention. *Library Hi Tech News*, 26-29.

Alison, L., Snook, B., & Stein, K. (2001). Unobtrusive measurement: using police information for forensic research. *Qualitative Research*, 1(2), 241-254.

Allen, M. (2011). *Textbook on Criminal Law.* Oxford: Oxford University Press.

Argyris, C., & Schön, D. (1978). *Organization learning: A theory of Action perspective.* Reading Mass: Addison Wesley.

Ashworth, A. (2010). *Sentencing and Criminal Justice.* New York: Cambridge University Press.

Ask, K., & Alison, L. (2010). Investigators' decision making. *Forensic psychology in context: Nordic and international perspectives*, 35-55.

Ask, K., & Granhag, P. (2005). Motivational sources of confirmation bias in criminal investigations: then need for cognitive closure. *Investigative Psychology*, 2(1), 43-63.

Ask, K., & Granhag, P. (2007). Motivational Bias in Criminal Investigators' Judgements of Witness Reliability. *Journal of Applied Social Psychology*, 37(3), 561-591.

Awan, I., & Blakemore, B. (2016). Policing Cyber Hate, Cyber Threats and Cyber Terrorism. In I. Awan, & B. Blakemore, *Policing Cyber Hate, Cyber Threats and Cyber Terrorism* (pp. 173-192). Abingdon: Routledge.

Ayson, R. (2004). *Thomas Schelling and the Nuclear Age: Strategy as Social Science.* London: Taylor & Francis.

Baggili, I. M., Mislan, R., & Rogers, M. (2007). Mobile Phone Forensics Tool Testing: A Database Driven Approach. *International Journal of Digital Evidence*, 6(2), 1-11.

Bailey, A., Barr, O., & Bunting, B. (2001). Police attitudes toward people with intellectual disability: an evaluation of awareness training. *Journal of Intellectual Disability Research*, 45(4), 344-350.

Balinksi, M., & Laraki, R. (2011). *Majority Judgement: Measuring, Ranking, and Electing.* London: The MIT Press.

Bard, M., & Berkowitz, B. (1967). Training police as specialists in family crisis intervention: A community psychology action program. *Community Mental Health*, 3(4), 315-317.

Barnes, S. (2006, September 4). *A privacy paradox: Social networking in the United States.* Retrieved from First Monday: http://www.firstmonday.org/ojs/index.php/fm/issue/view/203

Barrett, E. (2005). Psychological research and police investigations. In L. Alison, *The forensic psychologist casebook: psychological profiling and crminal investigation* (pp. 47-67). Cullompton: Willan Publishing.

Bayley, D. (1998). Criminal Investigation: Introduction. In D. Bayley, *What Works in Policing* (pp. 71-74). Oxford: Oxford University Press.

Bayley, D. (2002). Law Enforcement and the rule of law: is there a tradeoff? *Criminology & Public Policy*, 2(1), 133-154.

Berger, M. (2005). What Has a Decade of Daubert Wrought. *American Journal of Public Health*, No. S1, p. 59-65.

Berry, G., & Klein, R. (1993). Motion-induced grouping may not modulate the flander compatibility effect. A failure to replicate Driver & Baylis. *Canadian Journal of Experimental Psychology*, 47(4), 714-729.

Biggs, S., & Vidalis, S. (2009). Cloud Computing: The impact on digital forensic investigations. *International Conference for Internet Technology and Secured Transactions* (pp. 1-6). Newport: IEEE Xplore.

Bossler, A., & Holt, T. (2012). Patrol officers' percieved role in responding to cybercrime. *Policing: An International Journal of Police Strategies and Management*, 35(1), 165-181.

Bowers, D., House, A., & Owens, D. (2011). *Getting Started in Health Research.* Oxford: John Wiley & Sons.

Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.

Braga, A. (2008). *Problem-oriented policing and crime prevention.* New York: Criminal Justice Press.

Brams, S. (2008). *Mathematics and Democracy: Designing Better Voting and Fair-Division Procedures.* Princeton: Princeton University Press.

Brand, S., & Price, R. (2000). *The Economic and Social Cost of Crime.* London: Home Office Research Study No. 217.

Brandl, S., & Frank, J.. (1994). The relationship between evidence, detective effort, and the disposition of burglary and robbery investigations. *American Journal of Police*, 13, 149 - 168.

Brannick, T., & Coghlan, D. (2007). In Defense of Being "Native". *Organizational Research Methods*, 10(1), 59-74.

Brannon, L., & Carson, K. (2003). The representativeness heuristic: infleunce on nurses' decision making. *Appolied Nursing Research*, Vol. 16, 201-204.

Bransford, J., & Stein, B. (1984). *The IDEAL problem solver.* New York: W H Freeman.

Bregant, J., & Bregant, R. (2014). Cybercrime and Computer Crime. *The Encyclopedia of Criminology and Criminal Justice*, 1-5.

Brenner, S. (2007). Private-public sector cooperation in combating cybercrime: in search of a model. *Journal of International Law and Technology*, 2.

Brenner, S. (2007). Cybercrim: re-thinking crime control strategies. In Y. Jewkes, *Crime Online* (pp. 12-28). Cullompton: Willan Publishing.

Bringer, J., Johnston, L., & Brackenridge, C. (2004). Maximizing transparency in a doctoral thesis: the complexities of writing about the us of QSR*NVIVO within a grounded theory study. *Qualitative Reseaerch*, Vol. 4(2), 247-265.

British Society of Criminology. (2006, February). *British Society of Criminology Code of Ethics.* Retrieved from British Society of Criminology: http://www.britsoccrim.org/docs/CodeofEthics.pdf

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408-433.

Brookfield, S. (1998). Critically Reflective Practice. *Journal of Continuing Education in the Health Professions*, 197 - 206.

Brown, J. (1996). Police Research: Some critical issues in. In F. Leishman, S. Savage, & B. Loveday, *Coure Issues in Policnig* (pp. 177-190). London: Longman.

Brown, D. (2008). Prosecutors and Overcriminalization: Thoughts on Polictical Dynamics and a Doctrinal Response. *Ohio State Journal of Criminal Law*, 6, 453-466.

Brunty, J., & Helenek, K. (2015). *Social media investigation for law enforcement.* New York: Routledge.

Bryant, R. (2016). *Policing Digital Crime.* Farnham: Routledge.

Bryant, R., & Stephens, P. (2014). Policing Digital Crime: the International and Organisational Context. In R. Bryant, *Policing Digital Crime* (p. 111-121). Farnham: Ashgate Publishing Limited.

Burns, R., Whitworth, K., & Thompson, C. (2004). Accessing law enforcement preparedness to address internet fraud. *Journal of Criminal Justice*, 32(5), 477-493.

Burton, M. (2000). Prosecution decisions in cases of domestic violence involving children. *Journal of Social Welfare and Family Law*, 22(2), 175-191.

Button, M., Frimpong, K., Smith, G., & Johnston, L. (2007). Professionalising counter fraud specialists in the UK: assessing progress and recommendations for reform. *Crime Prevention & Community Safety*, 9(2), 92-101.

Buzawa, E., & Buzawa, C. (2002). *Domestic Violence: the criminal justice response.* Beverly Hills: Sage.

Bynum, T., Cordner, G., & Greene, J. (1982). Victim and Offense Characteristics: Impact on Investigative Decision Making. *Criminology*, 20(3-4), 301-318.

Cabrer, A., & Cabrera, E. (2002). The knowledge sharing dilemna. *Organisational Studies*, 23(5), 687-710.

Cabrera, A., Collins, W., & Salgado, J. (2006). Determinants of individual engagement in knowledge sharing. *The International Journal of Human Resource Management*, 17(2), 245-264.

Camerer, C., Issacharoff, S., Loewenstien, G., O'Donoghue, T., & Rabin, M. (2003). Regulation for Conservatives: Behavioural Economics and the Case for "Asymmetric Paternalism". *University of Pennsylvannia Law Review*, 151, (3), 1211-1254.

Campbell, S. (2007). A cross-cultural comparison of perceptions and uses of mobile telephony. *New Media & Society*, 9(2), 343-363.

Canter, D., & Alison, L. (2003). Converting Evidence into Data; The use of law enforcement archives as unobtrusive measurement. *The Qualitative Report*, 8(2), 72-99.

Carr, J., & Hilton, Z. (2011). Combating child abuse images on the Internet: international perspectives . In J. Davidson, & P. Gottschalk, *Internet Child Abuse: Current Research and Policy* (pp. 52-78). Abingdon: Routledge.

Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. *International Journal of Digital Evidence*, 1(4), 1-12.

Casey, E. (2002). Practical Approaches to Recovering Encrypted Digital Evidence. *International Journal of Digital Evidence*, 1(3), 1-26.

Casey, E. (2004). *Digital Evidence and Computer Crime.* Jordan Hill: Academic Press.

Chakrabarti, S. (2008). A Thinning Blue Line? Police Independence and the Rule of Law. *Policing*, 2(3), 367-374.

Chase, W., & Simon, H. (1973). Perception in Chess. *Cognitive Psychology*, 4(1), 55-81.

Chatterton, M. (2008). *Loosing the Detectives: Views from the Frontline.* Surbition: Police Federation of England & Wales.

Chemerinsky, J. (2009). Counting Offenses. *Duke Law Journal* , 709-746.

Chen, P., & Popovich, P. (2002). *Correlation.* Thousand Oaks: Sage Publcations.

Cheng, J. (2010, October 13). *Govt relies on Facebook 'narcissism' to spot fake marriages, fraud.* Retrieved from Ars Technica: https://arstechnica.com/tech-policy/2010/10/govt-takes-advantage-of-facebook-narcissism-to-check-on-users/

Chibnik, M. (2011). *Anthropology, Economics and Choice.* Austin: University of Texas Press.

Choo, A. (2009). *Evidence.* Oxford: Oxford University Press.

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital Investigation*, 9(2), 81-95.

Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, 37(4), 671-680.

Cole, S. (2005). *Applied transport economics: policy, management & decision making.* London: Kogan Page Publishers.

Coliandris, G. (2015). Book review: Multi-Agency Safeguarding in a Public Protection World: A Handbook for Protecting Children and Vulnerable Adults. *The Police Journal: Theory, Practice and Principles*, 204-208.

Connor, P. (2009). *Blackstones Police Manual: Volume 1 Crime.* Oxford: Oxford University Press.

Cookson, S. (2017). An Important Failure: Lessons from Daedalus and Icarus. In N. Stanton, S. Landry, D. Giuseppe, & A. Vallicelli, *Advances in Human Aspects of Transportation* (pp. 863-872). Walt Disney World: Sprenger International Publishing.

Copi, I., Cohen, C., & Flage, D. (2007). *Essentials of Logice.* Upper Saddle River: Pearson Education.

CPIA. (1996). *Criminal Procedure and Investigations Act.* London: Home Office.

Crown Prosecution Service. (2005, April 4th). Disclosure Manual. *Disclsoure Manual*. London, UK: Crown Prosecution Service.

Crown Prosecution Service. (2017). *About CPS.* Retrieved from Crown Prosecution Service: https://www.cps.gov.uk/

Crow, I., & Semmens, N. (2008). *Researching criminology.* Maidenhead: McGraw-Hill Education.

Crozier, R., & Raynard, R. (1997). Cognitive process models and explanations of decision making. In R. Raynard, R. Crozier, & O. Svenson, *Cognative Models and Explanations* (pp. 5-20). London: Routledge.

Crump, D. (2011). What are the police doing on Twitter? Social Media, the Police and the Public. *Policy & Internet*, 3(4), 1-27.

Cutcliffe, J. (2000). Methodological issues in grounded theory. *Journal of Advanced Nursing*, 31(6), 1476-1484.

Damshenas, M., Dehghantanha, A., Mahmoud, R., & Solahuddin, S. (2012). Forensic investigation challenges in cloud computing environments. *International Conference on Warfare and Digital Forensic (Cybersec)* (pp. 190-194). Putra: IEEE Xplore.

Dane, E., & Pratt, M. (2007). Exploring Intuition and its Role in Managerial

Day, I. (2002). Grounded Theory. In C. Seale, & G. Gobo, *Qualitative Research Practice* (pp. 80-94). London: Sage Publications.

Decision Making. *Academy of Management Review*, 32(1), 33-54.

De Martino, B., Kumuran, D., Seymour, B., & Dolan, R. (2004). Frames, Biases, and Rational Decision-Making in the Human Brain. *Science*, 313(5787), 684-687.

Denef, S., Bayerl, P., & Kaptein, N. (2013). Social media and the police: tweeting practices of british police forces during the August 2011 riots. *CHI '13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3471-3480). New York: ACM.

DeSousa, J. (2013). Self-storage Units and Cloud Computing: Conceptual and Practical Problems with the Stored Communications Act and Its Bar on ISP Disclosures to Private Litigants. *Georgetown Law Journal*, 102, 247-270.

Devlin, K. (1970). *Sentencing Offenders in Magistrates' Courts.* London: Sweet and Maxwell.

Dewey, J. (1933). *How we think: A restatement of the relation of reflective thinking to the educative process.* Chicago: Henry Regnery Co.

Dijck, J. (2013). *The culture of connectivity. A critical history of social media.* Oxford: Oxford University Press.

Dolman, E. (2005). *Pure Strategy.* London: Frank Cass.

Dorfman, J. (1997). *Bayesian economics through numerical methods: a guide to econometrics and decision-making with prior information.* New York: Springer Science & Business Media.

Drake, P., & Heath, L. (2011). *Practitioner Research at Doctoral Level: Developing Coherent Research Methodologies (1).* Abingdon: Routledge.

Duggan, M., Ellison, N., Lampe, C., Lenhart, A., & Madden, M. (2015, January 9). *Social Media Update 2014.* Retrieved from Pew Research Internet Projcect: http://www.foothillspresbytery.org/wp-content/uploads/sites/175/2015/07/Social-Media-Site-Usage-2014-_-Pew-Research-Centers-Internet-American-Life-Project.pdf

Duncan, J., & Owen, A. (2000). Common regions of the human frontal lobe recruited by diverse cognitive demands. *Trends in Neurosciences*, 23(10), 475-483.

Eck, J. (1983). *Solving Crimes: The investigation of Burglary and Robbery.* Washington DC: Police Executive Research Forum.

Eck, J., & Spelman, W. (2005). Who ya gonna call? The police as problem-buster. In T. Newburn, *Policing Key Readings* (pp. 412-427). Cullompton: Willan Publishing.

Edosomwan, S., Prakasan, S., Kouame, D., Watson, J., & Seymour, T. (2011). The History of Social Media and its Impact on Business. *The Journal of Applied Management and Entrepreneurship*, 16(3), 79-91.

Edwards, L., & Urquhart, L. (2016). Privacy in public spaces: what expectations of privacy do we have in social media intelligence. *International Journal of Law and Information Technology*, 24, (3), 279-310.

Einhorn, J., & Hogarth, R. M. (1981). Behavioural Decision Theory: Processes of Judgement and ChoicE. *Annual Review of Psychology*, 53-88.

Elio, R. (2002). *Common sense, reasoning, & rationality.* Oxford: Oxford University Press.

ESRC. (2012, September). *ESRC Frameword for Research Ethics.* Retrieved from ESRC: https://esrc.ukri.org/files/funding/guidance-for-applicants/esrc-framework-for-research-ethics-2010/

Etzioni, A. (2016). Apple: Good Business, Poor Citizen? . *Journal of Business Ethics*, 1-11.

Eraut, M. (1994). *Developing professional knowledge and competence.* Abingdon: Routledge

Feist, A., Ashe, J., Lawrence, J., McPhee, D., & Wilson, R. (2007). *Investigating and detecting recorded offences of rape.* London: Home Office Research Development and Statistics Directorate.

Findley, K., & Scott, M. (2006). The multiple dimensions of tunnel vision in criminal cases. *Wisconsin Law Review*, p.291-297.

Fitzpatrick, B., & Taylor, N. (2001). Human Rights and the Discretionary Exclusion of Evidence. *Journal of Criminal Law*, 65(4), 349-359.

Flanagan, R. (2008). *Independent Review of Policing: Final Report.* London: Home Office

Fleming, M., Greentree, S., Cocotti-Muller, D., Elias, K., & Morrison, S. (2006). Safety in cyberspace: Adoloscents safety and exposure online. *Youth & Society*, 38, (2), p.135-154.

Fontana, A., & Prokos, A. (2007). *The Interview: from Formal to Postmodern.* Walnut Creek: Left Coast Press.

Frauenknecht, M., & Black, D. (2010). Is it social problem solving or decision making? Implications for health education. *American Journal of Health Education*, 41(2), 112-123.

Fried, Y., & Slowik, L. (2004). Enriching Goal-Setting Theory wtih Time: An Integrated Approach. *The Academy of Management Review*, 29, (3), 404-422.

Gabbay, J., & Le May, A. (2004). Evidence based guidelines or collectively constructed 'mindlines?' Ethnographic study of knoweldge managemetn in primary care. *British Medical Journal*, 329.

Gadd, D., Karstedt, S., & Messner, S. F. (2011). *Criminological Research Methdos.* London: Sage Publications Ltd

Gagnier, C. (2011). On Privacy: Liberty in the Digital Revolution. *Journal of High Techonology*, 11, 229-279.

Garb, H. (1996). The representativeness and past-behaviour heuristics in clinical judgment. *Professional Psychology: Research and Practice*, 27(3), 272-277.

Garfinkel, S. (2012). Digital forensics research: The next 10 years. *Digital Investigation*, Vol. 7, p.64-73.

Geach, N., & Haralambous, N. (2009). Regulating Harassment: Is the Law Fit for the Social Networking Age? *Journal of Criminal Law*, 73(3), 241-257.

Geddes, M., & Pooneh, Z. (2016). Forensic analysis of private browsing. *International Conference On Cyber Security and Protection of Digital Services* (pp. 1-2). Leicester: IEEE Xplore.

Getzels, J. (1982). The problem of the problem. In R. Hogarth, *Question framing and reponse consistency* (pp. 37-50). San Fransisco: Jossey-Bass.

Gibbs, G. (1988). *Learning by Doing: A Guide to Teaching and Learning Methods.* London: Further Education Unit

Gideon, K. (1996). Behavioral Decision Making: Some Critical Notes. *Organization behaviour and human decision processes*, pp.169-178.

Gigerenzer, G. (2008). *Rationality for mortals: How people cope wih uncertainty.* Oxford: Oxford University Press.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic Decision Making. *Annual Review of Psychology*, 62, 451-482.

Gigerenzer, G., & Todd, P. (1999). *Simple heuristics that make us smart.* Oxford: Oxford University Press.

Gilespie, A. (2015). *Cybercrime.* Florence, US: Routledge.

Gillespie, A. (2002). Child protection on the internet - challenges for criminal law . *Child and Family Law Quarterly*, 411-426.

Gillham, B. (2005). *Research Interviewing: The range of techniques.* Maidenhead: McGraw-Hill Education.

Gilovich, T., & Griffin, D. (2002). Heuristics and biases: Then and now. In T. Gilovich, D. Griffin, & Kahneman, *Heuristics and biases: The psychology of intuitive judgement* (pp. 1-18). Cambridge: Cambridge University Press.

Glaser, B. (1978). *Theoretical Sensitivity. Advances in the Methodology of Grounded Theory.* Mill Valley: The Sociology Press.

Glaser, B. (1992). *Basics of Grounded Theory Analysis: Emergence vs. Forcing.* Mill Valley: Sociology Press.

Glaser, B., & Strauss, A. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Chicago: Aldine.

Glaser, R. (1999). Expert Knowledge and Processes of Thinking. In R. McCormick, & C. Paechter, *Learning and Knowledge* (pp. 88-102). London: Sage Publications Ltd.

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, 8(4), 597-606.

Goldsmith, A. (2015). Disgracebook policing: social media and the rise of police indiscretion. *Policing and Society*, 25(3), 249-267.

Goodman, M. (1996). Why the police don't care about computer crime. *Harvard JL & Tech*, 10, 465.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, 2(1), 13-20.

Goulding, C. (2002). *Grounded Theory.* London: Sage.

Gozna, L., & Horvath, M. (2009). Investigative Interviewing. In S. Tong, R. Bryant, & M. Horvath, *Wiley Series in Psychology of Crime, Policing and Law : Understanding Criminal Investigation* (pp. 115-134). Singapore: Wiley.

Gray, C., & Williamson, M. (2002). *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History.* London: Taylor & Francis.

Green, N., & Haddon, L. (2009). *Mobile communications: An introduction to new media.* Oxford: Berg.

Greenberg, A. (2016, May 17). *Senate draft encryption bill privacy nightmare.* Retrieved from wired.com: https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare

Greenwood, P. (1970). *An analysis of the Apprehension Activities of the New York Police Department.* New York: Rand.

Greenwood, P., Chaiken, J., & Petersilia, J. (1976). Response to: An Evalution of the Rand Corporation's Analysis of the Criminal Investigation Process. *Police Chief*, 62-71.

Griffith, G., & Roth, L. (2007). *Protecting children from online sexual predators.* Sydney: NSW Parliamentary Library Research Service.

Groeneveld, R. (2005). *Arrest Discretion of Police Officers : The Impact of Varying Organizational Structures.* New York: LFB Scholarly Publishing LLC.

Gross, G. (2016). *The Myth and Reality of German Warfare.* Kentucky: University Press of Kentucky

HAC. (2013). *Home Affairs Select Committee E-crime.* London: Home Office.

Hannibal, M., & Mountford, L. (2015). *Criminal Litigation.* Oxford: Oxford University Press.

Harte, J., & Koele, P. (1997). Psychometric and methodological aspects of process tracing research. In R. Ranyard, W. Ray, & O. Svenson, *Decision Making: Cognative Models and Explanations.* London: Routledge.

Herring, J. (2014). *Criminal Law: Text, Cases, and Materials.* Oxford: Oxford University Press.

Hester, M., & Lilley, S.-J. (2015). *More than Support to Court ISVAs in Bristol.* Bristol: University of Bristol in association iwth the Northern Rock Foundation.

Hickson, L., & Khemka, I. (2013). Problem Solving and Decision Making. In M. Wehmeyer, *The Oxford Handbook of Positive Psychology and Disability* (pp. 198-227). Oxford: Oxford University Press.

Higham, P., & Vokey, R. (2000). Judgment heuristics and recognition memory: Prime identification and target-processing fluency. *Memory & Cognition*, 28(4), 574-584.

Hill, J. (2002, July). High-speed police pursuits: Dangers, dynamics, and risk reduction. *FBI Law Enforcement Bulletin*, 71, 14-18.

Hinduja, S., & Patchin, J. (2013). Social Influences on Cyberbullying Behaviours Among Middle and High School Students. *Journal of Youth and Adolescence*, 42(5), 711-722.

HM Government. (2010). *Working together to safeguarhd children: a guide to inter-agency working to safeguard and promote the welfare of children.* Nottingham: DCSF.

HMIC. (2012). *The Crime Scene: a review of police crime and incident reports.* London: Her Majesty's Inspectorate of Constabulary.

HMIC. (2015). *Reshaping Policing for the Public.* London: HMIC.

HMIC. (2017). *www.gov.uk/government/organisations.* Retrieved from HM Inspectorate of Constabulary:
https://www.gov.uk/government/organisations/hm-inspectorate-of-constabulary

HMICFRS. (2018, March 26). *Crime Data Integrity Inspections Avon and Somersent.* Retrieved from HMICFRS Peel Assessment: https://www.justiceinspectorates.gov.uk/hmicfrs/crime-data-integrity-inspections-explanatory-notes/#auditable-route

HMICFRS. (2018, March 26). *HMICFRS.* Retrieved from Peel Assessment Avon and Somerset Constabulary: https://www.justiceinspectorates.gov.uk/hmicfrs/peel-assessments/peel-2017/avon-and-somerset/?#

HMICFRS. (2018, March 22). *Thames Valley Police.* Retrieved from Justice Inspectorates Police Forces: https://www.justiceinspectorates.gov.uk/hmicfrs/police-forces/thames-valley/

Hodge, M. (2006). The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com . *Southern Illinois University Law Journal*, 31, 95-122.

Hoffman, E. (1980). Goals and Objectives for the Eighties. *Music Educators Journal*, 67(4), 48, 49, 66.

Hogan, B., & Quan-Haase, A. (2010). Persistence and Change in Social Media. *Bulletin of Science, Technology and Society*, 30(5), 309-315.

Holt, T., & Bossler, A. (2012). Predictors of Patrol Officer Interest n Cybercrime Training and Investigation in Selected United States Police Departments. *Cyberpsychology, Behaviour, and Social Networking*, 15(9), 464-472.

Holt, T., Belvins, K., & Burkert, N. (2010). Considering the paedophile subculture on-line. *Sexual Abuse: Journal of Research and Treatment*, 22(1), 3-24.

Holton, J. (2007). The Coding Process and Its Challenges. In A. Bryant, & K. Charmaz, *The SAGE Handbook of Grounded Theory* (pp. 265-289). Sage: London.

Home Affairs Committe. (2013). *E - Crime.* London: House of Commons.

Home Office. (1988, July 29). *legislation.gov.uk.* Retrieved July 08, 2016, from The National Archives: http://www.legislation.gov.uk/ukpga/1988/27/contents

Home Office. (1994, November 3). *legislation.gov.uk.* Retrieved July 08, 2016, from The National Archives: http://www.legislation.gov.uk/ukpga/1994/33/introduction

Home Office. (1997, March 21). *legislation.gov.uk.* Retrieved July 08, 2016, from The National Archives: http://www.legislation.gov.uk/ukpga/1997/40/introduction

Home Office. (2014, April). *Vision and Purpose Statements for Crime Recording.* Retrieved from www.gov.uk/government/uploads: https://www.gov.uk/government/uploads/system/uploads/attachment_data/fil e/387762/count-vision-december-2014.pdf

Home Office. (2014, July). *Multi Agency Working and Information Sharing Project: Final Report.* Retrieved from www.gov.uk: https://www.gov.uk/government/uploads/system/uploads/attachment_data/fil e/338875/MASH.pdf

Home Office. (2015, July 16). *National Statistics Police Work Force England and Wales 31 March 2015.* Retrieved from www.gov.uk: https://www.gov.uk/government/statistics/police-workforce-england-and-wales-31-march-2015-data-tables

Home Office. (2016, April 11). *Counting Rules General Rules.* Retrieved from gov.uk: https://www.gov.uk/government/uploads/system/uploads/attachment_data/fil e/513279/count-general-april-2016.pdf

Home Office. (2018, January 25). *Police Work Force, England and Wales March 2017: open data tables.* Retrieved from Government statistics police work force: https://www.gov.uk/government/statistics/police-workforce-open-data-tables

Home Office. (2018, April 11). *Home Office Counting Rules for Recorded Crime.* Retrieved from gov.uk publications:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694432/count-general-apr-2018.pdf

Horn, R. (1996). Negotiating research access to organisations. *The Psychologist*, 9(12), 551-554.

Horvath, M. A., & Brown, J. (2006). Using Police Data for Empirical Investigations of Rape. *Issues in Forensic Psychology*, 6, 49-56.

Hough, M., & Mayhew, P. (1983). *British Crime Survey - First Report.* London: Home Office Research and Planning Unit.

Hsiaw, A. (2010, June). *Essays on the economics of self-control and lifestyle brands.* Retrieved from Princeton University, ProQuest Dissertations Publishing:
https://search.proquest.com/openview/28d5d3f95852139d69ddef227a6fd87c/1?pq-origsite=gscholar&cbl=18750&diss=y

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), 528-535.

Hurlbert, R., & Heavey, C. (2001). Telling what we know: Descrbing inner experience. *Trends in Cognative Science*, 5(9), 400-403.

Hutchinson, S. (1993). Grounded theory: The Method. In P. Munhall, & C. Boyd, *Nursing Research: A Qualitative Perspective* (pp. 180-212). New York: National League for Nursing Press.

Innes, M. (2003). *Investigating Homocide: detective work and the police response to criminal homocide.* Oxford: Oxford University Press.

Isaacs, H. (1967). *Police Operations: The Apprehension Process.* Washington DC: United States Government Printing Office.

Izzo, M., Pritz, S., & Ott, P. (1990). Teaching problem-solving skills: A ticket to a brighter future. *The Journal for Vocational Special Needs Education*, 13, 23-26.

Jarzabkowski, P. (2005). *Strategy as practice.* London: Sage Publications.

Jewkes, Y. (2013). Public Policing and Internet Crime. In Y. Jewkes, & M. Yar, *Handbook of Internet Crime* (pp. 525-545). Cullompton: Willan Publishing.

Jewkes, Y., & Andrews, C. (2005). Policing the filth: The problems of investigating online child pornography in England and Wales. *Policing and Society*, 15(1), 42-62.

Jewkes, Y., & Andrews, C. (2007). Internet child pornography: internation repsonses. In Y. Jewkes, *Crime Online* (pp. 60-80). Cullompton: Willan Publishing.

Jewkes, Y., & Yar, M. (2008). Polcing cybercrime: emerging trends and future challenges. In T. Newburn, *Handbook of Policing* (pp. 580 - 606). Wilan Publishing.

Johns, C. (1995). Framing learning through reflection within Carper's fundamental ways of knowing in nursing. *Journal of advanced nursing*, 226 - 234.

Johnson, S. (1997). Will our research hold up under scrutiny? *Journal of Industrial Teacher Education*, 32(3), 3-6.

Jones, T. (2004). *Business economics and managerial decision making.* Chichester: John Wiley & Sons.

Jones, D., Grieve, J., & Milne, B. (2008). The Case to Review Murder Invesetigations. *Policing*, 2(4), 470-480.

Jordan, J. (2001). Worlds Apart? Women, Rape and the Police Reporting Process. *British Journal of Criminology*, 41(4), 679-706.

Jupp, V. (1989). *Methods of criminological research.* London: Unwin Hyman.

Kao, D., & Wang, S. (2009). The IP address and time in cyber-crime investigation. *Policing: an international Journal of Police strategies & Management*, 32(2),194-208.

Kaplan, A., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Science Direct*, 53(1), 59-68.

Kardasz, F. (2012). Sex Offenders on the Internet: Cyber-Struggles for the Protection of Children. In M. DeLisis, & P. Conis, *Violent Offenders* (pp. 301-318). Burlington: Jones & Barlett Learning.

Keane, M., & Eysenck, M. (2010). *Cognitive Psychology: A student's handbook.* Hove: Psychology Press.

Kebbell, M. R., Muller, D. A., & Martin, K. (2010). Understanding and managing bias. *Dealing with uncertainties in policing serious crime*, *16*(1), 87.

Kelle, U. (2007). The Development of Categories: Different Approaches in Grounded Theory. In A. Bryant, & K. Charmaz, *The SAGE Handbook of Grounded Theory* (pp. 191-213). London: Sage Publishing.

Kennedy, T., & Lingard, L. (2006). Making sense of grounded theory in medical education. *Medical Education*, 40(2), 101-108.

Kerrigan, S. (2011, February 18). *US Gov. Software Creates 'Fake People' on Social Networks.* Retrieved from Examiner: www.examiner.com/social-media-in-national/us-gov-software-creates-fake-people-on-social-networks-to-promote-propaganda

Kietzmann, J., Hermkens, K., McCarthy, I., & Silvestre, B. (2011). Social media? Get Serious! Understanding the functional building blocks of social media. *Business Horizons*, 54(3), 241-251.

Kim, W., Jeong, O., & Lee, S. (2010). On Social Web Sites. *Information Systems*, 35(2), 215-236.

Kingstone, A., Smilek, D., & Eastwood, J. (2008). Cognative Ethology. *British Journal of Psychology*, 99(3), 317-340.

Kirk, J., & Miller, M. (1986). *Reliability and validity in qualitative research.* Beverly Hills: Sage Publications.

Klayman, J. (1995). Varieties of Confirmation Bias. *Psychology of Learning and Motivation*, 32, 385-418.

Klein, G. (1999). *Sources of power: How people make decsions.* Cambridge, MA: MIT Press.

Knoops, G. (2013). *Redressing Miscarriages of Justice.* Leiden: Martinus Nijhoff Publishers.

Kokkinos, C. M., Baltzidis, E., & Xynogala, D. (2016). Prevalence and personality correlates of Facebook bullying among university undergraduates. *Computers in Human Behavior*, *55*, 840-850.

Koksalan, M., Wallenius, J., & Zionts, S. (2011). *Multiple Criteria Decision Making: from early history to the 21st century.* Singapore: World Scientific.

Kolb, D. A. (1984). *Experimental Learning: Experience as the source of Learning and Development.* Englewood Cliffs: Prentice Hall.

Kothari, C. R. (2004). *Research Methodology; Methods and Techniques.* New Dehli: New Age International.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM - Finding the Fun in Computer Science Educatioon*, 52(12), 141-144.

Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in Human Behavior*, *29*(1), 16-25.

Lamb, H., Weinberger, L., & DeCuir Jr, W. (2002). The Police and Mental Health. *Psychiatric Services*, 53(10), 1266-1271.

Laming. (2009). *The Protection of Children in England: A progress report.* London: HMSO.

Langville, A., & Meyer, C. (2012). *Who's #1? The Science of Rating and Ranking.* Princeton: Princeton University Press.

Latham, G., & Yukl, G. (1975). A review of Research on the Application of Goal Setting in Organisations. *Academy of management*, 824-845.

Lees, S., & Gregory, J. (1993). *Rape and Sexual Assault: A study of Attrition: Multi-agency Investigation into the Problem of Rape and Sexual Assault in the London Borough of Islington.* London: Islington Council.

Leighton, J., & Sternberg, R. (2013). Reasoning and Problem Solving. In A. Healy, & R. Proctor, *Handbook of Psychology: Volume 4 Experimental Psychology.* Hoboken: Wiley.

Lenhard, A., Purcell, K., Smith, A., & Zickuhr, K. (2010, February 3). *Social Media & Mobile Internet Use Among Teens and Young Adults.* Retrieved from Pew Internet: Pew Internet & American Life Project: http://files.eric.ed.gov/fulltext/ED525056.pdf

Lempert, L. (2007). Asking Questions of the Data: Memo Writing in the Grounded Theory Tradition. In A. Bryant, & K. Charmaz, *The SAGE Handbook of Grounded Theory* (pp. 245-264). London: Sage.

Lesgold, A., Rubinson, H., Feltovich, P., Glaser, R., Klopfer, D., & Wang, Y. (1988). Expertise in a complex skill: Diagnosing x ray pictures. In M. Chi, R. Glaser, & M. Farr, *The nature of expertise* (pp. 311-432). Hillsdale: Lawrence Erlbaum Associates.

Levitt, S. (1998). The relationship between crime reporting and police: implications for the use of uniform crime reports. *Journal of Quantative Criminology*, 14(1), 61-81.

Liebetrau, A. (2018). *Measures of Association.* Thousand Oaks: Sage Publications.

Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry.* Beverly Hills: Sage.

Lindvall, C. (1964). *Introduction in defining educational objectives.* Pittsburgh: A report of the Regional Commission on Educational Coordination and the Learning Reasch and Development Center. University of Pittsburgh Press.

Lock, R., Cooke, L., & Jackson, T. (2013). Online social networking, order and disorder. *The Electronic Journal of e-Government*, 11(1), 229-240

Locke, E., & Latham, G. (2013). Introduction. In E. L. Locke, *New Developments in Goal Setting and Task Performance* (pp. 3-15). London: Routledge.

London Borough of Merton. (2014, 04 01). London Multi Agency Safeguarding Hubs (MASH) Governance. London.

Loveday, B. (2006). Basic Command Units (BCUs) and local authorities: Future mechanisms of police accountability and service delivery. *International Journal of Police Science & Management*, 9(4), 324-335.

Lutz, A., & Thompson, E. (2003). Neurophenomenology: Integrating subjective experience and brain dynamics in the neuorscience of consciousness. *Journal of Consciousness Studies*, 10(9-10), 31-51.

Lyle, J. R. (2003). NIST CFTT: Testing Disk Imagine Tools. *International Journal of Digital Evidence*, 1(4), 1-10.

Lynch, J. (2001). *Surveillance Society: Monitoring Everyday Life.* Buckingham: Open University Press.

MacDonald, Z. (2002). Official cime statistics: their use and inerpretation. *The Economic Journal*, 112, 85-106.

Madoc-Jones, I., Hughes, C., & Humphries, K. (2015). Where next for victim services in England and Wales. *The Journal of Adult Protection*, 17(4), 245-257.

Maguire, M. (2003). Criminal Investigation and Crime Control. In T. Newburn, *Handbook of policing* (pp. 430-464). Cullompton: Willan Publishing.

Mahmood, S. (2012, November). Online social networks: The overt and covert communication channels for terrorists and beyond. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for* (pp. 574-579). IEEE.

Manzhai, O. (2012). Procedure Analysis of the Special Investigative Actions Through Cyberspace in Countries of Common and Continental Law. *Internal Security*, 4(1), 141-152.

Marcum, C., Higgins, G., Freiburger, T., & Ricketts, M. (2010). Policing possession of child pornography online: investigating the training and resources dedicated to the investigation of cybercrime. *International Journal of Police Science & Management*, 12(4), 516-525.

Mari, D., & Kotz, S. (2001). *Correlation and Dependence.* London: Imperial College Press.

Mason, J. (2002). Qualitative interviewing: asking, listening and interpreting. In T. May, *Qualitative research in action.* London: Sage.

Mason, S., & George, E. (2011). Digital evidence and 'cloud' computing. *Computer Law & Security Review*, 27(5), 524-528.

May, T. (2011). *Social Research.* Maidenhead: McGraw-Hill Education.

Maxfield, M., Lewis, D., & Szoc, R. (1980). Producing official crimes: verified crime reports as measures of police output. *Science Quarterly*, 61(12), 221-236.

McGhee, G., Marland, G., & Atkinson, J. (2007). Grounded theory research: literature reviewing and reflexivity. *Journal of Advanced Nursing*, 60(3), 334-342.

McMillan, L., & Thomas, M. (2013). Police interviews of rape victims: tensions and contradictions. In M. Horvath, & J. Brown, *Rape: Challenging Contemporary Thinking* (pp. 255-280). Cullumpton: Willan.

Metcalfe, C. (2007). Policing operation ore. *Criminal Justice Matters*, 8-9.

Meyers, M., & Rogers, M. (2005). Digital forensics: Meeting the challenges of scientific evidence. *IFIP International Conference on Digital Forensics* (pp. 43-50). Boston: Springer.

Miles, M., & Huberman, M. (1994). *Qualitative Data Analysis: An expanded Sourcebook.* Thousand Oaks: Sage Publications.

Miller, G. G., & Pribram, K. (1960). *Plans and the structure of behaviour.* London: Holt, Rinehart & Winston.

Mills, J., Platts, K., Bourne, M., & Richards, H. (2002). *Strategy and Performance: Competing through competencies.* Cambridge: Cambridge University Press

Milne, R., Poyser, S., Williamson, T., & Savage, S. (2010). Miscarraiges of Justice. What can we learn? . In J. Adler, & J. Gray, *Forensic Psychology: Concepts, Debates and Practice* (pp. 17-37). Abingdon: Willan Publishing.

Ministry of Justice. (2013). *Victims' Services Commissioning Framework.* London: Ministry of Justice.

Ministry of Justice. (2016, Jan 18). *Open Justice Making Sense of Justice.* Retrieved from gov.uk: http://open.justice.gov.uk/courts/criminal-cases/

Mocas, S. (2004). Building theoretical underpinnings for digital foresnic research. *Digital Investigation*, 1(1), p.61-68.

Moissidis, C. (2008). *Criminal Discovery: From Truth to Proof and Back Again.* Sydney: Institute of Criminology Press.

Moore, R. (2010). *Cybercrime.* London: Routledge.

Moore, R. (2016). *Cybercrime.* Cincinnati: Routledge.

Moriarty, D. (2015). *Practical Human Factors for Pilots.* Kidlington: Elsevier Science. Mruck, K., & Mey, G. (2007). Grounded Theory and reflexivity. In A. Bryant, & K. Charmaz, *The Sage handbook of grounded theory* (pp. .515-538). London: Sage.

Morse, J. M. (2001). Situating Grounded Theory within Qualitative Enquiry. In R. S. Schreiber, & P. S. Stern, *Using Grounded Theory in Nursing* (pp. 1-16). New York: Springer Publishing Company.

Murphy, P. (2007). *Murphy on Evidence.* Oxford: Oxford University Press.

National College of Policing. (2014, January 28th). *Managing investigations.* Retrieved from www.app.college.police.uk: http://www.app.college.police.uk/app-content/investigations/managing-investigations/

National College of Policing. (15, December 2014). *National Decision Model.* Retrieved from College of Policing: https://www.app.college.police.uk/app-content/national-decision-model/

National College of Policing. (2015, May 26). *Major investigation and public protection: Staffing and the child abuse investigation unit.* Retrieved from College of Policing: https://www.app.college.police.uk/app-content/major-investigation-and-public-protection/child-abuse/police-response/staffing/

National College of Policing. (2016, February 19). *The role of domestic abuse specialists.* Retrieved from College of Policing: Major Investigation and public protection: https://www.app.college.police.uk/app-content/major-investigation-and-public-protection/domestic-abuse/investigative-development/the-role-of-domestic-abuse-specialists/

National College of Policing. (2017). *About us.* Retrieved from College of Policing: http://www.college.police.uk/About/Pages/default.aspx

National College of Policing. (2017). *Investigation.* Retrieved from College of Policing: Professional Training: http://www.college.police.uk/What-we-do/Learning/Professional-Training/Investigation/Pages/Investigation.aspx

National College of Policing. (2018, March 20). *Investigation: Managing Investigations.* Retrieved from College of Policing Authorised Professional Practice: https://www.app.college.police.uk/app-content/investigations/managing-investigations/#investigative-strategies

Thames Valley Police. (2017, May 3). *Crime Statistics for Thames Valley Police 2016/17.* Retrieved from Thames Valley Police, General News: https://www.thamesvalley.police.uk/news/general/crime-statistics-thames-valley-police-201617/

Thames Valley Police. (2018, March 22). *About the force.* Retrieved from Thames Valley Police: https://www.police.uk/thames-valley/

Newburn, T. (2007). *Handbook of Criminal Investigation.* Abingdon: Willan Publishing.

Newman, G., & Clarke, R. (2003). *Superhighway Robbery: Preventing E-commerce Crime.* Cullompton: Willan Publishing.

Nickerson, R. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2), 175-220.

Nicol, C., Innes, M., Gee, D., & Feist, A. (2004). *Using progress reviews to improve investigative performance.* London: Home Office.

Nisbett, R., & Wilson, T. (1977). Telling more than we can know: Verbal reports on mental processes. *Psychological Review*, 84(3), 231-259.

Nowacki, J., & Willts, D. (2016). The use of specialised cybercrime policing units: an organizational analysis. *Criminal Justice Studies*, 29(2), 105-124.

NPIA. (2012). *Officer Safety Module.* Retrieved from NPCC Documents: http://www.npcc.police.uk/documents/FoI%20publication/Disclosure%20Log

s/Uniformed%20Operations%20FOI/2013/003%2013%20Att%2002%20of%2015%20Police%20Officer%20Safety%20Manual%20Module%202.pdf

O'Ciardhuain, S. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, 3(1), p.1-22.

O'Keefe, G., & Clarke-Pearson, K. (2011). The Impact of Social Media on Children, Adoloscents, and Families. *Pediatrics*, 127(4), 800-804.

O'Keeffe, S., Brown, J., & Lyons, E. (2013). Seeking proof or truth: naturalistic decision-making by police officers when considering rape allegations. In M. Horvath, & J. Brown, *Rape: Challenging Contemporary Thinking* (pp. 229-254). Cullompton: Willan.

Oksman, V., & Rautiainen, P. (2003). Perhaps It is a Body Part: How the Mobile Phone Became an Organic Part of the Everyday Lives of Finnish Children and Teenagers. In J. Katz, *Machines that become us* (pp. 293-308). London: Transaction Publishers.

O'Neal, C. (2012). *Data-Driven Decision Making.* London: International Society for Technology in Education.

Orasanu, J., Martin, L., & Davison, J. (2001). Cognitive and Contextual Factors in Aviation Accidents. In E. Salas, & G. Klein, *Linking Expertise and Naturalistic Decision Making* (pp. 209-226). Hove: Psychology Press.

Oswal, M., & Grosjean, S. (2004). Confirmation Bias. In R. Pohl, *Cognative Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory* (pp. 79-96). Hove: Psychology Press.

Owusu-Bempah, A. (2015). Prosecuting hate crime: procedural issues and the future of the aggravated offences. *Legal Studies: The Journal of the Society of Legal Scholars*, 35(3), 443-462.

Parker, N. (2013). *Independent review of ACPO.* Retrieved from Association of Police and Crime Commissioners: http://apccs.police.uk/wp-content/uploads/2013/08/Independent-review-of-ACPO.pdf

Patton, M. (2002). *Qualitative evaluation and research methods.* Thousand Oaks:

Sage Publications.

Percy, K. (1973). Aims and Objectives of Staff. *Higher Education*, 2(2), 252-253.

Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, 9,(8), 38-44.

Petrashek, N. (2010). The Fouth Amendment and the Brave New World of Online Social Networking. *Marquette Law Review*, 93, 1495-1532.

Pilavin, I., & Briar, S. (1964). Police encounters with juveniles. *American Journal of Sociology*, 70(2), 206-214.

Police Federation of England and Wales. (2015, 23 October). *Police Federation*. Retrieved from Final Report on PFEW National Detectives Survey: http://www.policemag.co.uk/images/Final_Report_on_PFEWs_National_Detectives_Survey_2015.pdf

Pretz, J., Naples, A., & Sternberg, R. (2003). Recognising, defining and representing problems. In J. Davidson, & R. Sternberg, *The Psychology of Problem Solving* (pp. 3-33). Cambridge: Cambridge University Press.

Qi, M., & Edgar-Nevill, D. (2011). Social networking searching and privacy issues. *Information Security Technical Report*, 16(2), 74-78.

Quan-Haase, A. (2008). University students' local and distant social ties: Using and integrating modes of communication on campus. *Information, Communication & Society*, 10(5), 671-693.

Rassin, E. (2010). Blindness to alternative scenarios in evidence evaluation. *Journal of Investigative Psychology and Offender Profiling*, 7(2), 153-163.

Rassin, E., Eerland, A., & Kuijpers, I. (2010). Let's find the evidence: an analogue study of confirmation bias in criminal investigations. *Journal of Investigative Psychology and Offender Profiling*, 7(3), 231-246.

Reichertz, J. (2007). Abduction: The Logic of Discovery of Grounded Theory. In A. Bryant, & K. Charmaz, *The SAGE Handbook of Grounded Theory* (pp. 214-228). London: SAGE.

Reiner, R., & Newburn, T. (2007). Police Research. In R. King, & E. Wincup, *Doing Research on Crime and Justice.* Oxford: Oxford University Press.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1-12.

Richards, L., Letchford, S., & Stratton, S. (2008). *Policing domestic violence.* Oxford : Oxford University Press.

Richardson-Foster, H., Stanley, N., Miller, P., & Thomson, G. (2011). Policing intervention in domestic violence incidents where children are present: police and children's perspectives. *Policing and Society*, 22(2), 220-234.

RIPA. (2000, July 28). *Regulation of Investigatory Powers Act.* Retrieved from The National Archives: http://www.legislation.gov.uk/ukpga/2000/23/contents

Rivett, M., & Kelly, S. (2006). From awareness to practice: children, domestic violence and child welfare. *Child Abuse Review*, 15(4), 224-242.

Roberts, P., & Zuckerman, A. (2010). *Criminal Evidence.* Oxford: Oxford University Press.

Rose, C. (2011). The security implications of ubiquitous social media. *International Journal of Management and Information Systems*, *15*(1), 35.

Rosen, C. (2004). Our Cell Phones, Ourselves. *The New Atlantis*, (6), 26-45.

Rossmo, K. (2009). *Criminal Investigative Failures.* Boca Raton: Taylor and Francis .

Rowley, I. (2010). Knowledge Management in UK police forces. *Journal of Knowledge Management*, 14(4), 611-626.

Ryan, D., & Spantzer, G. (2002, September). *Legal aspects of digital forensics.* Retrieved from euro.ecom.cmu.edu/program/law: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf

Said, H. A., Al Awadhi, I., & Guimareas, M. (2011). Forensic Analysis of Private Browsing Artifacts. *7th International Conference on Innovations in Information Technology* (pp. 197-202). Abu Dhabi: IEEE Xplore.

Sanders, A., & Young, R. (2012). Police Powers. In T. Newburn, *Handbook of Policing* (pp. 281-312). Cullompton: Willan Publishing.

Savirimuthu, J. (2012). *Online child safety: law, technology and governance.* Basingstoke: Palgrave MacMillan.

Saylor, J., & Alexander, W. (1974). *Planning curriculum for schools.* New York: Holt, Rinehart & Winston.

Schell, B., Martin, M. H., & Rueda, L. (2007). Cyber child pornography: A review paper of the social and legal issues and remedies-and a proposed technological solution. *Aggression and violent behaviour*, 12(1), 45-63.

Schon, D. A. (1983). *The reflective practitioner: How professionals think in action.* London: Temple Smith.

Schneider, C. (2016). *Policing and Social Media: Social Control in an Era of New Media.* London: Lexington Books.

Policing (pp. 281-312). Cullompton: Willan Publishing.

Schreiber, R. S. (2001). The "How To" of grounded theory: Avoiding the pitfalls. In R. S. Schreiber, & P. N. Stern, *Using grounded theory in nursing* (pp. 56-84). New York: Springer Publishing Company.

Schuster, D., & Powers, W. (2005). *Translational and Experimental Clinical Research.* Philadelphia: Lippincott Williams & Wilkins.

Sharma, S. (2017). *Nursing Research and Statistics.* New Delhi: Elsevier Health Sciences

Shea, M. (1974). A study of the effect of the prosecutor's choice of charge on magistrates' sentencing behaviour. *British Journal of Criminology*, 14, 269-272.

Sherlock, L., & Cambridge, P. (2009). Working effectively with the police in safeguarding vulnerable adults: sharing experience from Somersent. *The Journal of Adult Protection*, 11(4), 6-19.

Shevlyakov, G., & Oja, H. (2016). *Robust Correlation: Theory and Applications.* Chichester: Wiley.

Shields, S. (2008). An evaluation of police complaince with domestic violence documentation. *Best Practices in Mental Health*, 4(1), 65-73.

Shogren, K., Wehmeyer, M., Palmer, S., Soukup, J., Little, T., Garner, N., & Lawrence, M. (2008). Understanding the Construct of Self-Determination. *Assessment for Effective Intervention*, 33(2), 94-107.

Silverstone, R., & Haddon, L. (1996). Design and the Domestication of Information and Communication Technologies: Technical Change and Everday Life. In R. Silverstone, & R. Mansell, *Communication by Design: The Politics of Information and Communication Technologies* (pp. 44-74). Oxford: Oxford University Press.

Simmonds, L. (2009). What victims want! Victim support, an objective or relative approach to victims needs. *Social & Public Policy Review*, 3(2), 11-29.

Simmons, J., Legg, C., & Hosking, R. (2003). *National Crime Recording Standard (NCRS) an analysis of the impact on recorded crime.* Lodnon: Home Office.

Simon, H. (1955). A behavioural model of rational choice. *Quarterly Journal of Economics*, 99-118.

Simon, D., & Simon, H. (1978). Individual differences in solving physics problems. In R. Siegler, *Children's thinking: What develops?* (pp. 325-348). Hillsdale: Lawrence Erlbaum Associates.

Simonton, D. (1999). *Origins of Genius.* New York: Oxford University Press.

Sindall, K., & Sturgis, P. (2013). Austerity policing: Is visibility more important that absolute number in determining public confidence in the police. *European Journal of Criminology*, 10(2), 137-153.

Slack, N., & Lewis, M. (2008). *Operations Strategy.* London: Pearson.

Smith, N., & Flanagan, C. (2000). *The Effective Detective: Identifying the skills of an effective SIO.* London: Home Office.

Snook, B., & Cullen, R. (2008). *Bounded rationality and criminal investigations: Has tunnel vision been wrongfully convicted?* Retrieved from http://www.mun.ca/psychology/brl/publications/: http://www.mun.ca/psychology/brl/publications/Snook2.pdf

Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud & Security*, 2004(1), 8-12.

Spalek, B. (2006). *Crime Victims: Theory, Policy and Practice.* Basingstoke: Palgrave Macmillan.

Stelfox, P. (2007). Professionalising criminal investiation. In P. Stelfox, *Handbook of Criminal Investigation* (pp. 628-651). Cullompton: Willan.

Stelfox, P. (2009). *Criminal Investigation: An introduction to principles and practice.* Cullompton: Willan Publishing.

Stelfox, P., & Pease, K. (2005). Cognition and detection: reluctant bedfellows? In M. Smith, & N. Tilley, *Crime Science: New approaches to detecting and preventing crime* (pp. 198-207). London: Willan.

Stelfox, P.; Pease, K. (2013). In M. Smith, N. Tilley, & G. Laycock, *Crime Science: New Approaches to Preventing and Detecting Crime* (pp. 191-207). Cullompton: Willan Publishing.

Stern, P. N., & Covan, E. K. (2001). Early Grounded Theory: Its processes and products. In R. S. Schreiber, & P. N. Stern, *Using Grounded Theory in Nursing* (pp. 17-34). New York: Springer Publishing Company.

Sternberg, R. (1985). *Beyond IQ: A Triarchic Theory of Human Intelligence.* Cambridge: Cambridge University Press.

Sternberg, R. (1986). *Intelligence applied? Understanding and increasing your intelectual skills.* San Diego: Harcourt Brace Jovanovich.

Stevens, E. (2013). Safeguarding vulnerable adults: exploring the challenges to best practice across multi-agency settings. *The Journal of Adult Protection*, 15(2), 85-95.

Strauss, A., & Corbin, J. (1990). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* London: Sage Publications.

Strauss, A., & Corbin, J. (1994). Grounded theory methodology: an overview. In N. Denzin, & Y. Lincoln, *Handbook of Qualitative research* (pp. 273-285). London: Sage.

Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* Newbury Park: Sage Publications.

Stuart, A. (2014). Finding Privacy in a Sea of Social Media and Other E-Discovery. *Northwestern Journal of Technology and Intellectual Property*, 12, 149-176

Northwestern Journal of Technology and Intellectual Property, 12, 149-176.

Suvorov, A., & van de Ven, J. (2008). *Goal Setting as a Self-regulation Mechanism.* Moscow: Center for Economic and Financial Research (CEFIR) Working Paper no. w0122.

Svenson, O. (1996). Decision making and the search for fundamental psychological regularities: What can be learned from a process perspective. *Organizational behaviour and human decision processes*, 65(3), 252-267.

Taylor, W. (1997). Aims and Objectives of Secondary Education. *European Journal of Education*, 32, (1), 15-32

Taylor, J. (2015, July 29). *Police Overtime costs up due to staff shortages.* Retrieved from BBC news: http://www.bbc.co.uk/news/uk-33686121

Taylor, R., Fritsch, E., & Liederbach, J. (2014). *Digital crime and digital terrorism.* Upper Saddle River: Pearson Prentice Hall.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review*, 26(3), 304-308.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security*, 2011(3), 4-10.

Temkin, J. (1997). Reporting Rape in the 1990s. *British Journal of Criminology*, 37(4), 507-528.

Temkin, J. (1999). Reporting Rape in London: A Qualitative Study. *The Howard Journal of Crime and Justice*, 38(1), 17-41.

Thames Valley Police. (2017, January 13). *Home / Forensics / Computer and electronic base evidence / Mobile phones/sim cards/ACESO.* Retrieved from Thames Valley Police Knowzone: http://knowzone/kz-for-cbe-mobile-phones

The Police Foundation. (2016, September 3). *Home Affairs Committee inquiry into policing and mental health.* Retrieved from The Police Foundation improving policing for the benefit of the public: http://www.police-foundation.org.uk/uploads/holding/policy/policing_and_mental_health_resp.pdf

Thompson, N. (2000). *Theory and Practice in Human Service.* Buckingham: Open University Press.

Thornberry, T., & Krohn, M. (2000). The self-reported method for measuring delinquency and Crime. *Measurement and Analysis of Crime and Justice, 4,* 33-83.

Tong, S., & Bowling, B. (2006). Art, Crart and Science of Detective Work. *The Police Journal*, 79(4), 323-329.

Trottier, D. (2012). Policing Social Media. *Canadian Review of Sociology*, 411-423.

Trottier, D., & Lyon, D. (2011). Key Features of Social Media Surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval, *The Internet and Surveillance: The Challenge of Web 2.0 and Social Media* (pp. 89-105). London: Routledge.

Urdan, T., & Maehr, M. (1995). Beyond a two-goal theory of motivation and achievement. *American Educational Research Association*, 65, (3), 213-243.

Usher, R. S., & Bryant, I. (1987). Re examining the theory - practice relationship in continuing professional education. *Studies in Higher Education*, 201-212.

Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New Media & Society*, 11(8), 1349-1371.

Veigas, H., & Lum, C. (2013). Assessing the evidence base of a police service patrol portfolio. *Policing: A journal of Policy and Practice*, 7(3), 248-262.

Victims' Commissioner. (2018, March 20). *Victims code and witness charter.* Retrieved from Victims' Commissioner: https://victimscommissioner.org.uk/advice/victims-code-and-witness-charter/

Walkalte, S. (2007). *Imagining the Victim.* Maidenhead: Open University Press.

Wall, D. (2001). Cybercrime and the Internet. In D. Wall, *Crime and the Internet: Cybercrimes and Cyberfears* (pp. 1-17). London: Routledge.

Wall, D., & Williams, M. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing. *Policing and Society*, 409-412.

Ward, R. (2011). Discovering Facebook: Social Network Subpoenas and the Stored Communications Act. *Harvard Journal of Law & Technology*, 24, 563-588.

Ward, S. (2007). MySpace Discovery: Lawyers are mining social networks for nuggets of evidence. *ABA Journal*, 93(1), 34.

Wate, R., & Boulton, N. (2015). *Multi-Agency Safeguarding in a Public Protection World: A Handbook for Protecting Children and Vulnerable Adults.* Brighton: Pavilion Publishing.

Weimann, G. (2014). *New terrorism and new media.* Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars.

Weir, G. R., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles?. *Information security technical report*, *16*(2), 38-43.

Westenberg, M., & Koele, P. (1994). Multi-attribute evaluation processes: Methodological and conceptual issues. *Acta Psychologica*, 87(2), 65-84.

White, S., Fook, J., & Garnder, F. (2006). Critical reflection: a review of contemporary literature and. In S. F. White, *Critical reflection in health and social care* (pp. 1 - 18). Maidenhead, Berkshsire: Open University Press.

Williams, L. (2008). Catch Me If You Can: A taxonomically structured approach to cybercrime. *The Forum on Public Money.*

Wilson, T. (1994). The proper protocol: Validity and completeness of verbal reports. *Psychological Science*, 5(5), 249-252.

Winter, G. (2000). A Comparative Discussion of the Notion of 'Validity' in Qualitative and Quantitative Research. *The Qualitative Report*, 4(3), 1-14.

Wise, R. (1976). The Use of Objectives in Curriculum Planning: A critique of planning by objectives. *Curriculum Theory Network*, 5(4), 280-289.

Woods, D. (1993). Process tracing methods for the study of cognition outside of the experimental psychology laboratory. In D. Woods, *Decision making in action: models and methods* (pp. 228-251).

Yar, M. (2013). *Cybercrime and Society.* London: Sage Publications.

Yexley, M., & Horvath, M. (2012). Developments in investigative approaches to rape: the investigative heritage. In J. Brown, & S. Walklate, *Handbook on Sexual Violence* (pp. 114-136). Abingdon: Routledge.

Youngs, E., & Canter, D. (2006). *Introducing investigative psychology.* Cape Town: Juta & Co ltd.

Zalman, M., & Carrano, J. (2014). *Wrongful Conviction and Criminal Justice Reform: Making Justice.* New York: Routledge.

Zargari, S., & Benford, D. (2012). Cloud Forensics: Concepts, Issues and Challenges. *Third International Conference on Emerging Intelligent Data and Web Technologies* (pp. 236-243). Derby: IEEE xplore.

Zarraga, C., & Bonache, J. (2003). Assessing the team environment for knowledge sharing: an empirical analysis. *International Journal of Human Resource Management*, 14(7), 1227-1245.

<u>Introduction</u>

Introduction of myself and the purpose of the interview

Read through the participant information sheet.

Read through the consent form and confirm that consent is being given by the individual to the interview taking place.

Explain that the interviewer will take notes during the course of the interview.

Ask whether the participant will consent to the interview being digitally recorded

Confirm that consent has been given to digitally record the interview.

Give an explanation of the format of the interview including the topics that will be covered.

Explain that the hypothetical case scenario that will be put the interviewee is not a test. Explain that the scenario is reasonably involved and that a written sheet of the basic circumstances will be provided as an aid memoir. Invite the interviewee to use paper and pen if they wish to note the details of the scenario in order to assist them. Note that the interviewee is being given a short period of time to respond to a complicated scenario and that if this were a real life case, they would both be given more time to analyse the issue, as well as have the opportunity to consult both reference material and colleagues.

Explain that they may be prompted for their rational behind the decisions that they have made.

<u>Part One – The extent to which social media features in investigations</u>

Describe the way in which you would define social media

Tell me about your experience of the extent to which social media plays a part in your investigations.

In what proportion of your investigations does social media feature?

In those investigations, how frequently does it appear?

Estimate the proportion of your time that enquiries around social media take.

In what proportion of your investigations would social media be classed as:

1. relevant material

2. Evidence within an investigation

3. Evidence critical to the successful outcome of an investigation

Describe the types of investigation that social media plays a role in.

Part Two – Previous case dealt with not resulting in a prosecution

The case

Without giving me any details about the individuals involved or the exact location of incident, tell me about a case that you have dealt with, that featured social media but that did not result in a successful prosecution.

How did social media feature in this case?

When did you first become aware of the presence of social media in the case?

How significant a part did it play in the investigation?

Investigative strategy that was chosen

How did you approach social media in this case?

Describe the way in which you preserved the information provided by it or within it.

Explain your reasons for choosing this approach.

Other investigative strategies that were considered

Describe any other approaches that you considered.

If you did consider any other approaches, why did you do so.

Explain the reasons for not choosing those approaches.

With retrospect, were you comfortable with the approach that you did take.

In retrospect would you take a different approach.

Did the approach you take impact on the result of the investigation.

Considerations in the ACPO guidelines

Describe any considerations that you had about seizing physical devices that may have assisted in preservation of evidence.

Describe any consideration that you had with regard to obtaining advice (high tech crime unit / authorities bureau / other specialist dept.) around how to treat social media in this case.

Describe whether you gave any consideration to preserving an audit trail of the actions you took.

Describe whether you gave any consideration to whether your actions would alter any stored electronic data.

Tell me about the reason for choosing this case as an example

Part Three - Investigative approaches taken with regard to cases that have resulted in prosecutions

Without mentioning any specific cases, tell me about approaches to social media that you have taken in investigations that have resulted in a successful prosecution?

Did the approach that you took in your opinion affect the outcome of those investigations?

Explain the reason for adopting the strategies that you did.

Did you consider any other strategies and if so what were they?

Why did you not adopt the other strategies that you considered?

In retrospect, would you adopt different strategies?

Part Four - Other information

Tell me about any factors that have had an impact on how you approach social media.

Has court, training, supervision, professional knowledge or previous experience had an influence on how you deal with social media?

Tell me about the factors that influence how you deal with social media, for example time, resources, effort, professional knowledge, specialist resources.

Tell me about anything else that you think is pertinent.

Part Five – Open scenario

With regard to social media and how the police deal with it:

In the best possible world what would you hope for?

In the worst possible world what are your greatest fears?

What pivotal events from the past few years provide good lessons for the future?

What major decisions with long-term implications are faced at the moment?

What major constraints do you experience inside/outside the organisation / system?

If all constraints were removed, and you could direct what is done, what would you do?

Part Six – Specific scenario: Harassment

Process tracing:

You've been asked to review / look at an investigation, which involves rape, grooming and sexual activity with a child with a social media aspect to it. The suspect is in custody during night time hours for grooming and they're suspected of raping the victim, the victim of the grooming. The grooming has taken place over the suspect's social media.

In front of you on the table there are 2 columns. The first column looks at how you access the suspect's social media. The second column shows options for how to

record the social media content once it is accessed. Could you have a look through the options in both columns. Any that pique your interest or that you would naturally seek out were this to be a real investigation, please pick up. Under some there is some further information that may assist you, under others the information is fairly generic.

FORM UPR16

Research Ethics Review Checklist

Please include this completed form as an appendix to your thesis (see the Research Degrees Operational Handbook for more information

UNIVERSITY OF PORTSMOUTH

Postgraduate Research Student (PGRS) Information		Student ID:	UP675071
PGRS Name:	Wojciech Spyt		
Department:	Institute of Criminal Justice Studies	**First Supervisor:**	Dr Karagiannopoulos
Start Date: (or progression date for Prof Doc students)		**01.10.2012**	

Study Mode and Route:	Part-time	☒	MPhil	☐	MD	☐
	Full-time	☐	PhD	☐	Professional Doctorate	☒

Title of Thesis:	Social Media and Police investigations: Understanding the strategies that officers pursue when they encounter social media in their investigations
Thesis Word Count: (excluding ancillary data)	49270

If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University's Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study

Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).

UKRIO Finished Research Checklist:

(If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: http://www.ukrio.org/what-we-do/code-of-practice-for-research/)

a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?	YES NO	☒ ☐
b) Have all contributions to knowledge been acknowledged?	YES NO	☒ ☐
c) Have you complied with all agreements relating to intellectual property, publication and authorship?	YES NO	☒ ☐
d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?	YES NO	☒ ☐
e) Does your research comply with all legal, ethical, and contractual requirements?	YES NO	☒ ☐

Candidate Statement:

I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)

Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):	4/15:35

If you have *not* submitted your work for ethical review, and/or you have answered 'No' to one or more of questions a) to e), please explain below why this is so:

Signed *(PGRS)*:	Wojciech Spyt	**Date:** 31.05.18