

Capturing Killers: The Construction of CCTV Evidence during Homicide Investigations

Fiona Brookman^{a*} and Helen Jones^b

^aCentre for Criminology, Faculty of Life Sciences and Education, University of South Wales, Treforest Campus, Pontypridd, CF37 1DL, Wales. 01443 482572.

Fiona.brookman@southwales.ac.uk; ^bCentre for Criminology, Faculty of Life Sciences and Education, University of South Wales, Treforest Campus, Pontypridd, CF37 1DL, Wales. 01443 454668. Helen.jones11@southwales.ac.uk.

**Centre for Criminology, Faculty of Life Sciences and Education, University of South Wales, Treforest Campus, Pontypridd, CF37 1DL. Fiona.brookman@southwales.ac.uk.*

Fiona Brookman is Professor of Criminology at the University of South Wales, UK. Her research focuses primarily on homicide, violence and policing and she invariably adopts qualitative research methods, including ethnographic approaches.

Helen Jones is a Research Fellow at the University of South Wales, UK and has previously worked in a number of roles for the police. Her research interests include homicide, major crime investigation, and policing, with a focus on qualitative research methods.

This work was supported by the Leverhulme Trust under Grant number RPG-2014-143.

Capturing Killers: The Construction of CCTV Evidence during Homicide Investigations

Drawing upon quantitative and qualitative data gathered during a four-year ethnographic study of 44 British homicide investigations, this paper advances the sparse literature on how closed-circuit television (CCTV) contributes to criminal investigations and the risks associated with its use. Based on insights gleaned from interviews with homicide detectives, analysis of case files and observations of live homicide investigations, we examine how CCTV is used during homicide investigations focusing principally on two key investigative moments – identifying and charging suspects. Our quantitative data indicate that CCTV is used more frequently than any other kind of forensic science or technology to both identify and charge suspects. Nevertheless, our qualitative data reveal numerous challenges associated with how CCTV footage is recovered, viewed, shared, interpreted and packaged for court. We reveal the individual and organisational processes and workarounds that have emerged in a socio-technical landscape that lacks clear standards and principles. We discuss the implications of these findings for practice and policy and their relevance to questions about the socially constructed nature of forensic scientific knowledge.

Keywords: homicide investigation, CCTV, interpretation, expert evidence.

Introduction

Forensic science evidence plays an important, often pivotal role, in many criminal investigations, determining whether, when and how a crime has been committed, identifying or eliminating suspects, linking suspects to crime scenes, validating accounts and establishing sequence of events (Kruse 2016, Home Office *et al.* 2018). Most recently, forensic evidence has incorporated traces obtained from digital devices, and almost every crime now contains some kind of digital evidence (Vincze 2016). Information may be extracted from a range of devices including closed-circuit television

(CCTV), mobile phones, computers, sat navs and smart watches, and used for both intelligence and evidential purposes (Tully *et al.* 2020). Notably, in the UK and other countries, such as the United States, there has been a rapid expansion in the use of video-recording technologies by law enforcement agencies, including footage captured by CCTV in public and private spaces (for example, commercial premises, public transport, car parks and residential properties) and on dash cams and police body worn cameras (Porter 2007, Piza 2018). Nevertheless, very little research has examined how CCTV contributes to the investigation of crime or the risks associated with its use.

This paper seeks to advance current knowledge of how CCTV contributes to criminal investigations, focusing on homicide inquiries. The investigation of homicide provides a particularly useful lens through which to examine the contribution of CCTV because it is often considered the gold standard of crime investigation and seeks to maximise the chance of detecting each and every case (Stelfox 2009, Brookman and Innes 2013). Compared to volume crime, homicide investigations are resource rich and multi-layered endeavours that push technological boundaries and mobilise different professionals within and outside policing (Brookman *et al.* 2020). The diverse range of criminal justice actors involved in the investigation of homicide have varying levels of training, understanding, experience and skill in the use of CCTV for investigative purposes. For example, digital experts (who are often outsourced) complete specialist training in order to retrieve and enhance CCTV footage, and may provide expert witness evidence at court. In contrast, CCTV officers or coordinators are invariably police staff or detectives, who may not have received specialist training but can be tasked to identify, recover and view footage, and create CCTV packages for use during suspect interviews, charging decisions and at court. Forensic imaging technicians (invariably police staff as opposed to officers) work in-house and are trained to recover

CCTV, produce electronic packages for court and enhance footage. Others, who handle or analyse CCTV with little or no training, include uniformed officers, senior investigating officers (SIOs) and intelligence analysts. Whether and how CCTV is recovered and interpreted depends upon the level of training, experience, knowledge and skill of the individual undertaking the task.

A series of obstacles confront criminal justice actors in making appropriate and effective use of CCTV during homicide investigations. Whilst many of these challenges exist in other kinds of criminal investigations, some are amplified within homicide investigations because of the vast amount of CCTV footage that is often retrieved. For example, during one of the investigations that we studied, more than 12,000 hours of footage was recovered during one weekend. Such voluminous data pose difficulties and risks for criminal justice actors in how they: manage and (re)view the data for the purposes of disclosure (McCartney 2018); interrogate data in a timely manner (House of Lords Science and Technology Committee 2019); deal with footage stored on an increasingly diverse range of file formats (Surveillance Camera Commissioner 2017); and analyse and compare CCTV footage (Tully 2020).

Finally, CCTV is an important forensic discipline to explore from a social science perspective because it has largely been ignored. For example, science and technology studies (STS) scholars point to the socially constructed nature of forensic evidence and contest its credibility or 'truthfulness' but have concerned themselves with traditional forensic methods (e.g. DNA, fingerprinting), leaving digital evidence unexplored (Jasanoff 2006, Lynch *et al.* 2008, Kruse 2016). CCTV is a form of forensic evidence with one important difference - its retrieval and interpretation happens outside the scientific laboratory, which makes it interesting to examine the practices of its production. CCTV footage, like other forms of forensic evidence, does not provide an

absolute truth. Rather, it requires numerous actors, from the crime scene through to court, to interpret and evaluate the images, ascribing to them a factual status (Casey 2019a). Risks of ‘mishandling, misinterpretation, misunderstanding, and manipulation’ (Casey 2019a, p. 1) exist at each stage of the criminal justice process.

Drawing on quantitative and qualitative data gathered during a four-year ethnographic study of 44 homicide investigations in Britain, we explore, in this paper, how CCTV contributes to criminal investigations and the risks associated with its use. Based on insights gleaned from interviews with homicide detectives, analysis of case files and observations of live homicide investigations, we examine how CCTV is used to identify and charge homicide suspects. We then consider in detail the challenges and risks associated with how CCTV footage is recovered, viewed, shared, interpreted and packaged for court and reveal how current practices compromise the integrity and provenance of CCTV evidence. We begin, below, by providing a review of existing literature that examines the contribution of CCTV to criminal investigation and potential barriers to its effective use. Next, we describe the methods of data collection and analysis used in the present study. In the remainder of the article, we present our findings and discuss their implications.

The contribution of CCTV to criminal investigations

There exists a large body of research which explores whether CCTV prevents crime (see Piza *et al.* 2019 for a review of 80 studies) and impacts crime clearance. For example, Morgan and Dowling (2019) found that when investigators were given access to CCTV footage for crimes occurring on the rail network in New South Wales, Australia, there were associated improvements in investigation outcomes, with larger improvements for theft and property damage in comparison with assault. Other studies

have found only a minimal improvement in crime clearance rates associated with the introduction of CCTV in cities (Robin *et al.* 2020), with improvements dependent on offence type (e.g. Jung and Wheeler 2019 found improvements were limited to thefts, whereas Gerrell 2020 found small improvements associated with violent crime). None of these studies have analysed whether CCTV impacts homicide clearance rates.

Furthermore, few studies have developed a detailed and nuanced understanding of *how* CCTV is used during investigations and how footage may assist investigators. Among the few exceptions, Gill and Spriggs (2005) evaluated the overall impact of 13 CCTV schemes in England, acknowledging that all schemes provided some images to the police, which they could use to identify or eliminate suspects from their enquiries, or to identify witnesses and victims. Similarly, La Vigne *et al.* (2011) evaluated the use of public CCTV for crime control purposes in three American cities and found that investigators used CCTV to assist with identifying suspects and witnesses, corroborating witness accounts and documenting sequences of events.

Other studies have used data obtained from crimes committed on railway networks, which operate a large number of cameras. For example, Ashby (2017) analysed data for more than 250,000 crimes recorded by the British Transport Police that occurred on the railway network in England and Wales between 2011 and 2015. The data included responses from first-line supervisors as to whether CCTV had been useful, or not, in the investigation and why. Ashby found that footage was more likely to be available in more-serious offences. Overall, CCTV was perceived as useful in 65% of cases where available and, with the exception of drugs/weapons possession and fraud, was associated with an increase in the likelihood of crimes being solved. Responses indicated some of the ways in which CCTV was not helpful to officers, including the incident not being captured and the images not being of sufficient quality.

In an Australian study, Dowling *et al.* (2019) surveyed 146 investigators in the New South Wales police force who had recently requested footage from the rail system's network of CCTV cameras. Focusing on assault, robbery, theft, sexual offences and property damage, their analysis revealed that footage was more likely to be requested and used, and perceived as useful, by those investigating assault offences. Across all offence types, 87% of investigators used footage as part of their investigation, using it to locate or confirm the identity of suspects, generate intelligence/investigative leads, corroborate statements and determine whether an offence had happened. Nevertheless, 13% of investigators reported poor image quality or difficulties accessing footage. Although these studies deepen our understanding of how investigators use CCTV, the railway setting is unique because elsewhere cameras are not deployed so widely or are less readily accessible (Ashby 2017).

Broadly, the aforementioned studies highlight how CCTV may serve as an investigative tool, providing investigators with answers to questions of source and activity (i.e. who, what, when, where and how) (Milliet *et al.* 2014, p. 474). Hadjimatheou (2017) also suggests that CCTV may help to safeguard against wrongful convictions because it provides a source of data through which to eliminate suspects. Additionally, CCTV may assist the prosecution process. Research suggests that good quality images are instrumental in facilitating charging decisions against suspects, often lead to an early admission of guilt and, when properly presented, can influence sentencing at court because they reveal contextual information about the severity of an offence (Levesley and Martin 2005).

Very few studies have explored the contribution of CCTV to homicide investigations. As exceptions, Levesley and Martin (2005) sought the views of more than 250 police officers from across 33 British police services about their attitude

towards and use of CCTV. Responses from a sample of unstructured interviews provided numerous examples where officers felt CCTV had been invaluable to serious crime investigations, including murder, although their reasons were not recorded. Other studies have considered CCTV as part of a broader range of evidence types and factors that help to solve homicide cases. In their quantitative analysis of 294 homicide case files between 2008 and 2011, in Cleveland, Ohio, McEwan and Regoeczi (2015) identified that digital devices (including video surveillance tapes) were seized from nearly one third of homicide scenes but were not positively related to case closures (suspect arrest). In contrast, Roycroft (2007) interviewed 32 SIOs from the Metropolitan Police Service, responsible for the investigation of 166 murders between 2001 and 2003 and found that 21.7% of cases relied on CCTV to help solve cases (i.e. arrest and charge suspects). Furthermore, his findings indicate how investigators used CCTV to identify suspects but also to disprove alibis and to pursue other evidential opportunities.

In contrast to the sparse academic research, there is a growing body of policy documents and specialist literature that recognises the value and contribution of CCTV to criminal investigations, and which supports the aforementioned studies. For example, the Surveillance Camera Commissioner (2016) states CCTV was fundamental in identifying and prosecuting suspects involved in riots across the UK in 2011, which took place after the shooting of Mark Duggan in London. Similarly, guidance issued by the Forensic Science Regulator (FSR) (2016) details how video and still images may provide opportunities for enhancement and expert forensic interpretation, which, for example, can identify or eliminate suspects. The College of Policing (2020) also outlines a number of ways in which CCTV may benefit investigations, such as capturing the nature of an offence, demonstrating inconsistencies in witness and suspect accounts, and helping to direct forensic recovery and examinations. Based on

professional experience, Gerrard (2007) argues that CCTV can assist all kinds of police investigation. Furthermore, he suggests that in comparison with more traditional evidence types, such as DNA and fingerprints, CCTV offers the potential for more detections.

The challenges of using CCTV in criminal investigations

A small body of researchers have focussed upon the challenges of using CCTV in criminal investigations. Brady and King (2017, p. 527) contend that for technologies such as CCTV to be effective in criminal investigation, they must be part of a three-legged stool composed of efficient people and processes, and robust technologies. More than ten years ago, Gerrard (2007, p. 14) argued that the police approach to CCTV was inadequate. He suggested that the police did not recognise CCTV as a specialist discipline, training was ad hoc and patrol officers or detectives were relied upon to gather footage without the appropriate technology to recover or view images. Other studies have identified similar shortcomings, recommending that those who recover and use CCTV footage are trained properly (La Vigne *et al.* 2011). More recently, scholars suggest that the police still lack the knowledge and skills to identify and recover effectively digital devices or traces at scenes (Casey 2019b, Wilson-Kovacs 2019).

CCTV images may serve both an investigative purpose and offer the potential for expert forensic interpretation through which to identify or eliminate a suspect, such as facial image comparison, clothing comparison, gait analysis, vehicle identification or comparison, and object comparison (FSR 2016). Each technique poses challenge and risks. The Forensic Science Regulator observes that in the UK there are no accredited providers of image analysis and comparison, and no standardised techniques for how images should be compared or interpreted. She highlights the comparison of faces,

clothing, footwear and vehicles from CCTV imagery as a particularly problematic area, warning that experts may be straying beyond the limits of their knowledge or expertise (Tully 2020, p. 9). This poses challenges for lawyers, judges and juries who are tasked to assess and evaluate the credibility of such evidence (Tully and Stockdale 2019). Hak (2019) suggests that appropriate mandatory training is required for some areas of expertise, such as facial comparison, in order that only properly trained experts provide an evaluative opinion for court. Finally, Edmond (2013) also highlights that the credibility of (external) experts' findings may be compromised when detectives share their suspicions of what can be seen with experts (see also Sunde and Dror 2019).

In the absence of standardised and proven techniques and practices, questions inevitably arise about who is best placed to interpret CCTV images (e.g. police officers, detectives or experts), and how can we evidence the validity and reliability of their techniques and claims (Edmond 2010). Ultimately, investigators with inadequate training, skills or expertise, and inefficient processes and technology, inevitably heighten the risk of CCTV evidence being compromised, which in turn, increases the possibility of misleading evidence being presented at court with potentially serious consequences for justice (Porter 2012, Smit *et al.* 2018). Lastly, the processes involved in packaging and presenting CCTV evidence for court (often referred to by police as storyboards) are neither standardised across police services nor amenable easily to challenge. CCTV images provide a particularly compelling form of evidence (Evison 2015, p. 533) though they rarely 'simplistically mirror reality' (Porter 2012, p. 41). Rather CCTV undergoes a series of (re)construction processes that can result in contested interpretations of the same CCTV footage (Goodwin 1994) and the emergence of 'alternative truths' (Kim 2016).

All of the aforementioned deficiencies cast doubt on the potential veracity of CCTV evidence and whilst the socially constructed nature of scientific knowledge has long been recognised amongst STS scholars (Cole and Bertenthal 2017, p. 354), attention to digital forensic evidence is less well developed.

Overview

There remain large gaps in our understanding of precisely how CCTV footage is used during the investigation of homicide and, in particular, the challenges and risks associated with its use. Existing studies have tended to focus upon the (potential) value of CCTV to crime prevention or clearance, with little academic attention to the potential hazards of its use. The STS literature, that illuminates the socially constructed nature of scientific knowledge, has largely ignored digital forensic evidence. Our aim in this article is to help to fill some gaps in knowledge and suggest potential solutions to the ongoing risks posed by the use of CCTV. Our interviews are useful for exploring detectives' and CCTV officers' views, understandings and experiences of CCTV work. Our observations are useful for revealing working practices amongst these investigators and examples of how CCTV is socially produced. In the following section, we describe the methods of data collection and analysis used in the present study. In the remainder of the article, we present our findings and discuss their implications.

Data and methods

The study and research sites

This paper draws upon data gathered during an ethnographic study of the use of forensic

sciences and technologies (FSTs) in British homicide investigations.¹ Broadly, the aims of the research were to provide an in-depth understanding of how FSTs contribute to the police investigation of homicide. The data include case papers, interview transcripts and ethnographic fieldnotes relating to 44 homicide investigations across four police services. The four police services that took part in the research were chosen due to their distinctively different models of forensic science provision, ranging from comprehensive services provided by a public forensic laboratory through to those with smaller in-house capabilities, such as blood screening, who rely on private forensic science providers (FSPs) for the vast majority of their work.² In addition, we visited three major private FSPs and two public laboratories in order to gather data on how they operate and, principally, to interview forensic scientists. We also toured one police service's in-house capabilities. All research sites and data related to research participants and homicide cases have been given pseudonyms or disguised to maintain anonymity of the data.

The homicide cases and data

All offences, except for two, took place between 2011 and 2017, with most cases ($n=32$) occurring between 2014 and 2017. Thirty-three of the investigations were completed (or virtually completed) at the time of data gathering (i.e. a guilty verdict of murder or manslaughter was reached at court or agreed through pleas). We selected

¹ We adopt a broad and inclusive view of the range of FSTs that can be utilised in homicide investigations, such as DNA profiling, fingerprint examination, blood pattern analysis, ballistics interpretation, trace evidence analysis and digital evidence from mobile phones, computers and CCTV.

² The term public in this context refers to forensic science provision that is funded by the police service or the police authority.

these cases from summary lists provided by each police service to reflect a range of modus-operandi, victim-offender relationship, motive, circumstance and forensic contributions. These cases were chosen specifically to enable us to chart how a variety of FSTs had contributed to the successful investigation and prosecution of a range of homicide and to unravel the decisions and processes that led to this endpoint. The remaining 11 cases were live homicide investigations that we observed as they unfolded, including two cases in which the victims survived despite the prognosis that they were likely to die from their injuries. These cases were investigated as homicides though, ultimately, the suspects were convicted of lesser offences. Additionally, in a third case, the prosecution service directed that no further action would be taken. The selection of live investigations was less structured in that we took cases that arose at each police service (see below). Nevertheless, they represent the kind of diversity reflected in the completed investigations.

The 44 cases studied reflect a range of modus-operandi (broken down into cases involving: sharp instrument (20), blunt instrument (5), shooting (5), hitting/kicking (5), strangulation/asphyxiation (3), poisoning (2), shaking (1) and where the cause of death was unascertained (3)) and victim-offender relationship (i.e. victims who were: a friend/acquaintance (17), a current/former partner (9), strangers (8), children of the offender (5), parents of the offender (3) and customers/clients (2)). Across the 44 cases, there were 47 victims (27 males, 20 females) and 62 offenders (55 males, 7 females). Our cases include those where suspects were identified very quickly through to complex, protracted investigations that were not resolved for many months or years.

For each homicide investigation we retrieved case papers and/or made extensive notes from documents. The documentary material included police closing reports, policy files from SIOs and crime scene managers, minutes from forensic strategy

meetings, briefing notes, statements and reports from forensic scientists and other experts, and prosecution documents. We spent 650 hours (81 working days) retrieving these data.

In-depth semi-structured interviews were undertaken with 134 criminal justice practitioners who were involved in homicide investigation – 118 of whom were involved directly in one of the 44 cases that we studied. Participants were recruited to reflect a range of roles and experiences, and included SIOs or deputy SIOs, detectives, crime scene managers/coordinators, forensic scientists, fingerprint examiners, digital forensic experts and CCTV officers. With the exception of one, all interviews were, with the permission of interviewees, digitally recorded and transcribed verbatim. The average length of interviews was 83 minutes. In addition, we conducted 10 informal interviews with forensic practitioners during tours of forensic science facilities.

The third phase of our research was the most immersive and involved ethnographic observations of 11 live homicide investigations across the four police services. We spent 700 hours (88 working days) observing different moments of homicide investigation, from the initial scene attendance by detectives and forensic scientists, through to trials at court. We were given virtually unfettered access to these investigations and were usually able to attend within a day (depending upon the location). We entered crime scenes and observed discussion and debate amongst crime scene managers, SIOs, forensic scientists, and other experts. We also accompanied detectives on house-to-house and CCTV enquiries, and attended daily briefings, forensic strategy meetings, prosecutors' conferences, and different stages of the trial process.

Whilst the cases in our sample reflect a range of modus-operandi and victim-offender relationship, our 44 cases are not a representative cross-section of all British

homicides. Further, we have targeted cases that utilise and exemplify particular, lesser-known forensic technologies, which are not characteristic of all British homicide investigations. Moreover, our sample does not capture cases that were not solved. This is because three quarters of our sample were successfully completed investigations that we studied retrospectively and, of the eleven live cases that we observed as the investigations unfolded, only one case failed to result in a suspect being charged.³ As a result, our sample of cases has a higher clearance rate than the annual average across Britain.⁴ Our sample is also relatively small, particularly in contrast with studies that have examined the value of CCTV for investigating crimes that occurred on the railway network (see Ashby 2017). However, our approach was to produce ‘thick descriptions’ (Geertz 1973) of how science and technology is used within homicide investigations – thus, achieving depth rather than breadth.

Data analysis

The interview transcripts, fieldnotes, case papers and notes made from case papers and documents were all uploaded into NVivo 12 and analysed thematically (Braun and

³ In this case, whilst detectives considered that the victim’s partner was in some way responsible for her death, the forensic pathologist was unable to determine whether her injuries were caused in some kind of attack or were the result of inappropriate attempts at assistance, movement and resuscitation. The prosecuting authority determined that there was insufficient evidence to charge the suspect.

⁴ In England and Wales, over the 10-year period 2008/09-2017/18, police charged a suspect in an average of 86% cases (Morgan *et al.* 2020, calculated from table for figure 22) and in Scotland, for the period 2010/11-2019/20, 98% of cases were classed as solved, i.e. an accused individual had been identified (Scottish Government 2020).

Clark 2006). This involved engaging with the data at different stages of the project in order to become familiar with it in the first instance and then creating memos containing more general reflections and codes of conceptual categories in accordance with grounded theory (Corbin and Strauss 2008). At regular points we met (in person or virtually) to discuss and debate the emerging findings. Throughout this process some codes were expanded whilst others were collapsed. In this way, and with our different backgrounds and expertise, we developed and agreed more than 450 nodes. For the purposes of this paper, we focus on 14 nodes that reflect processes and practices associated with CCTV, drawing upon data from case papers, interviews and observations. For example, CCTV viewing and interpreting, CCTV relevance or value, and CCTV enhancement (please see Table A1, Appendix, for full details and descriptions of the 14 nodes analysed).

In order to determine how a particular FST, including CCTV, had been used within a homicide investigation, we systemically read through all of the retrieved case papers and/or our extensive notes made from documents, charting which FSTs were used, who made the decision to use it and when, specific details of the examination and the results. These were supplemented, where possible, with data from interview transcripts and fieldnotes made during our observations. We documented not only positive results/outcomes but also those that did not impact (or impacted negatively) on the investigation. Through this process, we developed a comprehensive spreadsheet of which FSTs were used and how, for the 44 homicide cases studied.

Access and ethical considerations

Gaining access to the closed world of homicide investigation can be difficult given the sensitive nature of the work of homicide detectives. The experience and credibility of the research team, plus established relationships with key stakeholders and gatekeepers,

were central to negotiating access to research sites and ensuring that the research progressed effectively. Subsequently, the (trusting) relationships that the researchers formed with participants were crucial when renegotiating day-to-day access to people, places, and information (Brookman 2015, p. 243). The research was conducted in accordance with the British Society of Criminology code of ethics (2015) with particular attention to the issues of informed consent, anonymity, confidentiality, and stringent data management protocols.

Findings

In this section, we present evidence from our interviews, observations and examination of documents, of how CCTV is used during homicide investigations and the various challenges and risks it poses. For the purposes of this paper, we focus on instances where CCTV footage was retrieved from publicly or privately owned cameras (such as those installed on public transport, commercial premises and residential properties, and as dash cams on vehicles). This type of footage is much more prevalent in the UK than police-controlled cameras (Police Foundation 2014: 6). We begin by drawing upon our quantitative data to place the use of CCTV in broader investigative context. We then explore in detail, the challenges and risks associated with CCTV work, drawing mainly upon our observations and interviews.

How CCTV contributes to homicide investigations

CCTV is one of many investigative avenues that detectives pursue during homicide investigations. For the purposes of our research, we draw a broad distinction between information/evidence resulting from FSTs and that which arises from other sources, such as witness accounts, admissions by the suspect, intelligence held on police-systems

and circumstantial evidence. A total of 62 suspects were implicated in the 44 homicide cases that we studied.⁵ In one case, involving multiple gunmen, one of the three suspects (seen on CCTV), was never successfully identified. In a separate case, the suspect was identified, but never charged, due to insufficient evidence.

Findings from FSTs are used in various ways within criminal investigations. Specifically, our data revealed how CCTV affords numerous benefits to homicide investigators including, for example, identifying suspects and witnesses, implicating or eliminating suspects, corroborating or refuting accounts provided by suspects and witnesses, linking suspects to key exhibits, identifying further investigative or forensic opportunities, targeting or focusing other strategies, showing movements and associations of, or between, victims and suspects, directing charging decisions, and supporting prosecutions and/or refuting defence arguments at court. For the purposes of this paper, we focus on how CCTV was used to identify and charge suspects. We utilised SIOs' policy files and interviews, reports of prosecutors' charging decisions, current situation reports, closing reports and our fieldnotes to capture facts about how findings from CCTV had led, solely or in conjunction with other intelligence/evidence, to suspects being identified and charged.

Figures 1 and 2 illustrate the range and frequency of FSTs used to firstly identify suspects and subsequently to inform charging decisions.⁶ Specifically, 32 (of 61) suspects were identified and 51 (of 60) suspects were charged using findings from one

⁵ 130 suspects (94 relating to a cold case from the 1980s) were eliminated from these investigations, and will not be considered in this paper.

⁶ In some instances, identification included implication, i.e. the suspect was already known to the police but findings from FSTs implicated them in the offence allowing SIOs to categorise them as a suspect.

or more FSTs (sometimes used in conjunction with other sources of information).⁷ In particular, CCTV was used most frequently and featured in some capacity in 42 of the 44 homicide cases studied.⁸

[Figure 1 near here].

Figure 1. Type of forensic science and technology used to identify suspects.

Using CCTV to identify homicide suspects

Figure 1 illustrates that almost one quarter of all homicide suspects (15 of 61) were identified through CCTV, 12 of whom were identified in the first four days of these investigations. In all but one instance, CCTV was combined with other intelligence or evidence in order to identify suspects. Notably, in terms of frequency, witness accounts, intelligence held on police systems and/or phone data were used in conjunction with CCTV to identify suspects. To illustrate, in one case, the SIO recorded in the policy file their reasons for declaring a male a suspect in a gang-related shooting:

Previous intelligence connects him to gun crime and [this] area. Potentially one of the unidentified gunmen as seen on CCTV – description as 6ft black male of slim build - is consistent with this. (Extract from SIO policy file, Operation E01).

Of the 15 suspects who were identified (either solely or in part) by CCTV, our analysis reveals that CCTV played an important role in enabling detectives to identify suspects

⁷ The total number of times FSTs were used is greater than the number of suspects identified or charged because decisions often relied upon a combination of FSTs.

⁸ For the remaining two cases, one related to the reinvestigation of a cold case from the 1980s, the second was a domestic homicide, which occurred in the family home and the suspect admitted killing his wife.

in two stranger homicides. Moreover, without this footage, one case may have developed into a long-running whodunit investigation. CCTV also played an important role in two homicide investigations where victims knew the suspect in a customer-client capacity, i.e. they only had limited knowledge of one another. In one case, CCTV helped detectives identify a suspect and in the second case, CCTV images suggested that a young female who had been reported missing had been killed inside a commercial premises owned by the proprietor (this proved to be the case). In all four of these cases, suspects pleaded guilty to murder or manslaughter, by which point, there was corroborative evidence such as witness accounts, data from mobile phones, DNA and blood pattern analysis. In the remaining 11 cases (involving friends/acquaintances or partners/ex-partners), CCTV corroborated existing intelligence or witness accounts, helping detectives to build intelligence/evidence in order to identify or implicate suspects.

Using CCTV to charge homicide suspects

Figure 2 shows that of all the FSTs used to inform charging decisions, CCTV was used most frequently. CCTV directly informed charging decisions in respect of 20 (of 60) suspects in the first seven days of these 44 homicide investigations and ultimately, more than half of suspects (35 of 60) were charged by using evidence gleaned from CCTV footage. However, with the exception of one suspect, charging decisions were based on CCTV evidence combined with other forms of intelligence or evidence. Specifically, the most frequently used types of intelligence/evidence used alongside CCTV were witness accounts, followed by circumstantial evidence, phone data and DNA. For example, in one case, the Prosecutor used CCTV footage in conjunction with witness evidence and admissions in interview to inform their decision to charge the suspect with murder:

Suspect accepts that he hit the victim but claims he was acting in self-defence at the time. The CCTV undermines the suspect's account - showing he was not threatened by the victim at all... The witness evidence shows that the victim was hit with a high degree of force. I have considered whether this should be manslaughter (given the fact it is one punch) or murder given the degree of force used. I think it best to charge murder at this stage... (Extract from charging decision, Operation W10).

[Figure 2 near here].

Figure 2. Type of forensic science and technology used to charge suspects.

There are many reasons why CCTV stands out amongst FSTs at these stages of homicide investigation. For example, detectives may pursue CCTV enquiries more often than other activities, particularly since many consider it a cheaper option than 'wet' forensics, or the results from these enquiries may emerge more quickly than results from other FSTs (such as DNA interpretation, forensic pathology or toxicology). Hence, how often CCTV is used to identify or charge suspects does not (necessarily) reflect its value or usefulness. For example, some SIOs and detectives cited findings from lesser-used FSTs as a decisive factor in identifying or charging a suspect, such as toxicological analysis of hair samples.

The challenges and risks of using CCTV in homicide investigations

Aside from the obvious benefits accrued from using CCTV in assisting to both identify and charge homicide suspects, our data illustrate many challenges associated with recovering, interpreting and presenting CCTV footage, to which we now turn.

Recovery

Many of the detectives that we encountered lacked the skills, training or technology to

recover footage in a timely and efficient manner. In order to preserve the original CCTV footage (and for it subsequently to be made available to experts), it must be retrieved in its native (original) file format, from which a working copy is made. However, some detectives were ill equipped to recover native footage and one police service identified a noticeable lack of training for officers who recover CCTV. Sometimes these failures to recover CCTV resulted from a lack of equipment, on other occasions, detectives had not been trained in the basics of recovery from any (or different kinds of) systems, as the following extract from our fieldnotes illustrates:

Liz and Sara have a series of premises to visit and clear instructions to 'retrieve the CCTV and not to take no for an answer'. On route, both detectives tell me that they are concerned about their lack of techy knowledge. Sara says, "I'm not being sexist but why do they send women to do this as we don't understand it"... Sara and I head to the first shop on the list. The lady behind the counter doesn't know how to operate the system and says that we ought to return after 5pm when the manager is in and should be able to help... As we leave, Sara says "see, I don't know why they sent me, I can't operate this stuff". Later we bump into Liz and compare notes on progress. She, like us, has been unable to retrieve any CCTV from premises... the Co-op that she visited has CCTV that might be useful but they needed a CD not a memory stick in order to upload it for us (they had already explained this to an officer who visited previously) and Liz is clearly frustrated saying "this makes us look like idiots". (Extract from fieldnotes, Operation C02).

In this particular investigation, the SIO and deputy SIO had emphasised many times during the morning briefing how important CCTV was going to be for a charging decision and for use in the suspect interviews later that day. However, the detectives were not equipped to fulfil this crucial task.

Some detectives were unable to retrieve CCTV footage because owners were not available or did not have the necessary passwords or knowledge to access systems. This inevitably required a repeat visit by either a detective or technician in order to access

and retrieve the footage. On other occasions, the volume of CCTV requested was unmanageable or not achievable. For example, during an investigation into a fatal stabbing in a flat, detectives were tasked to recover five hours' worth of CCTV footage from all buses that had driven past the flat. It transpired that approximately 40 buses had passed the attack site during the time parameters and that each bus would have to be taken out of service temporarily in order for the CCTV to be downloaded. In this instance, the deputy SIO reduced the time parameter to one hour, in order to ensure that the bus company was not unduly impacted.

Our research revealed instances where detectives who were co-ordinating or undertaking CCTV enquiries were removed from these tasks in order to assist with other lines of enquiry, resulting in a lack of continuity and oversight of CCTV work. Inadequate processes for logging CCTV enquiries compounded these difficulties and hampered the flow of information between detectives, uniformed officers and the major incident room. Consequently, we observed detectives on CCTV enquiries re-visiting premises that police had previously attended, leading to frustration amongst detectives and delays in the identification and recovery of CCTV, as illustrated in the following extract from our fieldnotes:

The main aim of the CCTV trawl this afternoon is to find out where the suspect has gone after the murder... However, there had been a breakdown in communication and Ian [CCTV officer] wasn't sure which officers had gone to the scene, where CCTV had been located and what had been seized. Ian said he wouldn't have had an issue if he'd done all of the CCTV work from the beginning. Instead he'd been pulled away to do interviews... We went to one property, which had three cameras viewing the road outside... The images were very high quality but... the system began over-writing after 10 days and we were a day late. (Extract from fieldnotes, Operation W11).

Some detectives spoke of the challenges of being able to identify mobile or dash cam CCTV, installed in vehicles. In one investigation, CCTV footage was recovered from an ambulance that had driven past the scene of a shooting. The footage captured a lorry parked opposite the scene with potentially additional valuable dash cam footage. This line of enquiry was not pursued. However, the owner of the lorry firm saw TV coverage of the shooting and contacted the police, by which time the footage had been overwritten. In other instances, CCTV was overwritten because detectives lacked the training or technology to recover footage quickly, or because they missed critical timeframes. To illustrate, in a suspected domestic homicide, CCTV was identified at an elderly couple's address who lived opposite the house of the victim and suspect. A detective attended but she lacked both the skills and equipment to download the footage without removing the hard drive. The residents were reluctant to hand over their hard drive and assured the detective that the device did not re-write for two weeks. The detective, in turn, assured the SIO, who decided not to call a technician out at the weekend to assist with the recovery. When the technician arrived on Monday, the footage was overwritten.

Integrity and Provenance of CCTV Footage

Many detectives and CCTV officers were mindful of preserving the integrity and provenance of CCTV footage. For example, they used the speaking clock to verify the accuracy of time on CCTV systems and created master copies of the native file. Nevertheless, this good practice was not universal and we observed and heard about adverse practices. For example, some detectives and CCTV officers had purchased their own equipment in order to download footage more easily and quickly, such as a USB splitter to overcome problems with older systems having only one USB port. New and emerging technologies (such as doorbell cameras) with cloud-based storage, also

present novel challenges and risks associated with how (native) footage is captured, retrieved and shared, that detectives grapple with.

Viewing and Sharing CCTV Footage

We repeatedly heard about how resource-intensive it is for officers to view and log vast quantities of CCTV. For example, an excerpt from the CCTV strategy for Operation N11 stated, '[v]iewing logs... can be the most time consuming aspect of the CCTV enquiries with on average 1 minute of footage viewed and logged taking 1 hour of time'. We also observed technical challenges associated with viewing CCTV. Notably, detectives were often unable to view CCTV that had been downloaded by the local authority or commercial premises. In other investigations, we observed CCTV officers struggling to capture still images of suspects. All of these examples resulted in duplication of time and effort in order to try to resolve the difficulties.

Sharing CCTV footage with colleagues presented difficulties during some investigations. For example, during the investigation of a murder outside a nightclub, a CCTV officer attended and identified footage of the fatal assault. In an effort to share time-critical information quickly, the CCTV officer used WhatsApp on his own mobile device in order to capture a video of the footage and disseminate it to colleagues. Similarly, during our observations of a barrister's case conference, the CCTV officer was unable to share footage with the barrister because it would not play on the available laptops. Instead, he shared photographs taken from viewable footage and images from a WhatsApp group that had been used in the early days of the investigation. All of these dubious practices degraded the quality of the images that ultimately were shared and potentially impacted investigative lines of enquiry.

Interpreting, Comparing and Enhancing CCTV Footage

Poor-quality CCTV images (i.e. that are blurry or grainy) present particular challenges of interpretation and comparison and we observed, on many occasions, detectives and CCTV officers trying to make sense of poor-quality images. In one case, a male was found deceased inside his cottage. CCTV of the exterior of the property was recovered but it was of poor-quality and did not reveal any signs of activity around the cottage on the night when the victim was thought to have died. Consequently, detectives concluded that the deceased had likely committed suicide. This (mis)interpretation impacted the course of the investigation for some time. Following concerns about the mode of the death raised by the forensic scientist, the CCTV was examined by external experts, who enhanced the footage and identified faint light activity at the front door, during the night in question, indicative of it having been opened. Ultimately, this activity was linked to the suspect entering the property and fatally wounding the victim.

We also observed misinterpretations during attempts to identify suspects using comparison methods. During the investigation of a murder outside a nightclub (following which, the suspect fled), witnesses named the killer as Samuel. Detectives compared CCTV images from inside the club and of the lethal assault, with custody and open source images, combined with police-held intelligence, and identified a potential suspect (named Samuel), who they subsequently arrested. Further enquiries revealed that detectives had identified the wrong Samuel. The SIO explained how this misidentification had arisen:

I think the lighting [gave] a slightly false impression of what people look like... When you compare CCTV from a club and from a street in the night time with images from social media, Facebook profiles and with custody imaging that's been taken in the police station when people are arrested, clearly the lighting is different and you are making a comparison between those images... you've found somebody

who is called Samuel... we said "I think that's him" and we arrested the first Samuel and it wasn't him. (SIO, Operation W10).

Poor-quality CCTV footage also presents a dilemma for detectives who must decide whether to try to enhance it. Sometimes this enhancement is successful, as illustrated previously. However, in other instances it fails. In one of the cases that we observed, a fatal street stabbing was caught on CCTV. However, despite efforts to enhance it, the footage was too grainy to identify the attacker. In a few instances, detectives decided not to enhance CCTV footage. For example, during one investigation, officers seized a suspect's coat that appeared to be a different colour to that seen on CCTV. The detective minimised this discrepancy suggesting that the poor-quality image might be misleading. He decided against expert input on the ground that he was confident police had identified the right suspect:

It's not a great image... we had loads of trouble with the CCTV, the light changes. They were talking about getting an expert, I thought, well sod it, we know it's him, let's not... (Detective, Operation W12).

No clear guidance or formula exist for detectives to decide whether and when to pursue expert advice or to attempt the enhancement of CCTV footage. Nevertheless, the decisions made can have important implications for how an investigation unfolds and, ultimately, the credence that can, and should, be afforded to this footage.

Expert Viewers and Interpreters

Some detectives or CCTV officers were utilised repeatedly to view or interpret CCTV because they were regarded by others (or assigned themselves) as having a particular skill or expertise for viewing and interpreting footage. Various terms were used across police services to describe these experts including *super-user*, *super-recogniser* and

super-viewer. Their expertise was valued particularly when the CCTV footage was of poor-quality, for example, a CCTV officer explained:

What you quickly find if people have got the aptitude for it is they become a *super-recogniser*. They might be watching this camera, and when you see the quality, it isn't brilliant, but they would be able to work out that that person who is just running off down there was this person down here because they could recognise his footwear and his jacket. (CCTV officer, Operation E01).

Further research is required to understand whether there are individuals who possess special skills for viewing or interpreting CCTV footage, and if so, how they have acquired this expertise and whether they can provide expert evidence. Currently, it is not clear what such expertise is, on what basis super-recognisers may be considered expert (e.g. via training or experience) or the limits of their expertise. In the absence of such research, there are risks associated with how others perceive, understand and give credence to the role and expertise of super-recognisers or super-viewers.

During some homicide investigations, external experts were recruited to help to interpret CCTV footage, with varying outcomes. For example, in Operation E01, a gang-related shooting, an expert provided an assessment of a gunman's height but the methodology employed was subsequently discredited by the police and their evidence not used. In this same case, a second expert compared the gait of one of the gunmen seen on CCTV with footage of a suspect in custody. However, the police again did not deem the evidence reliable and the expert was not called to give evidence. In another case, gait analysis evidence was accepted. In a landscape where there are no accredited providers currently able to scientifically or reliably interpret or compare CCTV footage (Tully 2020), experts are unable to provide assurances that they have used a properly validated method or to report results whilst clearly articulating uncertainty of measurement or the limitations of evidence.

Some SIOs relied upon processes that lacked robustness in order to select external experts. Often, experts were selected from a list held (but not endorsed) by the National Crime Agency. The police then undertook further research to try to establish the credibility of these experts, including speaking with officers in other police services who had used them previously. SIOs and other investigators were generally swayed by how reliable these experts appeared and whether a conviction had been secured previously. For example, one CCTV officer explained:

I did speak to an officer from another force who said they had used [this expert] and he seemed fine, and his evidence was boring but seemed credible and they got a conviction. And you think “okay we will give it a go”. (CCTV officer, Operation E01).

How well an expert appears to present in court and/or whether they happened to give evidence in a case where the defendant was convicted, do not necessarily speak to the quality or robustness of the evidence provided by the expert.

Packaging CCTV Footage

Lastly, there are challenges and risks associated with how CCTV footage is packaged (and ultimately presented) for court. Whilst all of the processes that we have described thus far are part of the (social) construction of CCTV evidence, this final phase in the investigative trajectory is perhaps especially amenable to manipulation. Due to the volume of footage seized, CCTV officers made decisions (often in conjunction with prosecution actors) about which images to include and exclude for court. Images were usually pulled together to form a chronological narrative of events (often using coloured arrows or circles, superimposed onto the footage, to highlight defendants, their movements and actions). The overall objective in creating such packages was to tell a compelling story to the jury that supported the prosecution case. To illustrate, following

a domestic homicide, in which the suspect fled, the CCTV officer explained how footage was compiled and packaged in such a way as to show the defendant's state of mind and invite observers to infer that the defendant had taken medication *after* killing his wife, not before, thereby negating the legal defence to unlawful homicide of loss of control:

We actually tracked him, nearly all the time that he was missing for that nine hours... he was just wandering around... it just showed his demeanour and that he got more and more unsteady on his feet, which we believe was from the intoxication. The toxicology couldn't prove that for us, but the CCTV gave that inference that the jury could probably safely make that he'd actually taken a lot of medication that morning, not the night before. (SIO, Operation E02).

In another example, three male youths confronted and stabbed a young male outside a university building. The CCTV officer explained how he compiled footage to try to demonstrate that the suspect group had been searching for the victim, and not the other way round, as the defence argued:

[The suspect group] said they were just standing there... not really worried about who was coming and going. But the way we presented the case was that that wasn't the case. They were searching for these boys. They were looking everywhere... it was obvious, it was obvious to me and anyone else that looked at the CCTV that that's what they were doing. (CCTV officer, Operation W13).

The carefully choreographed footage and narrative enabled the prosecution to argue that the attack was pre-planned and had stemmed from existing tensions between the victim and suspect group. Whether or not these kinds of characterisations of suspects can truly be seen in CCTV footage is debatable. Nonetheless, detectives and barristers are becoming adept at selecting, organising and editing often hundreds of hours of footage into slick sets of packages enveloped within a narrative to support the prosecution case. In these ways, they socially construct the meaning of the footage, and,

as in other forensic disciplines, transform the results into ‘legally meaningful evidence’ (Kruse 2016, p. 16).

Discussion and Conclusion

Drawing upon quantitative data, our study reveals that CCTV played an integral role in helping to solve the homicides that we studied. Of all of the FSTs utilised, CCTV was used most frequently to both identify and charge suspects (albeit in combination with other intelligence or evidence, such as witness accounts, phone data and DNA).

Acknowledging the aforementioned limitations of the study, we are unable to generalize our findings to all British homicide investigations or police services. However, given the depth of our data, which was gathered from four distinct police services, and the diverse homicides and investigations that we studied, we have no reason to believe that our findings are not of relevance to many British police services investigating homicide.

Our findings suggest that in contrast with earlier studies by Roycroft (2007) and McEwan and Regoeczi (2015), CCTV has become a prominent feature of homicide investigations in Britain. There may be a number of reasons for this. For example, detectives may pursue CCTV inquiries more often because of the widespread coverage of CCTV in Britain and growing assumptions about its potential value to investigations, or because findings from CCTV may emerge more quickly than results from other FSTs or because, as several detectives told us, CCTV is perceived as a cheaper option than wet forensics. Certainly, CCTV, like house-to-house, is a standard line of enquiry on virtually every homicide investigation and is treated as a high priority action (Cook 2019, p. 221).

Drawing upon qualitative data, our findings advance knowledge and understanding of how precisely CCTV contributes to homicide investigations. Our data

reveal how investigators use CCTV frequently to identify and implicate suspects and to inform charging decisions, amongst other benefits. These findings build upon prior studies that suggest CCTV may improve clearance rates for particular crimes (Jung and Wheeler 2019, Morgan and Dowling 2019, Gerell 2020), and the scarce prior academic research on the benefits of CCTV to homicide investigation (Roycroft 2007) or criminal investigation more broadly (e.g. Gill and Spriggs 2005, La Vigne *et al.* 2011), as well as studies undertaken on the rail networks (e.g. Ashby 2017). Several of these benefits enable actors to pursue investigative or forensic lines of enquiry around source and activity, demonstrating who, what, when, where and how (Milliet *et al.* 2014).

Despite the prominence of CCTV as an investigative tool during homicide investigations, our ethnographic insights reveal the many challenges inherent in CCTV work. Even seemingly simple tasks, such as recovering, logging and sharing CCTV, are beset with difficulties and it is perhaps unsurprising that detectives have sometimes found their own solutions to these challenges or simply had to concede defeat. Our findings also illustrate the ways in which risky and unproven practices have evolved in the absence of organisational standards. Some detectives have gained reputations as *super-recognisers* or *super-viewers*, and some, arguably, have strayed beyond demonstrable expertise. Experts outside the policing fold, too, have assigned to themselves (or been assigned) expert status that is yet to be properly accredited.

Significantly, our research demonstrates that, despite some perceptions to the contrary among police, CCTV work is far from easy. In fact, we contend that the seemingly straightforward nature of CCTV work partly explains the lack of attention, nationally and locally, to training and the development of guidance and standards for this aspect of police work. Our findings empirically confirm concerns raised by Gerrard (2007) and, more recently, by Wilson-Kovacs (2019) and the Forensic Science

Regulator (Tully 2020), that processes and practices remain inadequate and ineffective. Importantly, the deficiencies that we observed are not new or unique to the UK. Rather, as Edmond (2010, p. 53) observed over a decade ago in Australia: ‘We do not know whether police officers, investigators and even *experts* can reliably produce the kinds of *identifications* that courts allow them to make. We do not know if their techniques are valid or reliable ... [or] the rates of error involved’. Our findings demonstrate that the situation now, is much the same as it was in 2010. Our findings also illustrate the socially constructed nature of CCTV evidence, highlighting the multiple social processes that are enacted to produce it, each of which shape the final product. CCTV evidence, like photographic evidence, elicits ‘a strong sense of objectivity’ and can be particularly persuasive (Porter and Kennedy, 2012, p.185-188) though, as we have hopefully demonstrated, using and making sense of CCTV is far more complex and subjective than might be presumed.

The extent to which the challenges that we encountered during CCTV enquiries directly impact the outcomes of investigations is difficult to determine. Certainly in some investigations, seemingly important footage was never recovered. These investigations may have faltered and become more costly, but were, nevertheless, still successfully resolved due to other compelling evidence. Further research is required to assess whether and how the kind of difficulties that we observed can contribute to investigative failure (given that we only studied successful investigations). What is clearer is that current practices are compromising the *integrity* of CCTV evidence and, we suggest, the full potential of CCTV evidence is not always realised.

Homicide investigations are often complex, high-pressured and resource intensive endeavours. CCTV inquiries are one amongst many investigative lines of enquiry that happen in tandem, and SIOs often have to juggle competing demands for

limited resources (see Brookman *et al.* 2019). Nevertheless, the challenges that we encountered are not inevitable and there are various ways to improve existing process and practice, which could offer the potential to identify and charge more suspects expeditiously whilst retaining the integrity of this form of evidence.⁹ One obvious avenue is the development of nationally accredited standards (overseen by the FSR) and training programmes (e.g. by the College of Policing) to equip new police recruits, as well as existing patrol officers, detectives and CCTV officers, with the knowledge and skills to effectively and appropriately recover, provenance and share CCTV footage without undermining the integrity of the footage. This also necessitates investment in equipment and technology. Currently, a few police services across the UK are developing their own training programmes, with some also establishing working groups, to tackle the challenges raised in this paper. However, this ad hoc, uncoordinated approach is leading to disparate practices and standards. Increased awareness of the challenge and risks associated with viewing, comparing and interpreting CCTV is, we feel, a further priority. CCTV footage is often grainy invariably lacks audio, and often lends itself to competing interpretations. Of particular concern are the risks associated with misinterpreting footage and/or misidentifying suspects. Those tasked with identifying people or things (e.g. suspects, vehicles, clothing or weapons) must be better able to demonstrate and articulate both the methods by which they reach conclusions and the strength and limitations of their expertise.

⁹ For a fuller list of recommendations for practitioners and policy-makers, refer to Brookman *et al.*, 2020. *HIFS Project Research Insight 3: The Use of CCTV during Homicide Investigations: Contributions, Challenges and Risks* [online]. Available from: <https://criminology.research.southwales.ac.uk/cirn/journals-and-publications/>.

Similarly, a transparent approach to how CCTV footage is packaged for court by CCTV officers or experts would be beneficial. After all, detectives (often in conjunction with prosecutors) purposively select, organise and edit many hundreds of hours of footage to arrange suspects, victims and events into a compelling and ordered storyline to present to the jury. At times, they turn ambiguities to their advantage and, presently, there is limited scope to challenge these processes in a meaningful way, given the lack of nationally adopted standards guiding their work (Tully 2020).

Ultimately, criminal justice actors transform findings from a range of forensic disciplines into legally meaningful evidence for court (see Brookman *et al.* 2020). However, the police are involved more directly and exclusively in the construction of some kinds of evidence than others – and CCTV is one such example.¹⁰ Police decide whether and how footage is retrieved, viewed, interpreted, enhanced and (with prosecutors) how it is packaged and presented at court. The socially constructed nature of this form of evidence is, we suggest, less amenable to scrutiny than evidence that is co-produced (e.g. between forensic scientists and police). Compared to other forensic evidence, that obtained from CCTV is neither accredited, nor peer-reviewed or quality assured independently. Whilst the digital forensic landscape in the UK is not quite the Wild West, practitioner-driven enterprise described by Sloan (2015), there is little doubt that there is scope to elevate standards and practices to those adopted in other forensic science disciplines. All of our proposed improvements to standards and practices,

¹⁰ Fingerprint examination is perhaps another example since the retrieval of marks are undertaken by police employees. Nevertheless, in contrast with CCTV, reporting fingerprint examiners have undertaken training, their work is peer reviewed and the majority of police fingerprint comparison bureaux have achieved accreditation (Tully 2020).

require organisational investment and effort, and the recognition within policing that current processes, if properly scrutinised, are vulnerable to successful challenge by defendants and defence counsel.

In conclusion, our findings suggest that currently, the integrity and provenance of CCTV evidence can be compromised easily due to inadequate systems, processes and practices at each stage in the life cycle of CCTV traces (i.e. from its initial recovery through to presentation at court). The challenges and risks identified in our research are likely to be exacerbated as digital technologies advance. For example, some police services in Britain are now using automated facial recognition technologies to identify suspects without robust independent evaluations of their effectiveness (see Davies *et al.* 2018 as an exception).¹¹ Equally, there are concerns about the ability of police to recognise and identify the purposeful manipulation of video footage through digital manipulation technologies such as Deepfake (Maras and Alexandrou 2019) or how to properly handle and provenance live stream video provided by members of the public (personal communication, National CCTV working group). These concerns are a timely reminder of how the pace of technological change moves more rapidly than the ability of police and the criminal justice system (CJS) to keep abreast of, and understand, its potentials or pitfalls. CCTV evidence, then, provides a glaring example of a forensic technology that is posing challenges for the CJS (Cole 2017). Given the prominence of CCTV in homicide investigation, and the grave implications of investigative errors, it is time for the CJS to acknowledge the socially constructed nature of CCTV evidence and guard against its misuse.

¹¹ In August 2020, the Court of Appeal ruled that use of Live Automated Facial Recognition technology by South Wales Police was unlawful ([2020] EWCA Civ 1058).

We would like to thank the anonymous reviewers for their helpful comments. The paper is based upon research that was funded by a Leverhulme Trust Grant and which involved Professor Robin Williams (Faculty of Health and Life Sciences, Northumbria University and School of Applied Social Sciences, Durham University) and Professor Jim Fraser (Centre for Forensic Science, University of Strathclyde). The authors wish to thank the Trust for the opportunity to undertake this research. The authors extend their gratitude to all of the detectives; police staff; forensic scientists; crime scene managers and coordinators; forensic accounts, submissions, and budget managers; prosecutors; judges; and other specialists within and beyond the criminal justice system who kindly gave up their time to take part in the research. We are also grateful to Dr Gill Tully, Forensic Science Regulator, for her insights on a draft of our CCTV Insight Briefing Paper and for meeting with us on several occasions to discuss the challenges of digital forensic evidence.

References

Ashby, M.P.J., 2017. The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research*, 23 (3), 441-459.

Brady, P.Q., and King, W.R., 2017. Technology and homicide investigation. In: F. Brookman, E.R. Maguire, and M. Maguire, ed. *The handbook of homicide*. Chichester: Wiley Blackwell, 517-532.

Braun, V., and Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77-101.

British Society of Criminology, 2015. *British Society of Criminology statement of ethics* [online]. Available from: <https://www.britisoccrim.org/documents/BSCEthics2015.pdf> [Accessed 29 October 2015].

- Brookman, F., 2015. Researching homicide suspects, offenses and detectives using qualitative methods. *In: H. Copes, and J. Mitchell Miller, eds. The Routledge handbook of qualitative criminology*. London: Routledge, 236-252.
- Brookman, F., and Innes, M., 2013. The problem of success: What is a “good” homicide investigation? *Policing and Society: An International Journal of Research and Policy*, 23, 292-310.
- Brookman, F., *et al.*, 2020. Dead reckoning: Unravelling how “homicide” cases travel from crime scene to court using qualitative research methods. *Homicide Studies* [online]. Available from: <https://doi.org/10.1177/1088767920907374> [Accessed 26 June 2020].
- Brookman, F., Maguire, E., and Maguire, M., 2019. What factors influence whether homicide cases are solved? Insights from qualitative research with detectives in Great Britain and the USA. *Homicide Studies*, 23 (2), 145-174.
- Casey, E., 2019a. Editorial. Trust in digital evidence. *Forensic Science International: Digital Investigation*, 31, 200898.
- Casey, E., 2019b. The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences*, 51 (6), 649-664.
- Cole, S.A., 2017. Changed science statutes: Can courts accommodate accelerating forensic scientific and technological change? *Jurimetrics*, 57 (4), 443–458.
- Cole, S.A., and Bertenthal, A., 2017. Science, technology, society, and law. *Annual Review of Law and Social Science*, 13 (1), 351-371.
- College of Policing, 2020. *Investigation. Passive data generators* [online]. Available from: <https://www.app.college.police.uk/app-content/investigations/investigative-strategies/passive-data-generators/#:~:text=Investigation->

,Passive%20data%20generators,can%20be%20accessed%20by%20investigators
&text=financial%20information,-CCTV [Accessed 8 June 2020].

Cook, T., 2019. *Blackstone's senior investigating officers' handbook*. 5th ed. Oxford, England: Oxford University Press.

Corbin, J., and Strauss, A., 2008. *Basics of Qualitative Research*. 3rd ed. Los Angeles, California: SAGE.

Davies, B., Innes, M., and Dawson, A., 2018. *An evaluation of South Wales Police's use of automated facial recognition*. Cardiff: UPSI.

Dowling, C., et al., 2019. How do police use CCTV footage in criminal investigations? *Trends and Issues in Crime and Criminal Justice*, 575, 1-15.

Edmond, G., 2010. Impartiality, efficiency or reliability? A critical response to expert evidence law and procedure in Australia. *Australian Journal of Forensic Sciences*, 42 (2), 83-99.

Edmond, G., 2013. Just truth? Carefully applying history, philosophy and sociology of science to the forensic use of CCTV images. *Studies in History and Philosophy of Science Part C: Studies in History and Philosophy of Biological and Biomedical Sciences*, 44 (1), 80-91.

Evison, M.P., 2015. The third forensics - images and allusions. *Policing and Society*, 25 (5), 521-539.

[2020] EWCA Civ 1058 [online]. Available from: <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> [Accessed 30 November 2020].

Forensic Science Regulator, 2016. *Forensic image comparison and interpretation evidence: Guidance for prosecutors and investigators. Issue 2* [online]. Available from:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/511168/Image_Comparison_and_Interpretation_Guidance_Issue_2.pdf [Accessed 5 June 2020].

- Geertz, C., 1973. *The interpretation of cultures: Selected essays*. New York: Basic Books.
- Gerell, M., 2020. CCTV in deprived neighbourhoods – a short-time follow-up of effects on crime and crime clearance. *Nordic Journal of Criminology*. DOI: 10.1080/2578983X.2020.1816023 [Accessed 30 November 2020].
- Gerrard, G., 2007. CCTV and major incident investigation: Professionalising the police approach. *The Journal of Homicide and Major Incident Investigation*, 3 (2), 7-20.
- Gill, M., and Spriggs, A., 2005. *Assessing the impact of CCTV. Home Office research study 292* [online]. Available from: https://techfak.uni-bielefeld.de/~iluetkeb/2006/surveillance/paper/social_effect/CCTV_report.pdf [Accessed 3 June 2020].
- Goodwin, C., 1994. Professional vision. *American Anthropologist*, 96, 606-633.
- Hadjimatheou, K., 2017. Surveillance technologies, wrongful criminalisation, and the presumption of innocence. *Philosophy & Technology*, 30, 39-54.
- Hak, J., 2019. Evaluation of the Forensic Science Regulator's recommendations regarding image comparison evidence. *Forensic Science International: Synergy*, 1, 294-297.
- Home Office, Association of Police and Crime Commissioners, and National Police Chiefs' Council, 2018. *Forensics review. Review of the provision of forensic science to the criminal justice system in England and Wales* [online]. Available from: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/atta>

chment_data/file/800447/Joint-review-of-forensics-provision-July-2018.pdf
[Accessed 30 April 2019].

House of Lords Science and Technology Select Committee, 2019. *Forensic science and the criminal justice system: A blueprint for change* [online]. Available from: <https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf>
[Accessed 2 May 2019].

Jasanoff, S., 2006. Just evidence: The limits of science in the legal process. *The Journal of Law, Medicine & Ethics*, 34, 328-341.

Jung, Y., and Wheeler, A.P. 2019. *The effect of public surveillance cameras on crime clearance rates* [online]. Available from: <https://osf.io/preprints/socarxiv/eh5bg/>
[Accessed 30 November 2020].

Kim, S., 2016. Alternative truths: The construction of narratives in the Rodney King trial. *Elements*, 12 (2), 83-96.

Kruse, C., 2016. *The social life of forensic evidence*. Oakland, CA: California University.

La Vigne, N.G., et al., 2011. *Evaluating the use of public surveillance cameras for crime control and prevention* [online]. Available from: https://www.urban.org/sites/default/files/publication/27556/412403-evaluating-the-use-of-public-surveillance-cameras-for-crime-control-and-prevention_1.pdf
[Accessed 4 June 2020].

Levesley, T., and Martin, A. 2005. *Police attitudes to and use of CCTV. Home Office Online Report 09/05* [online]. Available from: <https://webarchive.nationalarchives.gov.uk/20110218141420/http://rds.homeoffice.gov.uk/rds/pdfs05/rdsolr0905.pdf> [Accessed 29 May 2020].

Lynch, M., et al., 2008. *Truth machine: The contentious history of DNA fingerprinting*. Chicago, Illinois: Chicago University.

- Maras, M-H., and Alexandrou, A., 2019. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof*, 23 (3), 255-262.
- McCartney, C., 2018. Commentary: Disclosure in the criminal justice system. *Journal of Forensic and Legal Medicine*, 58, 72-73.
- McEwan, T., and Regoeczi, W., 2015. Forensic evidence in homicide investigations and prosecutions. *Journal of Forensic Sciences*, 60 (5), 1188-1198.
- Milliet, Q., Delemont, O., and Margot, P., 2014. A forensic science perspective on the role of images in crime investigation and reconstruction. *Science & Justice*, 54 (6), 470-480.
- Morgan, A., and Dowlng, C., 2019. Does CCTV help police solve crime? *Trends and Issues in Crime and Criminal Justice*, 576, 1-16.
- Morgan, N. *et al.*, 2020. *Trends and drivers of homicide: Main findings data tables* [online]. Available from: <https://www.gov.uk/government/publications/trends-and-drivers-of-homicide-main-findings> [Accessed 4 December 2020].
- Piza, E.L., 2018. The history, policy implications, and knowledge gaps of the CCTV literature: Insights for the development of body-worn video camera research. *International Criminal Justice Review*, April 2018, 1-21.
- Piza, E.L., *et al.*, 2019. CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18, 135-159.
- Police Foundation, 2014. *The briefing – CCTV* [online]. Available from: <http://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/cctv.pdf> [Accessed 30 November 2020].

- Porter, G., 2007. Visual culture in forensic science. *Australian Journal of Forensic Sciences*, 39 (2), 81-91.
- Porter, G., 2012. Zak Coronial Inquest and the interpretation of photographic evidence. *Current Issues in Criminal Justice*, 24 (1), 39-49.
- Porter, G., and Kennedy, M., 2012. Photographic truth and evidence. *Australian Journal of Forensic Science*, 44 (2), 183-192.
- Robin, L., Peterson, B.E., and Lawrence, D.S. 2020. How do close-circuit television cameras impact crime and clearances? An evaluation of the Milwaukee police department's public surveillance system. *Police Practice and Research*, DOI: 10.1080/15614263.2020.1772783.
- Roycroft, M., 2007. What solves hard to solve murders? Identifying the solving factors for Category A and Category B murders. Does the SIO's decision making make a difference? *Journal of Homicide and Major Incident Investigation*, 3 (1), 93-107.
- Scottish Government, 2020. *Homicide in Scotland 2019-2020: Statistics* [online]. Available from: <https://www.gov.scot/publications/homicide-scotland-2019-2020/> [Accessed 4 December 2020].
- Sloan, J.J., 2015. *There's no code of ethics to govern digital forensics –and we need one* [online]. Available from: <https://theconversation.com/theres-no-code-of-ethics-to-governdigital-forensics-and-we-need-one-45755> [Accessed 26 June 2020].
- Smit, N.M., Morgan, R.M., and Lagnado, D.A., 2018. A systematic analysis of misleading evidence in unsafe rulings in England and Wales. *Science & Justice*, 58 (2), 128-137.
- Stelfox, P., 2009. *Criminal investigation. An introduction to principles and practice*. Cullompton: Willan.

Sunde, N., and Dror, I.E., 2019. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, 29, 101-108.

Surveillance Camera Commissioner, 2016. *Surveillance Camera Commissioner's IFSEC speech* [online]. Available from: <https://www.gov.uk/government/speeches/surveillance-camera-commissioners-ifsec-speech> [Accessed 28 May 2020].

Surveillance Camera Commissioner, 2017. *A national surveillance camera strategy for England and Wales* [online]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/608818/NSCS_Strategy_post_consultation.pdf [Accessed 28 May 2020].

Tully, G., 2020. *Forensic Science Regulator Annual Report 17 Nov 2018 - 16 Nov 2019* [online]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/877607/20200225_FSR_Annual_Report_2019_Final.pdf [Accessed 25 February 2020].

Tully, G., and Stockdale, M., 2019. Commentary on: Hak. Evaluation of the Forensic Science Regulator's recommendations regarding image comparison evidence. *Forensic Science International: Synergy*, 1, 298-301.

Tully, G., *et al.*, 2020. Quality standards for digital forensics: Learning from experience in England & Wales. *Forensic Science International: Digital Investigation*, 32, 200905.

Vincze, E.A., 2016. Challenges in digital forensics. *Police Practice and Research: An International Journal*, 17 (2), 183-194.

Wilson-Kovacs, D., 2019. Effective resource management in digital forensics. An exploratory analysis of triage practices in four English constabularies. *Policing: An International Journal*, 43 (1), 77-90.

Appendix

Table A1. NVivo CCTV Nodes

NVivo Node	Description
CCTV Advancements and keeping up	The challenges of keeping up-to-date with advancements in CCTV technology – either examples of or discussions about
CCTV Enhancement	Instances where officers are discussing enhancing CCTV or have enhanced CCTV
CCTV Identifying, Recovery and Download	Any material related to identifying, recovering/seizing and downloading CCTV footage (good or bad)
CCTV Integrity and Provenance	Where officers or others have raised issues about trying to ensure the integrity/provenance of CCTV and/or issues raised about whether CCTV has integrity or provenance
CCTV Packages or reports	Packages or reports produced by CCTV officers or others relating to CCTV footage. Includes discussions about these packages and reports
CCTV Presentation for court	Pre-court discussions about how CCTV footage might be presented at court or to the jury
CCTV Quality	Any material that discusses the quality of CCTV footage – this includes officers and others discussing poor quality footage and references to good quality
CCTV Relevance or Value	How and why CCTV is of use/relevance/importance to homicide investigations. For example, it 'shows' movements of suspect(s), victims or witnesses; identifies other CCTV footage; links suspects to areas; informs the forensic strategy or phone work; helps to refute a witness or suspect
CCTV Resource issues	Challenges of resourcing CCTV enquiries - having staff to identify, recover, seize or view footage
CCTV Sharing footage	How CCTV is shared between officers and any challenges associated with this
CCTV Staffing, logistics and training	How staff are assigned/designated to work on CCTV and any issues related to their training
CCTV Strategy	References to CCTV strategies/decisions of any kind up until the point of trial
CCTV Super recognisers or special skills	Any references to the notion that some detectives have particular skills in viewing CCTV and 'finding' relevant people or things. Or any discussion about this notion
CCTV Viewing and Interpreting	Any material relating to whether and how CCTV is viewed and interpreted, understood or made sense of, and the challenges that this brings

