University of South Wales
Prifysgol De Cymru

LEVERHULME TRUST

RESEARCH INSIGHT

The Use of CCTV during Homicide Investigations: Contributions, Challenges and Risks

Professor Fiona Brookman, Dr Helen Jones, Professor Robin Williams and Professor Jim Fraser

This is one of a series of Briefing Papers based on research findings from the Homicide Investigation and Forensic Science (HIFS) Project.

Prof. Fiona Brookman and Dr Helen Jones,
Centre for Criminology,
University of South Wales,
Treforest Campus,
Pontypridd,
CF37 1DL

Fiona.brookman@southwales.ac.uk

Helen.jones11@southwales.ac.uk

criminology.research.southwales.ac.uk/cirn/

Acknowledgements: We are grateful to The Leverhulme Trust who funded this research and indebted to all of the detectives, forensic scientists and other experts who took part. We are also grateful to Dr Gill Tully, Forensic Science Regulator, who kindly responded to an earlier version of this paper.

Research Insight 3: April 2020

Introduction and Background

This research insight paper draws upon data from the Homicide Investigation and Forensic Science (HIFS) Project (details overleaf). It focuses principally on the use of CCTV in homicide investigations not least because CCTV was a prominent feature of nearly all of the investigations that we studied but also because of the complexities that arise in recovering, viewing, interpreting, 'packaging' and presenting CCTV footage.[1]

> In 42 of the 44 homicide cases studied, CCTV featured in the investigation in some capacity, for example, to identify offenders, to inform charging decisions and to support the prosecution case.

Amongst the many challenges of making use of CCTV during the investigation of homicide are: managing the sheer volume of data that enters an investigation; the difficulties of interrogating the evidence in a timely manner;[2] and risks associated with the analysis and comparison of CCTV footage.[3] Casey (2019: 1) notes that "[a]s reliance on digital evidence rises in all kinds of legal disputes, the risks of mishandling, misinterpretation, misunderstanding, and manipulation are escalating. These risks intensify when personnel are poorly trained and scientific practices are disregarded".[4]

Within homicide investigations, a diverse range of actors 'handle' and try to make sense of CCTV, with varying levels of experience, skill and expertise. For example, whist digital experts complete specialist training in order to retrieve and enhance CCTV footage, and may provide expert witness evidence at court, CCTV officers or co-ordinators are invariably police staff or detectives, who may or may not have received specialist training but can be tasked to identify, recover and view footage, and create CCTV packages for suspect interviews, charging decisions and court. Forensic imaging technicians are trained to recover CCTV and produce electronic packages for court, and may also be able to enhance footage. Others who may also handle footage but with limited training include uniformed officers, senior investigating officers (SIOs) and intelligence analysts. If and how CCTV is recovered and interpreted depends upon the level of experience, skill and expertise of the individual undertaking the task.

[1] This briefing paper does not deal with disclosure challenges.
[2] House of Lords Science and Technology Select Committee (2019). Forensic science and the criminal justice system: a blueprint for change. https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf.
[3] Tully, G. (2020). Annual report. 17 November 2018 – 16 November 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868052/20200225_FSR_Annual_Report_2019_Final.pdf.
[4] Casey, E. (2019). Trust in digital evidence. Forensic Science International: Digital Investigation, 31, 1-2.

HIFS Study: Data and Methods

The HIFS Project was a four-year ethnographic study that explored how forensic sciences and technologies (FSTs) contribute to the police investigation of homicide in Great Britain. We adopt a broad and inclusive definition of FSTs, including, for example, DNA profiling, fingerprint examination, ballistics interpretation, trace evidence analysis, and digital evidence from mobile phones, computers and CCTV.

Four police services from across Great Britain and three major private forensic science providers participated in the project. We gathered in-depth data including: (1) case papers for 44 homicide investigations; (2) interviews with 144 SIOs, detectives, forensic scientists and other specialists; and (3) over 700 hours of observations of 11 'live' homicide investigations, during which the researchers entered crime scenes, accompanied detectives on house-to-house and CCTV enquiries, and attended daily briefings, forensic strategy meetings, barristers' case conferences and different stages of the trial process.

The 44 cases studied reflect a range of modus-operandi (sharp instrument, blunt instrument, strangulation/ asphyxiation, shooting and poisoning) and victim-offender relationship (partner/ex-partner, child-parent, parent-child, friend/acquaintance, other known and strangers). Our cases include those where suspects were identified very quickly through to complex, protracted investigations that were not resolved for many months or years.

The Contribution of CCTV to Homicide Investigation

Throughout the homicide investigation, detectives and other criminal justice actors use findings from a broad range of FSTs, as well as other sources of information, such as witness accounts, admissions by the offender and intelligence held on police-systems, to inform their sense-making and decision-making.[5] In 42 of the 44 homicide cases studied, CCTV featured in the investigation in some capacity, for example, to identify offenders, to inform charging decisions and to support the prosecution case.[6] Sources of CCTV included public and private cameras, such as public transport (e.g. buses), commercial premises, residential properties and dash cams in vehicles, plus police body worn cameras. We now consider in detail when and how CCTV was used to identify offenders and to inform charging decisions.

Across the 44 homicide cases studied, there were 62 offenders. Of these, one offender was never identified (or charged) and a second offender was identified but never charged. Charts 1 and 3 (below and opposite) reveal that 32 (of 61) offenders were identified and 51 (of 60) offenders were charged using findings from one or more FSTs (sometimes used in conjunction with other information, e.g. witness accounts or admissions).[7]

Alongside charts 1 and 3, charts 2 and 4 present when findings from CCTV and other most frequently used FSTs were used to identify[8] and charge homicide offenders.

Chart 1: Type of FST by number of offenders identified (n=32)

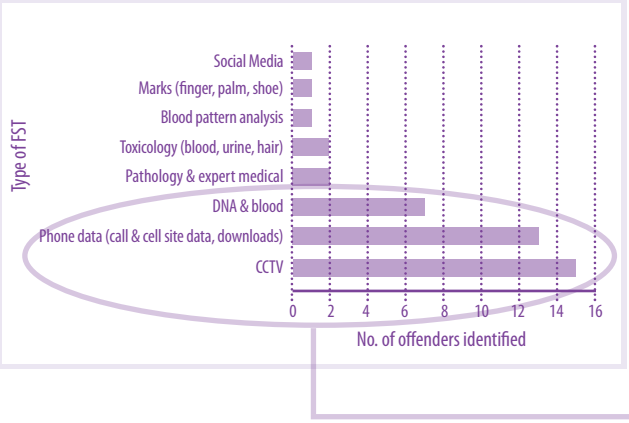
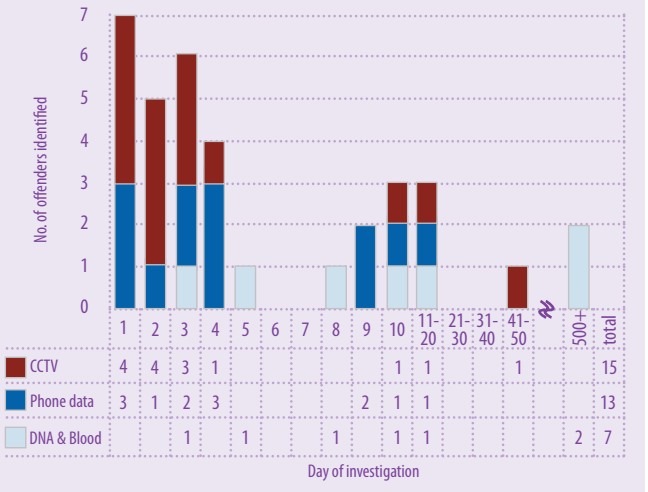


Chart 2: Number of offenders identified by day of investigation whether by CCTV, phone data and/or DNA



[5]For further detail, see HIFS Project Research Insight 2: The Role of Forensic Sciences and Technologies in Homicide Investigation in Britain, https://criminology.research.southwales.ac.uk/cirn/journals-and-publications/.

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

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

[8]In some instances, 'identification' includes implication, i.e. the offender was already 'known' to the police but findings from FSTs implicated them in the offence allowing SIOs to categorise them as a suspect.

Chart 3: Type of FST by number of offenders charged (n=51)

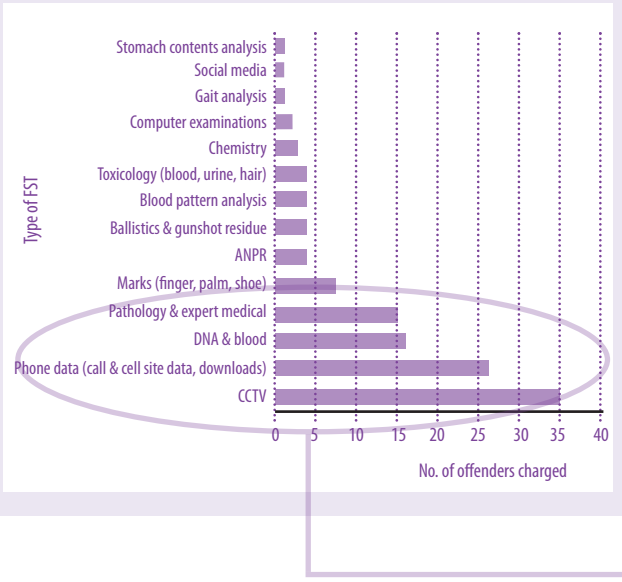
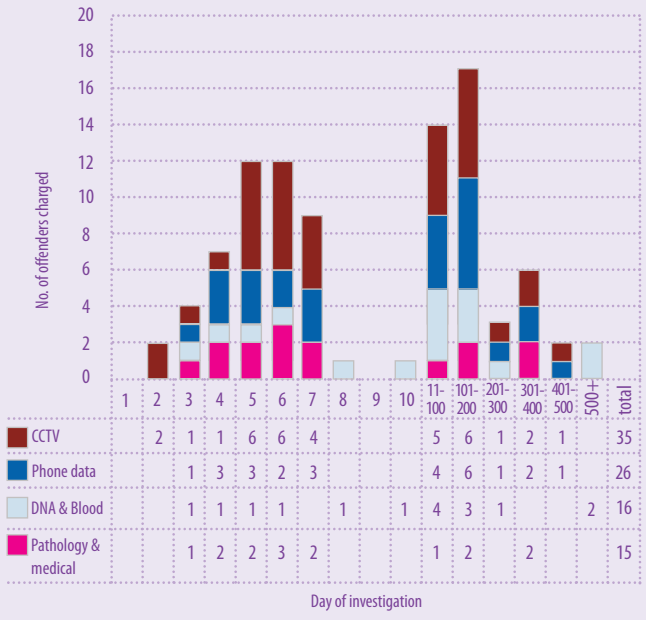


Chart 4: Number of offenders charged by day of investigation whether by CCTV, phone data, DNA and/or pathology



Using CCTV to Identify Offenders in Homicide Cases

Our data (illustrated in charts 1-4) reveal that of all the FSTs used to identify offenders, the most frequently used was CCTV, particularly within the first four days of an investigation. Twelve (of 61) offenders were identified via CCTV in the first four days of these 44 homicide investigations and a further three offenders were identified by CCTV later in the investigation. Put another way, almost one quarter of all homicide offenders (15 of 61) were identified by CCTV. However, in all but one instance, CCTV was combined with other intelligence or evidence (e.g. findings from other FSTs, witness accounts or suspect admissions) in order to identify offenders.

Data from mobile phones was also used frequently and just over one fifth of all homicide offenders were identified in part by phone data. Moreover, though not illustrated on the previous charts, 23 offenders were identified on the first day of the investigation without any information gathered from FSTs, i.e. they were identified solely through, for example, witness accounts or admissions from offenders.

How CCTV was used to Identify Homicide Offenders

Considering suspect identification in more detail, we explored the cases involving 15 offenders who were identified (either solely or in part) by CCTV (see charts 1 and 2). Our analysis revealed that CCTV played an 'important' role in two stranger homicides, enabling detectives to identify offenders. CCTV also played an important role in two homicide investigations where victims knew the offender in a 'customer-client' capacity, i.e. they only had limited knowledge of one another. In one case, CCTV helped detectives identify an offender and in the second case, CCTV images suggested that a young female who had been reported missing had been killed inside a shop by the proprietor (this proved to be the case). In all four of these cases, offenders pleaded guilty to murder or manslaughter. In all cases, there was corroborative evidence such as witness accounts, data from mobile phones, DNA and blood pattern analysis.

In other 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 offenders. The findings suggest that CCTV is used in many different ways to help to identify homicide suspects and implicate them in these offences.

Using CCTV to Inform Charging Decisions in Homicide Cases

Our data illustrate that of all the FSTs used to inform charging decisions, CCTV was used most frequently. Twenty (of 60) offenders were charged via CCTV in the first seven days of these 44 homicide investigations and ultimately, more than half of offenders (35 of 60) were charged by using evidence gleaned from CCTV footage. However, charging decisions were rarely based on CCTV footage alone – with the exception of one offender, decisions were based on CCTV combined with other forms of intelligence or evidence (e.g. findings from other FSTs, witness accounts or suspect admissions).

Other kinds of FSTs were also utilised regularly to inform charging decisions, including findings from phone data, DNA and blood, and pathology and medical expert reports. Finally, though not captured on the previous charts, two offenders were charged within the first day of each investigation based solely on admissions and witness accounts.

There are various possible reasons why CCTV 'stands out' amongst FSTs at these stages of investigations. For example, detectives may pursue CCTV enquiries more often or routinely than other activities, or the results from these enquiries may emerge more quickly than results from other FSTs (such as DNA interpretation, forensic pathology or toxicology).

Moreover, how often particular FSTs are used to identify or charge offenders does not (necessarily) reflect their 'value' or usefulness. For example, some SIOs and detectives cited findings from 'lesser used' FSTs as a decisive factor in identifying or charging an offender, for example, toxicological analysis of hair samples.

How CCTV Contributed to Homicide Investigations

Besides being used to identify and implicate suspects, CCTV footage afforded numerous benefits to homicide investigators. However, there are challenges associated with achieving these benefits, some of which present a potentially higher risk to the integrity of the investigation and/or prosecution than others, as illustrated in the two lists below:

Higher risk:

- Identify suspects and witnesses
- Implicate or eliminate suspects
- Link suspects to key exhibits (e.g. weapons, clothing, vehicles or mobile phones)
- Show movements and associations of, or between, victims and suspects
- Direct charging decisions
- Support prosecutions and/or refute defence arguments at court

Lower risk:

- Corroborate or refute accounts provided by suspects and witnesses
- Identify further investigative or forensic opportunities
- Target or focus other strategies (e.g. search, forensic or telecoms)
- Inform forensic scientists' or other experts' examinations and interpretations

CCTV Challenges

Our data illustrate many challenges associated with recovering, viewing, interpreting, 'packaging' and presenting CCTV footage, to which we now turn.

1. Recovery

(a) Inability to Recover CCTV Footage

Numerous detectives lacked the skills, training or technology to recover footage in a timely and efficient manner. For example, several detectives remarked that they had not received any specialist training and one police service identified a noticeable lack of training for officers who recover CCTV. In order to preserve the original CCTV footage (and for it to be made available to experts later), it must be retrieved in its native file format, from which a working copy is made. However, some detectives were ill equipped to recover CCTV footage in different formats. For example, at one premises, the officer needed a CD rather than a USB.

(b) Inaccessibility of CCTV Footage

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. On other occasions, the volume of CCTV requested was unmanageable or not achievable. For example, during our fieldwork, detectives were tasked to recover five hours' worth of CCTV footage from all buses that had driven past a flat where the deceased had been attacked. However, this was not possible because the period included 30 to 40 buses and each bus would have to be temporarily

taken out of service in order for the CCTV to be downloaded. In this instance, the deputy SIO reduced the time parameter to one hour, which was achievable for the bus company.

(c) Lack of Oversight and Co-ordination

Our research revealed instances where detectives who were co-ordinating, or engaged with, CCTV enquiries were removed from this task in order to assist with other lines of enquiry. This resulted in a lack of oversight of what CCTV had been identified and recovered. This was compounded by inadequate processes for logging CCTV enquiries, hampering the flow of information between detectives, uniformed officers and the major incident room (MIR). Consequently, we observed detectives on CCTV enquiries visiting premises that had previously been attended by police. Detectives were frustrated by this duplication of effort and time wastage, which sometimes delayed the identification and recovery of CCTV.

(d) Lost CCTV Footage

Failure to identify and recover CCTV footage in a timely manner can lead to the loss of potentially critical evidence as CCTV footage is recorded over before detectives are able to retrieve it. Some detectives spoke about the challenges of being able to identify 'mobile' CCTV users, such as lorry or tipper-truck drivers. In one case, 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 of the murder with potentially additional valuable dash cam footage. Nevertheless, this line of enquiry was not pursued. Later the owner of the lorry firm saw TV coverage of the shooting and contacted the police, by which time the footage was recorded over.

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 one case, CCTV was identified at an elderly couple's address who lived opposite a suspect. A detective attended but they 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 be without CCTV. The detective was assured that the device did not re-record for two weeks and in turn, assured the SIO. The SIO decided not to call a technician out at the weekend to assist and instead arranged that the technician attend on Monday, by which time the footage was overwritten.

2. 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 format. Nevertheless, this good practice was not universal and we heard about potentially risky evidence-handling practices. For example, some detectives and CCTV officers had purchased their own equipment in order to download footage more easily and quickly. New and emerging technologies (such as doorbell cameras) with cloud-based storage, also present new challenges and risks associated with how (native) footage is captured, retrieved and shared.

3. Viewing CCTV Footage

(a) Vast Volumes of Data

We repeatedly heard about the challenges associated with recovering vast volumes of CCTV and how resource-intensive it is for officers to view and log this footage. For example, an excerpt from the CCTV strategy for Operation N11[9] states, "[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".

(b) Technical Issues

There were also technical challenges associated with viewing CCTV. In one case, detectives were unable to view CCTV that had been downloaded by the local authority, explaining that this was a recurrent problem. In another case, we observed the CCTV officer repeatedly viewing footage in order to capture a still image of a suspect running up the street. On this occasion, the CCTV officer did not have the capability to pin-point frames or play frames at a faster or slower speed, which resulted in duplication of effort and time wastage.

4. Sharing CCTV Footage

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 this time-critical information quickly (the suspect had fled the scene), the CCTV officer used WhatsApp on their own mobile device in order to take 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 much of the footage with the barrister because it would not play on the available laptops. Instead, they shared (poor-quality) 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 practices degraded the quality of the images that were shared.

[9]Data related to homicide cases, offenders and research participants have been anonymised or given pseudonyms.

5. Interpreting and Comparing CCTV Footage

Poor-quality CCTV images (i.e. that are blurry or grainy) present particular challenges of interpretation and comparison. Our data reveal numerous examples of detectives and CCTV officers trying to make sense of poor-quality images during investigations. 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 that night, when the victim was thought to have died. Consequently, detectives felt that the deceased had most likely committed suicide. Initially, this (mis)interpretation framed the investigation. Following concerns raised by the forensic scientist, the CCTV was enhanced and experts identified faint light activity at the front door, during the night, suggesting that it had been opened. Ultimately, this activity was linked to the suspect entering the property and fatally wounding the victim.

Similar misinterpretations can occur when actors compare CCTV images against other images, for example, in order to identify a suspect. 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 arrested. Further enquiries revealed that detectives had identified the wrong 'Samuel'. The SIO explained that this misidentification had arisen because the lighting of the different images 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, Op. W10).

6. Enhancing CCTV Footage

Poor-quality CCTV footage also presents a dilemma for actors who must decide whether or not to try to enhance it. Our data suggest that detectives often assume that experts will be able to improve poor-quality images. Sometimes this enhancement is successful, as illustrated previously. However, in other instances it 'fails'. In one of the cases that we observed, a fatal stabbing was 'caught' on CCTV. However, despite efforts to enhance it, the footage was too grainy to identify clearly the attacker.

In a few instances, detectives decided not to enhance CCTV footage. Whilst further analysis and research is required to understand better how and why detectives make these decisions, the following example illuminates potentially risky decision-making. Officers seized a suspect's coat that appeared to be a different colour to that seen on CCTV. The detective sergeant (DS) minimised this discrepancy because of the poor-quality of the image and decided that an expert was not necessary because they felt they knew who the suspect was - "[i]t'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…" (DS, Op. W13).

7. 'Expert' Viewers and Interpreters

Some detectives or CCTV officers were drawn upon to help 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 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, "[w]hat 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, Op. E01).

Further research is required to understand better whether there are individuals who possess an enhanced level of skill for viewing or interpreting CCTV footage, and if so, how they have acquired this expertise and whether it can be evidenced. Currently, it is not clear what such expertise is, on what basis such 'super-recognisers' may be considered an 'expert' (e.g. via training or experience) or the limits of such expertise. In the absence of such evidence, there are risks associated with how others perceive and understand the role and expertise of super-recognisers or super-viewers. For example, colleagues may consider the identifications and interpretations made by super-recognisers or super-viewers to be more reliable than those made by other actors. Similarly, jurors may be more trusting of the evidence that super-recognisers or super-viewers give, especially if they are called by the court to give evidence as ad hoc expert witnesses. In these circumstances, the court must understand any limitations of evidence, for example, that a CCTV officer is a member of the investigation team and not an independent expert (whose duty is to the court).

Some homicide investigations also drew upon external experts to help interpret CCTV footage, for example, to provide an assessment of a suspect's height or gait. However, as the Forensic Science Regulator (Tully, 2020) has noted, there are risks associated with current practices

in a landscape where there are no accredited providers yet available to 'scientifically' or reliably interpret or compare CCTV footage. Notably, experts are unable to provide assurances that they have used a properly validated method and some are reporting results without clearly articulating uncertainty of measurement and limitations of evidence. Moreover, there are concerns that some experts may be straying beyond the limits of their knowledge or expertise.

8. Expert Selection

Some SIOs relied upon processes that lacked robustness in order to select external experts. Across a number of investigations, experts were selected from a list held (but not endorsed) by the National Crime Agency. The police then undertook further research around these experts, including speaking with officers in other police services who had previously used them. SIOs and other specialists (e.g. CCTV officers and crime scene managers) were generally swayed by how credible 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, Op. 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 evidence provided.

9. 'Packaging' and Presenting CCTV Footage

Lastly, there are challenges and risks associated with how CCTV footage is packaged for, and presented at, court. Due to the volume of footage seized, CCTV officers made decisions (often in conjunction with barristers) about which images to include and exclude for court. Images were usually pulled together to form a chronological narrative of events (often using different 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.[10] However, these practices are not without risk - they may be used to 'show' a defendant's mindset or could tell a potentially misleading story at court. There is also a risk that if the jury are told what they are 'seeing' from the footage, that they 'see' the same story.

To illustrate, following a domestic homicide, CCTV footage was gathered and presented to 'show' the defendant's state of mind, inferring that the defendant had taken medication *after* killing his wife and negating the legal defence of loss of control. In another example, a male was confronted and stabbed outside a university building by a group of three males. The CCTV officer explained how he had pulled footage together to tell a particular story, of how, prior to the stabbing, 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, W13).

Considerations and Recommendations

Opportunities exist to offset the risks associated with the retrieval and interpretation of CCTV footage:

- Detectives and CCTV officers require training and the appropriate technological equipment in order to be able to recover and view CCTV (in a range of formats) in a timely and efficient manner. Training ought to include best practice on how to retrieve and copy native footage
- During homicide investigations, SIOs could consider utilising leaflet drops to advise occupants and owners of premises that CCTV enquiries are being undertaken in the area
- At a national level, engagement with local authorities and industry may enable CCTV footage to be shared more efficiently and effectively
- To improve oversight and co-ordination of CCTV strategy, SIOs could prioritise, where possible, the continuity of staff undertaking CCTV enquiries
- SIOs could consider allocating the deputy SIO to manage and co-ordinate the CCTV strategy. Moreover, deputies require appropriate support from sergeants, with responsibility for teams of officers and technicians who (i) identify and retrieve footage and (ii) view footage.
- Results from CCTV enquiries ought to be logged appropriately and consistently, and shared promptly with the MIR
- Police services ought to ensure that frontline uniformed officers and detectives have the capability to share time-critical CCTV without threatening the integrity of the footage
- National standardised procedures, complemented with appropriate training, may help to ensure that the recovery and interpretation of CCTV footage is undertaken in a manner that preserves its integrity and provenance

[10]Brookman, F. and Jones, H. (2017). The narrative for the prosecution. Paper presented at the American Society of Criminology, Philadelphia.

- Experts who interpret and compare CCTV footage ought to be able to demonstrate their use of properly validated methods and have appropriate quality standards in place
- Experts who interpret and compare CCTV ought to understand and articulate both the strength and limitations of their expertise
- The National Crime Agency could consider developing a more robust process to assist SIOs when selecting external experts
- Consideration could be given to improving the transparency of how CCTV footage is packaged for, and presented at, court by CCTV officers or experts

Conclusion

Drawing upon quantitative data gathered as part of the HIFS Project, this paper reveals that of all the FSTs used to both identify and charge homicide offenders, the most frequently used were data gathered from CCTV (and nearly always in combination with other intelligence or evidence). However, as discussed, there are various possible reasons why CCTV featured more prominently than other FSTs at these stages of homicide investigations. Furthermore, how often particular FSTs are used is not (necessarily) a reflection of their value. Nevertheless, drawing upon qualitative data, our findings suggest that the "information profiles"[11] of different kinds of homicide may afford different CCTV opportunities. In particular, CCTV is used in many different ways to help to identify homicide offenders and implicate them in these offences.

This paper has illuminated some of the complexities and challenges inherent in recovering, viewing, interpreting, 'packaging' and presenting CCTV footage. These often present challenges for SIOs. For example, when setting the CCTV strategy, SIOs have to consider the risks of failing to identify and recover CCTV whilst being mindful of the resources and time needed to identify, retrieve, view and analyse the footage.

Our findings illustrate that CCTV co-ordinators do not always have an accurate picture of what CCTV has been identified and recovered. Moreover, those tasked with retrieving or viewing footage sometimes do not have the necessary skills, training or technology to do so. All of these factors can result in duplication of effort, time wastage and delays in the identification and recovery of CCTV. Our data reveal instances of potentially critical CCTV evidence being 'lost' (i.e. recorded over) before detectives were able to recover it.

Poor-quality CCTV footage present particular challenges and risks to detectives and CCTV officers, in trying to make sense of the images. Of particular concerns are the risks associated with misinterpreting footage and/or misidentifying suspects. Similarly, poor-quality CCTV footage presents dilemmas for detectives and CCTV officers who must decide whether or not to enhance it, and whether or not to utilise 'experts' to help view or interpret images. Our data illustrate potentially risky decision-making practices regarding whether or not to enlist external expertise and what that expertise might 'look like'. Equally, it is not yet clear whether and how 'super-recognisers' or 'super-viewers' may be considered to be 'experts' (e.g. via training or experience) or the limits of such expertise.

Currently, the integrity and provenance of CCTV 'evidence' may easily be compromised by risky practices and decisions made around how footage is recovered, shared, viewed, interpreted and 'packaged'.

Ultimately, these shortcomings may impact on the reliability of CCTV evidence that is presented and heard at court.

[11] Stelfox (2009: 99) refers to the information profile as "[t]he total information generated by the commission of a particular offence. . . Because offenders commit crime in different ways and in different types of environments, they generate different types and volumes of information". Stelfox, P. (2009). Criminal investigation: An introduction to principles and practice. London: Routledge.