CAMERA TO COURT

David Spreadborough *examines the many challenges of evidential video and reveals necessary improvements*

If you ask anyone about forensic evidence, the majority will probably talk about fingerprints and DNA. The years of crime dramas and news reports have instilled an understanding of what forensic relates to, and what evidence is. The minority may suggest computer evidence. Again, this is probably down to a huge increase in digital investigations being used in TV shows and Hollywood movies. I would guess that hardly any will mention CCTV footage. Although there are no publicly available studies, anecdotal research reveals that CCTV footage is the most common form of acquired forensic evidence within policing.

In a study conducted by Cheshire Constabulary in the UK, circa 2010, for every file submitted to the Crown Prosecution Service containing traditional forensic evidence (fingerprints/DNA), 15 were submitted with CCTV Images or video. CCTV is also nothing new, with it being used in investigations for over 50 years. With all this information in mind, you may expect that the processes and workflows for this type of evidence were straightforward. Think again.

> IT'S VITAL TO ENSURE THAT YOUR VIDEO SYSTEM CAN BE USED EASILY BY LAW ENFORCEMENT

Before I move on, let me talk about a very well-known coffee shop. They have something called a 'plant to cup' philosophy (or very similar). This documents the company's promise to ensure every stage in the coffee bean's journey. Starting from the plant to the final cup of coffee, everything is tracked and perfected. Ensuring efficiency and quality all the way through the process. This is only possible using standards and controls. Soil, plant, harvest, transport, equipment, people; everything has a standard and a control.

Let us now return to CCTV evidence, where a 'camera to court' philosophy is regularly used. This charts the forensic workflow required to take original multimedia from a surveillance system, through the Criminal Justice System (CJS), and into the courtroom as evidence. It is a great idea, but it doesn't easily work due to the lack of standards in the initial stages. Therefore, the recording, acquisition and processing of the multimedia for use as evidence is fraught with challenges. It is these challenges that I will be examining here, highlighting where improvements can be made to ensure the feasibility of the camera to court philosophy.

There are thousands of recording devices. DVRs, NVRs, PC-based recording, IP to cloud. The list is immense, with an industry estimation of approximately 10,000 different types of recorders. Although there is only a small number of base recording structures, all individual formats can be configured by the manufacturer and there is no standard within the industry to ensure that this is compatible with every other link in the CJS chain.

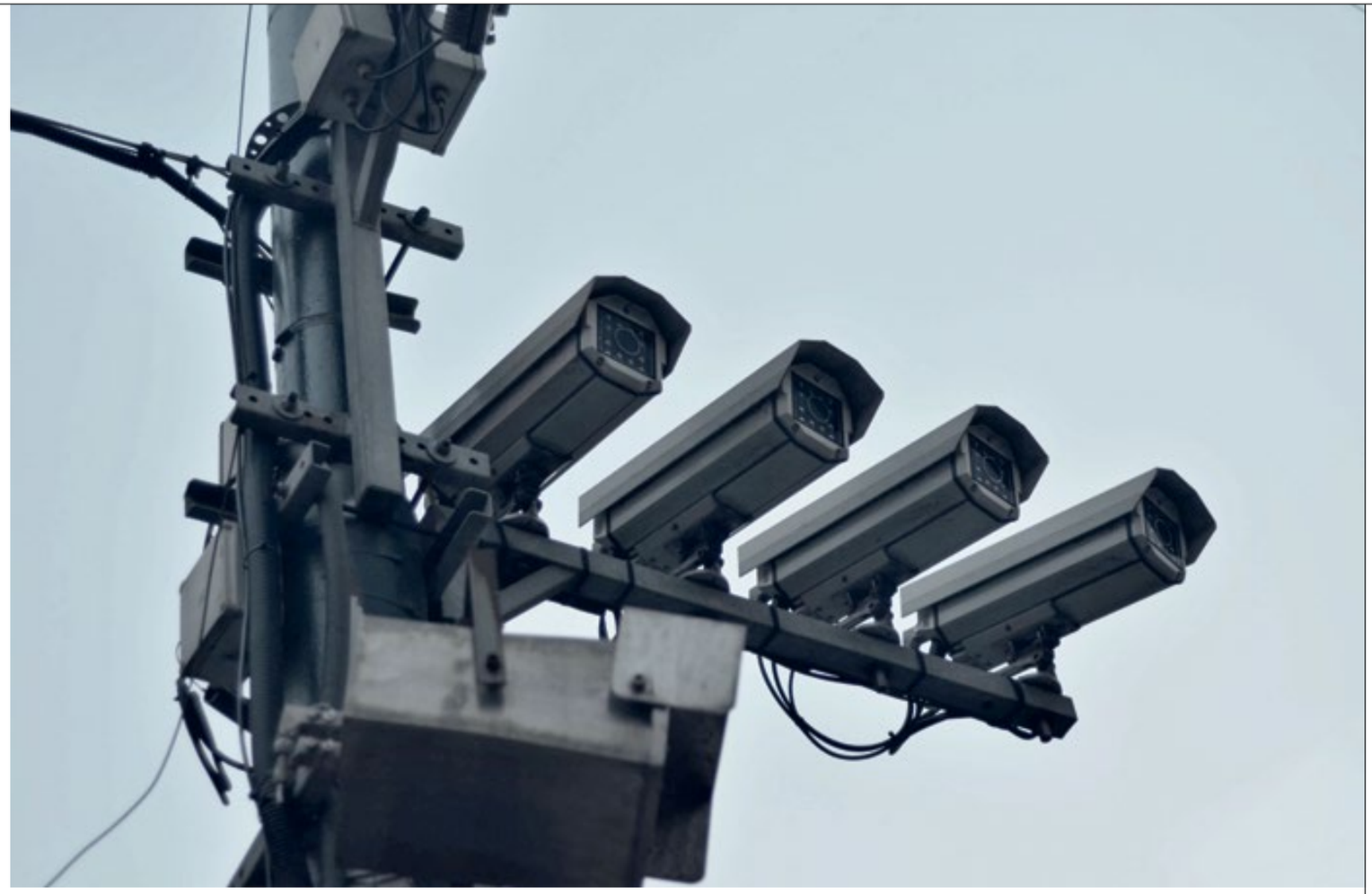
The consequence of this initial ill conformity is huge and causes problems for every other stage in the evidential process. Other forms of digital evidence do not have this burden. This is surprising, as smartphones, computers, in-car systems and smart devices are not designed to record evidence. They are regularly used as evidence, but they have an unconnected purpose.

CAPTURING THE EVENT

Recorded surveillance video, in contrast, has a single purpose. To capture an event in such a way that it can be later viewed. We will come back to the authenticity of such recorded events a bit later, but for this stage in our process, let us simply look at the raw data.

When a recording device is included in a surveillance system, the level of importance is significantly raised, as that material may be needed as evidence. As such, that material must be fit for purpose. This was recently highlighted by the UK's Security Camera Commissioner in his 'Buyers Toolkit'. The information to buyers is now slowly getting through, but why are devices still being made and sold that are not fit for purpose?

Back in 2014, I conducted a small study of some new recorders introduced to the market place. I came up with some help for manufacturers in the design and implementation of their recorders. Without going into full detail many of the recommendations involved ensuring that when the need arises, any and all data captured by CCTV systems is easily shared with local law enforcement. After all, in the worst-case scenario the ultimate end user isn't the person buying the system, but the police and courts tasked with relying on the video.



The recording, acquisition and processing of multimedia for evidence can be fraught with challenges

Some of these recommendations related to the physical design of the DVR/NVR to ensure retrieval of information was as simple as possible. For example, the positioning of USB 3.0 ports and the ability for simple HDD removal and reading. Others related to helpful functionality such as being able to view the estimated data size and time to transfer the footage before a download, or being automatically shown the export interface when a suitable device is inserted.

By far the most important recommendations related to the transparency of how the systems stored and processed the data. For example; the video and audio should be available in a standard, unmodified format; it should be viewable without the installation of a proprietary player or video codec; and the settings and recording information should also be easily exportable. In analysing the footage and preparing it for presentation in court the frame rate, frame count, motion detect recording, GOP, format, display and aspect ratio can all be vitally important.

You may remember that I mentioned the authenticity of video images. This relates to answering the question of whether the video accurately represents what it purports to be. The only way an investigator can answer this question is through forensic analysis of the footage and looking at authenticity on a question by question basis.

DETERMINING AUTHENTICITY

A video may be authentic, in that it shows a specific location or certain people, but it may not be authentic in that the motion may not be recorded properly (such as low or variable frame rate video). It is, therefore, vital that this authenticity analysis can be carried out, unhindered by proprietary, modified or encrypted formats. But authenticity is different from integrity. Integrity relates to the question of an image or video being unchanged since the time of original recording. This is a hugely important issue, especially for those manufacturers who transcode video material, or when a video must be transferred across networks. It is hopefully clear, that any complications can cause the evidential weight of a video to be lowered. Now that the challenges of the recording format have been identified, let's move forward to the initial investigation.

When an investigator gets the video, and all the data integrity questions and protections have been

answered, it's time to assess it. Easy, you may think. Well, only if the footage has been recorded correctly, and exported correctly. Thinking back to our coffee story, it would be like setting up an automated processing plant for the beans, but each farm putting their product in different containers and there being no information about what's inside.

FINDING A SOLUTION

Amped Software identified this bottleneck and went to work on a solution to this and several other subsequent challenges. First responders were not only having playback and decoding issues, but the police units dedicated to video analysis were unable to cope with some of the basic functions.

Review, basic enhancement and exporting can't be completed by just any software. Forensic guidelines dictate that safeguards must be in place. As a forensic image and video company, and the developers of the leading software, Amped FIVE (Forensic Image and Video Enhancement), the importance of scientific methodologies are easily understood.

Amped Replay, the company's recently launched product, is designed to immediately identify video, decode, interpret metadata and display time and frame information, making the initial review of video simple and quick. Replay includes enhancement and annotation functions that fully comply with the Forensic Science Regulator's guidelines and enables this stage to comply with ISO accreditation requirements.

After these processing functions are completed, the user can export what they require for the case. Images or video are all then compatible with the national repository systems. Every process is logged and documented in an automated report that can be used later to repeat and/or reproduce what was conducted. The benefits to volume crime investigations and the early hours of a major incident are huge, as all the reviewing and basic work can be completed immediately.

Replay will change how investigations are completed when they involve CCTV, image or video evidence.

CCTV FOOTAGE IS THE MOST COMMON FORM OF ACQUIRED FORENSIC EVIDENCE IN POLICING

But it can be so much better with the help of system manufacturers. Manufacturers need to ensure that they develop and build recording devices that can be supported. Modified and proprietary systems are causing problems and must stop.

If you are buying or upgrading systems ensure that whatever is purchased can be used easily by law enforcement. Even for a shoplifter – it is absurd that a specialised officer is required to decode the footage, on a dedicated workstation, purely because the system requires a proprietary codec that cannot be installed ●

David Spreadborough – Certified Forensic Video Analyst & International Trainer at Amped Software – has 24 year's experience in the police forces, specialising in forensic video analysis; currently develops and delivers training modules focused on the analysis, enhancement and interpretation of video and images within a legal environment.

Police officers monitor control screens in a Paris security command room

Picture credit: Getty