CAPITA

OPINION PIECE

The Management of Digital Evidence

A discussion paper for the UK criminal justice system

Introduction

Over the last few years there has been a concerted move in the criminal justice system to remove paperwork and move towards a digital case file. Significant funding streams have been put in place to support these initiatives.

This is bringing about technology challenges for the police, prosecutors, the courts and other stakeholders. The police are at the sharp end of managing digital information; responsible for identifying potential evidence from the vast volumes of data available, securing it, building it into cases and sharing it with those who need to see it.

The positive effect of digital evidence

Digital evidence now comes from many different sources. These include body worn video, the public sector, commercial and private CCTV footage, mobile phone images and video from the public, still images and video from crime scenes, digital interviews, text-based documents, ANPR, patrol car video, audio from contact centres… The list is long and growing all the time.

Taking body worn video (BWV) as an example, this has been widely piloted and some forces are now working towards equipping every officer with a camera. Reports are that it is playing a positive role in detection and conviction, and that there are increases in the rate of early guilty pleas from suspects confronted with this evidence.

In Paisley and Aberdeen a study found that: "There was a higher rate of early guilty pleas in the cases using body worn video. Most significantly, the percentage of cases requiring to proceed to the trial date was substantially reduced and there were no cases where a full trial was required." (ODS Consulting, 2011.)

A study also found that BWV reduces escalation during police-public interactions. (University of Cambridge's Institute of Criminology, 2014.)

With the benefits come data management challenges

The positive contribution that new and better forms of evidence can have on detection and conviction is very welcome of course. However, it also brings a significant challenge: the potential to create a mountain of new data every day that has to be downloaded, stored, catalogued, shared and analysed.

We know of at least one force that is eager to go ahead with a rollout of BWV but is not happy with the storage and retrieval solutions currently available to them. The force recognises the operational benefits of BWV, but the IT challenge of storing, cataloguing and sharing the data is holding back implementation.

This paper makes the case for police forces and other criminal justice agencies sourcing solutions for the management of digital evidence that enable them to achieve the following:

- Upload evidence of multiple types in multiple formats from internal and external sources.
- Catalogue the data so that it is searchable and store it in a way that makes retrieval and use simple.
- Share the data with relevant stakeholders whilst ensuring audit and security controls are in place, including the ability to track down the source of any security breaches should data wrongfully enter the public domain.
- Analyse the evidence as part of investigations, case building and case management.
- Integrate the solution with other systems, such as records management systems and share the data locally, regionally and nationally.

Capita does of course have a vested interest in this approach. We are a leading supplier to the police and criminal justice sectors and have invested significantly in developing a solution, EvidenceWorks®, for this integrated approach in partnership with our clients.

However, we believe that the issues in this paper are discussed free from bias. We hope that the paper itself will prove to be thought-provoking and of practical value for readers, regardless of whether they wish to explore our solution.

Understanding the challenges of digital evidence

It is useful to break down the issues and challenges associated with digital evidence into a few categories before we move on to how they might be overcome.

Multiple solutions lead to technology silos

On the face of it, it is much easier for a police force to buy a discrete IT solution as and when needed than it is to specify and implement a more integrated approach. However, this almost inevitably leads to a solution where a number of different solutions are working in silos around the force.

There may be a single dedicated solution for BWV, one for CCTV, another for recording interviews and so on. When individual solutions are sourced and implemented there is a significant risk that the police force involved finds it difficult to integrate solutions and data.

A single managed point of access for all departments and partners will improve security, improve reliability and reduce cost as well as reducing the complexity of implementing the Management of Police Information (MoPI) guidelines.

Using the above examples to illustrate this, if a suspect is filmed committing a crime and then interviewed about that crime, how easy is it for someone reviewing the evidence to quickly access the films and interview audio at the same time?

The amount of data will continue to grow

Already, the sheer amount of digital media being collated presents a huge challenge. Let's say that there's a particular shift with 20 officers wearing video cameras, with each one generating one hour of video. This means that in a 24-hour period there would be 60 hours of video footage to transfer, store and catalogue.

The future is one where the amount of digital data created will grow exponentially. It is also one where video quality will continue to improve: a smartphone today creates video of a quality that some camcorders a decade ago would have struggled to match. The advent of 4G and high bandwidth communications will also promote streaming and 'real-time' use of cameras but we won't get into a discussion on mobile data here.

The downside of more and better footage is that there will be huge amounts of data to transfer and store. This will become unwieldy to manage effectively if suppliers and forces simply focus on deploying more cameras without giving careful consideration to the implications.

The University of Cambridge study (2014) found that: "The sheer levels of data storage required as the [BWV] cameras are increasingly adopted has the potential to become crippling…The velocity and volume of data accumulating in police departments — even if only a fraction of recorded events turn into 'downloadable' recordings for evidentiary purposes — will exponentially grow over time…User licenses, storage space, 'security costs', maintenance and system upgrades can potentially translate into billions of dollars worldwide."

As with many areas of business the temptation may be to employ a cloud-based solution to provide the flexibility and future-proofing required with such an evolving challenge. Our belief is that secure cloud implementations could certainly help alleviate storage concerns but only as a small part of a holistic approach that encompasses a whole-force IT strategy rather than a piece-meal approach that wouldn't reap the cost benefits from decommissioning existing data centres nor take into account the cost of the network connectivity to the 'cloud solution' necessary for handling the growing demands of video data.

The strain on available bandwidth

Bandwidth becomes an especially problematic issue when individual officers are working in remote locations, or where rural police stations need to get video and other data over the network.

If the force is relying on whatever the telecoms providers can supply, and if that means poor performance levels in remote areas, limited bandwidth may not allow large files to be transferred. The situation is especially challenging in the UK where some forces have outlying islands and remote areas.

Some work-around solutions are already being used, such as burning footage to DVDs and then physically delivering the discs to HQ for uploading onto the main system. There are also solutions that allow just sections of video to be streamed in high definition rather than the whole video.

The need to add information to video and still images

Uploading video footage is one thing, but there is also a need to add significant amount of information (metadata) including location, date, the names of people involved and so on. That is potentially a very time-consuming task.

Some cameras, especially phone-based devices, include a facility for geo-tagging, through which the location will be automatically recorded and can be duplicated in text format for ease of reference. Similarly, date and time and other metadata are often also recorded. Features such as facial recognition can also be employed, subject to the requisite regulation and approvals.

However, there will often be a need for officers to manually record information. Whilst standards and formats can help automate some input, systems can be configured to provide check boxes for must-have information. Free-format text will of course also need to be added. This process should be as simple as possible to keep administration time to a minimum.

Coping with numerous formats

The huge number of file formats presents a considerable challenge. CCTV footage for example will come from many different manufacturers' cameras and may be in any one of hundreds of file types. Police forces cannot insist that businesses and the public use specified file formats, so the challenge instead is to be able to handle whatever format may be supplied.

Facilities for transcoding formats into something that can be edited and played on PC-based editors and media players are vital. Just as important is the means to record details of every viewing and editing action taken, as well as preserving the footage in its original format (ideally with whatever video player is appropriate for that format) for evidential purposes.

We should also remember that evidence is still sometimes provided in analogue format, so facilities for converting VHS (for example) to digital are also necessary.

Making decisions on storage protocols

Another issue concerns the process for deciding what data to store and what to delete. Many files are unlikely to be of evidential value and some forces ask officers to delete them rather than download them. Other forces take a policy that everything should be downloaded and stored for a certain period (e.g. 31 days) and then deleted after that time if it is not required.

Deciding on which approach to take requires an understanding of the legislation, guidance and best practice as well as an analysis of the administration times involved, the cost of storage facilities and the operational value of keeping rather than deleting data.

Converting audio to text

There is still a heavy reliance on text-based information in the criminal justice system and that will continue to be the case until all partner agencies and the courts are fully digital. Digital evidence solutions therefore need to manage transcription of audio, or integrate well with whatever systems or functions perform that task.

As a footnote, we recognise that voice recognition transcription isn't reliable enough yet for criminal justice purposes. However, this will almost inevitably change and systems will need to accommodate this when it happens.

What is needed to address the challenges?

Our belief is that police forces and the wider criminal justice system need solutions that bring all of the digital evidence data together into a single repository, held under the right security standards, with workflow processes to enable it to be processed and integrated into case record and criminal justice systems.

Under the Modernising Justice agenda we will see more and more police force data made available in real time to the Crown Prosecution Service (CPS). Here again, there is a powerful need for digital evidence management solutions that can accommodate this. There is an initiative already in place that solutions must support: the Home Office Collaborative Digital Information Service (CDIS). Capita is pleased to be part of the Home Offices' supplier engagement programme and is committed to supporting CDIS through **Evidence***Works*®.

We believe that forces have a lot to gain from implementing digital evidence solutions individually, but there are even greater operational and financial benefits from forces forming strategic partnerships with each other. Inter-force collaboration and sharing of resources could in fact be the only way that some smaller forces are able to make use of such solutions.

In this paper we haven't touched on security in any detail: we believe that UK police forces already have very secure networks and on-premises deployment of evidence applications presents no additional challenge. Where things get more complicated is the regional deployment of solutions where there is inter-force collaboration and so very secure firewalls are essential, and the large investment that forces have made in secure data centres will prove invaluable.

Summary: the case for digital evidence strategies, policies and systems

Having robust digital evidence strategies in places, brought to life by equally robust policies and solutions, will break down the silo nature of the current landscape. This has the potential for operational benefits and opens up the potential for long-term cost savings:

- A common platform opens the door for efficient processes, from minimising administration time spent by frontline officers on (in effect) being data processors rather than law enforcement officers, to sharing data with external agencies including the CPS.
- Economies of scale from having a common platform as opposed to multiple third party systems, both in terms of purchase and licensing costs.
- A camera-agnostic platform supporting a hybrid technology estate will allow a force to meet differing operational needs and avoid 'lock in' to specific vendor technologies.
- Savings also come from the 'bulk buying' of storage rather than piecemeal purchases across many different systems and storage locations. A secure cloud solution could help as part of a holistic IT strategy but isn't necessarily a panacea for this specific challenge.
- Integrated solutions inevitably involve lower implementation costs than the alternative that sees multiple multiple applications being implemented multiple times in an uncoordinated way.

At the time of writing (May 2015) Capita's understanding is that few UK police forces have set themselves on a journey of fully integrating evidence data. Some are trying to integrate data by getting various parties to share data more widely, such as CSI teams sharing crime scene evidence with other departments. But we are not aware of many forces going the next step and creating one holistic data repository that can be accessed by all relevant stakeholders.

A single digital evidence repository should, however, remain separate from a force's Records Management System but, with the right level of integration can ensure that business processes are streamlined and joined up.

Implementation needn't be a 'big bang' that disrupts the organisation. It is possible to implement a digital evidence strategy in a phased approach so that a single repository used by one department or one station is then rolled out to additional departments and stations. The repository can then be expanded to encompass further sources of evidence as the strategy evolves, for example, with the use of specialist data extraction technology for mobile devices in custody suites.

We cannot see an alternative to taking this integrated approach and are proud to be investing in solutions that make it possible. This is of course an ever-changing environment and we look forward to further engagement with police forces and other criminal justice agencies in this vital work.

References

The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomized Controlled Trial. Journal Quantitative Criminology. University of Cambridge's Institute of Criminology, published in the Journal of Quantitative Criminology, November 2014.

Body Worn Video Projects in Paisley and Aberdeen: Evaluation Report. ODS Consulting, July 2011.

Point of contact

Tom Edmonds

07702513267

tom.edmonds@capita.co.uk

Capita
Methuen Park
Bath Road
Chippenham
Wiltshire
SN14 0TW
United Kingdom

E sds.info@capita.co.uk

W www.capitasecuredigitalsolutions.co.uk