masonadvisory

WHITE PAPER

POLICE, CAMERA, ACTION!

Getting the best from body-worn video

Introduction

Body-worn video (BWV) cameras (i.e. robust, solid-state video cameras attached to an officer's uniform, capable of recording a 'point-of-view' video file on demand) represent a recent technology development that is being driven by the Home Office and by operational requirements for widespread adoption within the police and other emergency services.

While public perception of the usefulness of the technology is influenced by media reports of its use in an officer accountability role (in particular, the community tensions created in the USA after several high-profile police shooting incidents), the operational benefits are much wider. There are particular benefits in areas such as staff protection from crime, and automated evidence gathering during an incident – leading to a higher rate of guilty pleas.

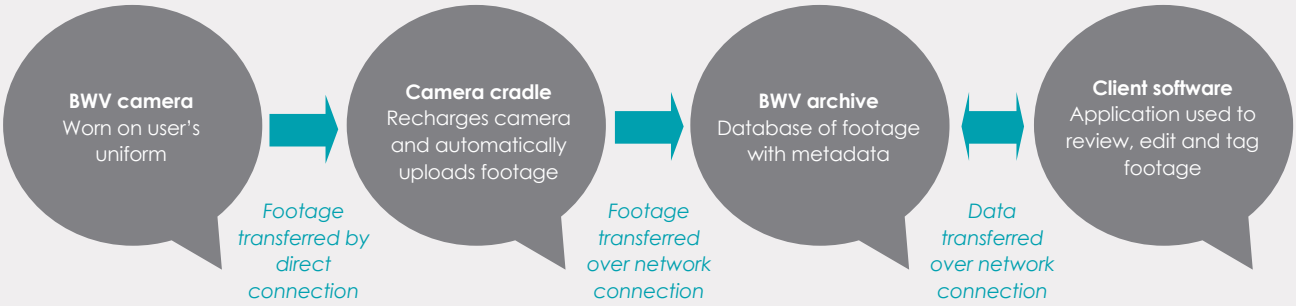
However, these benefits can only be fully realised if the whole BWV deployment is correctly integrated into the wider ICT strategy and infrastructure in use within an organisation. Many organisations are (for reasons of expediency and cost) deploying the technology in a vertical, stand-alone capacity that risks undermining the eventual benefits. This paper discusses these risks and how they might be addressed.

Technology components

BWV systems are relatively simple on their own, and at a high level are made up of the components described below and illustrated in Figure 1.

- **Camera** – a robust, uniform-mounted solid-state camera with a fixed-focus, wide-angle lens and an internal rechargeable high-capacity battery. Most models record on a constant loop, but only commit images to the internal flash memory when a button is pushed on the front of the camera (typically as the user decides that an incident needs to be recorded). In many cases, a short, predetermined amount of footage from immediately before the recording button is pressed is automatically added to the file to ensure that the beginning of an incident is not missed in the recording process.

Figure 1: Overview of the components of a body-worn video system



- **Docking station** – located at the user's station, this is a cradle where the cameras can be charged, ready for their next use. While docked the camera's captured footage is uploaded to an archive system. Once this is complete, the camera's memory is securely deleted.
- **Network transport** – data is uploaded from the camera docking stations over a network link. This can either be an Internet connection or an internal private wide-area network (WAN) operated by the user's organisation. Typically, the video data is encrypted in transit to preserve a 'chain of evidence' and to eliminate any concerns over the possibility of data tampering.
- **BWV archive** – this is a storage system for hosting the recorded data from the cameras, with suitable at-rest data security to preserve a chain of evidence for the video data. Such a system must also include digital asset management facilities, to allow the data to be appropriately tagged with metadata (i.e. data that describes the data) to indicate what the footage represents, which user obtained the footage, the incident with which the footage is associated etc. This allows the data to be retained, deleted or handled appropriately based on the rules outlined for BWV within the organisation.
- **Client software** – this is an image processing and management system accessible to the BWV camera users, allowing them to review footage, add metadata, perform necessary editing functions (i.e. trimming footage or highlighting items in the images for review purposes – the original footage is still retained untouched), and interact with the footage as required by their role. This software is offered in a variety of modes depending on the particular solution, and may be installed locally on a client PC, run on a wireless-enabled tablet or accessed remotely using a Web browser.

The challenge of integration

The relative simplicity of a BWV solution is deceptive: the power of such a system comes from being able to integrate these components into the wider ICT infrastructure to enable the real benefits to be realised. However, there are some challenges associated with this process.

Network transport bandwidth – *are the network links between the docking stations and the BWV archive sized appropriately for transferring large amounts of video data?*

- Data must be transferred in a timely manner to make it available for metadata tagging and post-processing. Slow network links can make this a lengthy and perhaps unreliable process.
- Particularly in smaller locations with few on-site users, the network links may be sized for relatively low traffic levels. This can mean that a typical data upload from BWV cameras can take many hours.
- Link saturation by video transfers may render networks slow or unavailable until transfers complete.

Device security – *does the presence of docking stations compromise on-site device security?*

- Many organisations prevent the use of universal serial bus (USB) devices on their workstations to prevent memory cards and thumb drives being used as a way for viruses or malware to infect PCs or central systems.
- Some docking stations require a local PC for upload, and use a USB connection to achieve this.
- Even where docking stations can operate independently, they often run internally as cut-down PCs with fully fledged operating systems, that are uncontrolled and unmanaged by the organisation. This represents a maintenance and patching problem for the ICT infrastructure.

Client software performance – *can the clients running the editing and management software handle video effectively?*

- Many client devices deployed in organisations are optimised for line-of-business tasks, rather than complex graphical work such as viewing, scrolling through and editing video files.
- This work can also place additional demands on the client network, as temporary video caches and streams are often directed over the network to client devices to aid local client performance.

Footage availability – *can uploaded footage be accessed relatively quickly to aid a fast-moving investigation or incident?*

- A key advantage of BWV should be rapid availability, meaning that an on-site incident can be reviewed quickly for action or decision-making.
- Private CCTV footage requires significant time to find and gather as the cameras are physically distant from typical incidents and the police are dependent on third-party compliance. By contrast, BWV is available on site and up close with any particular incident.
- Availability of footage with audio can make decisions on charging and/or obtaining an early guilty plea much more robust. However, the end-to-end system must be able to upload, process and share footage to allow this to happen.
- Home Office guidelines call for unused footage (i.e. not required for evidence or an organisational process) to be deleted after 30 days. This means any lag at the beginning of the footage management process shortens the opportunity for footage to be used to support investigations or incident-based decisions.

Records integration – *can BWV footage be accessed and integrated into the records of other systems, particularly intelligence, custody and case preparation systems?*

- In order for BWV to be used effectively, the footage captured needs to be made available for integrated use within the other processes associated with the organisation. This calls for systems integration with the BWV archive, so that records can be referenced without the need for duplication of large video files.
- Manual processing of video data is time and resource intensive; the use of manually generated video records (such as DVD optical disks or similar) for video evidence is therefore inefficient and can result in evidence loss or compromise.

These issues are a combination of technical and business process challenges. Solving them to make best use of BWV, therefore, requires a joint approach between ICT and the operational side of the organisation.

Meeting the BWV challenge

In order to address the challenges of building BWV into an organisation, there are a number of project considerations that can help to achieve improved outcomes.

- **BWV projects should involve (but not be led by) ICT and the business**. It is important to get all of the appropriate stakeholders involved as early as possible in a BWV implementation ot ensure that requirements meet both technical and business objectives. However, to avoid compromising one set of objectives in favour of the other, it is better, if possible, for the project to be led independently.

...continued overleaf

> *Benefits can only be fully realised if the whole BWV deployment is correctly integrated into the wider ICT strategy and infrastructure in use within an organisation.*

- **Identify the actual uses**. BWV is a solution that offers a variety of functional possibilities, and it is easy for the combination of supplier marketing material and management desires to lead to unrealistic technical expectations. In addition, the need for detailed technical capacity planning in areas such as the network means that detailed and realistic use cases are extremely helpful. These should be developed by operational leads and ICT staff, and should represent the likely patterns of end users, rather than the assumptions of managers.
- **Develop a long-term roadmap**. The expediency of end-to-end solution delivery from suppliers (such as cloud-based BWV archives offered in tandem with the camera system) is useful in getting proof-of-concept and pilot systems up and running. However, any project should recognise the constraints that such implementations impose, and either plan to integrate such solutions into the wider organisation at a later date or recognise that a more integrated system will need to be costed, planned and deployed as part of the overall project delivery.
- **Work with the strategy**. Most organisations will have a business and technical strategy for ICT systems delivery and operational requirements handling, as well as security policies that must be complied with. Such strategies and policies should not be ignored in delivering a BWV requirement; instead these documents will help to inform the development and design of the BWV system components (especially the network requirements) and ensure that the BWV solution is delivered is a supportable and cost-effective way for the overall organisation. Early engagement with these documents is important.

To address these considerations, ideally any BWV project should be undertaken as part of the overall ICT development and implementation work, with full awareness and reference to the rest of a force's ICT improvement programme. In this way an organisation can minimise the risks of 'silo' development and improve a BWV project's fit with requirements, return on investment, and outcomes.

Contact us

If you would like to discuss how we can support you please email contact@masonadvisory.com or call +44 (0)333 301 0093.

www.masonadvisory.com