Proceedings of the

2nd Australian Security and Intelligence Conference

1st to 3rd December 2009

Kings Hotel,
Perth, Western Australia

Published By

secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia

Edited by
David Michael Cook
secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia

ISBN 978-0-7298-0679-4

CRICOS Institution Provider Code 00279B

Information overload: CCTV, your networks, communities and crime

Vandra Harris[1] & Crispin Harris[2]
[1] School of Law
Flinders University

[2] Security Consultant

Abstract

Electronic surveillance continues to play a central but often unobserved role in contemporary Western societies and attempts to police them. This paper focuses on closed circuit television (CCTV) footage and its technological implications, particularly relating infrastructure and data storage and integrity. While CCTV might appear attractive in augmenting law enforcement systems, the authors argue that the debate on use of CCTV in crime prevention remains incomplete without an effective understanding of the diverse costs. This discussion reveals startling ICT resource needs and associated costs, together with very specific technological capacity. These contribute significantly to the costs of such systems, reinforcing the authors' argument that CCTV is no golden bullet for law enforcement.

Key words

CCTV; data security; live streaming; law enforcement; policing

INTRODUCTION

Closed circuit television (CCTV) systems collect video and direct it to a central monitoring system that may be monitored in real time or 'near real time'[1], and/or record the video for later inspection or playback. There are four key aims of these systems in law enforcement: deterrence, rapid response, investigation and identification, and prosecution of crime. As technological developments in the last four decades have made CCTV cheaper, smaller and easier to operate, its use has expanded significantly, to the point that a European survey revealed that nearly one in three premises and institutions utilised CCTV surveillance in 2002 (Hempel and Töpfer, 2004, p. 3). As use has increased, so too has commentary on the effectiveness of the medium, its impact on society, and the attempt to balance the rights and liberties of 'the innocent' with the responsibility to protect them and apprehend 'the guilty'. This paper aims to balance that commentary with a clear understanding of the technological impact and requirements of such systems, to assist effective planning and decision-making regarding CCTV use for law enforcement.

A scan of Australian newspapers reveals that CCTV is popularly perceived as effective in deterring crime and securing convictions. Prior to the 2007 APEC Summit in Sydney, the number of CCTV cameras monitoring that city's public transport network was increased to 6,400, as a 'strong deterrent to common criminals and thugs' (NSW Acting Premier John Watkins, cited by AAP, 2007). Similarly, a more recent article in *The Australian* (Martin, 2009) stated that the showing of CCTV footage on news broadcasts acts 'as an overarching safeguard and deterrent'. This perception is not necessarily matched by evidence, and needs to be balanced with a clear understanding of the actual efficacy as well as the technological requirements of systems. Understanding this will contribute to the ongoing dialogue about the usefulness of this tool in an era of increased surveillance and shifting perceptions of a need to balance civil liberty and civic safety.

Our specific contribution to this debate concerns the technological aspects of CCTV, in particular the impact on technology and data storage requirements for enforcement regimes, notably by police. The paper commences with a brief explanation of the technologies we address, and the contexts in which their applications relate to law enforcement. We then briefly address the academic literature on the efficacy of CCTV in crime prevention and prosecution, before moving to our primary focus on the realities of data management arising from CCTV applications in mainstream law enforcement. This discussion includes attention to the question of whether CCTV is a cost-effective method, and whether technological resources currently available to Australian police forces are adequate for optimal use of CCTV tools. We note that significant investment would be necessary in the short term to ensure that police services can adequately manage the data arising from increasing CCTV application and to ensure that the technology meets the needs and expectations of these services. We conclude that while CCTV can be useful in a number of ways, the expectations must be well defined, and infrastructure impact must be carefully considered as a core component of the implementation.

[1] That is, within minutes of the actual events.

TERMS AND TECHNOLOGIES

It is important to commence with a strong understanding of the terms and technologies in focus in this paper. CCTV cameras record individual images that together create a moving image. Most CCTV systems collect these images at a rate of over 15 per camera per second. Individually, these images – or 'video frames' – are smaller than most commonly available images (less than 16Kb per frame)[2]. While the individual images are small, the collection of this information for later playback can add up to a substantial amount of data: one camera recording low quality video for 24 hours at this rate will record at least 1.3million images, generating over 20Gb of video (equivalent to 5 movie-length DVDs).

'**Streaming'** of data refers to the practice of sending a constant flow of data (usually audio or video) over a data network to a remote location, and 'live streaming' refers to transmission of this data at the time that it is captured. In practical application, live streaming of CCTV is the exception rather than the rule – video is usually recorded for later reference rather than being monitored immediately. Banks, for example, store CCTV footage at branches rather than centrally, due to the volume of data created by 16-32 cameras per branch, generally recording higher quality (and thus larger) images than those described above. Such a high volume of data would require significant bandwidth for transmission, but in this case identification *after* the fact has been deemed sufficient when combined with other security mechanisms.

Live streaming is usually used for transient data (that is, data that will not normally be stored after viewing) and in most cases involves the transfer of high volumes of data. Examples of cases in which live video streaming may be applied include internet broadcasts of sporting matches and the NASA 'net-cast' space shuttle launches[3]. In crime prevention applications, CCTV footage is streamed to enable live monitoring of locations or events as they occur. An example of a substantial, actively monitored CCTV system is a public railway network: metropolitan rail networks frequently have over 5,000 cameras and are actively monitored by railway police in a central location. Where data is not streamed, it is stored on the site of collection.

While CCTV **system sizes** vary, a regular 'off-the-shelf' system (which can be sold as a pre-packaged bundle or in separate pieces) generally comprises up to 16 cameras[4]. Systems of this size would be appropriate for a small to medium business with a single physical location, and includes approximately a terabyte[5] (Tb) of local storage (adequate for seven days of recorded data) and dvd burner to allow data to be recorded for review. As will be discussed, both storage and transmission of this volume of information can involve substantial financial investment (including conversion equipment, storage space and systems that enable later retrieval of data). Public space systems tend to be many times larger than this, as in the case of the rail network referred to above.

LAW ENFORCEMENT APPLICATIONS

Where CCTV is used for surveillance it is rarely a police operation: private enterprise or different levels of government frequently install and/or monitor cameras, either exclusively or in partnership with police. According to Wilson and Sutton (2003, p. 2) 'the push to establish CCTV in Australia has come from local government', and this diversified ownership and responsibility has particular implications that will be expanded below. Where CCTV is used in crime/incident investigation (to assist investigations into crimes that have already occurred), the video is generally sourced from non-law enforcement CCTV systems such as these. It is therefore not useful to limit this discussion only to police-owned and operated CCTV systems.

Nonetheless CCTV is used in a diverse range of law enforcement contexts, for one or more of the four purposes listed above (deterrence, response, investigation and prosecution). Live-monitored CCTV may be used for control and management of major events, to ensure that public safety is maintained and to respond quickly to emerging disturbances. An example of this is the large public New Year's Eve celebrations in the South Australian beachside suburb of Glenelg, where live streamed CCTV monitoring has been used by police for some years. A similar usage is in the active CCTV monitoring of high crime locations or of places such as prisons. In both of these applications, CCTV may be used as a deterrent as well as facilitating rapid response to incidents. Of course this is not always foolproof, as seen in the case of a recent violent melee at Sydney's domestic airport in which one person died, when

[2] A standard 15x10cm photographic print at full resolution requires about 67,500kb. A small web picture or logo will commonly require 16-64kb, and while such an image would be clear at the size of 6x4cm, it would be heavily pixelated at 12x8cm.

[3] A football match would typically be distributed at 1megabit/second for 'Slow' connections or 5-12Megabits/second for 'high-speed' connections leading to a total of up to 9gb for a one hour broadcast.

[4] Both components and full systems can be purchased online through sites such as Amazon, eBay, or specialist suppliers for less than 1400AUD.

[5] A terabyte is 1,024 gigabytes, while a gigabyte is 1,024 megabytes. Thus a terabyte is equivalent to the storage of 4 to 8 current domestic laptops.

'despite the banks of CCTV cameras, which are supposedly monitored, it took a member of the public to dial 000 and alert police' (O'Brien and Creedy, 2009)[6].

CCTV use in response to crime may involve the deployment of officers in response to an action caught on camera, or provision of specific operational intelligence in real-time support of tactical operations (for example infrared and visible light cameras in a helicopter or unpiloted aerial vehicle). Such operational support video can be used and monitored at the point of capture, however it is frequently sent in real-time ('as it happens') to a command and control facility to assist in directing resources. Video captured by police cameras during an operation such as this would normally be retained after viewing as a part of operational record-keeping requirements.

CCTV EFFECTIVENESS

Our purpose here is to provide a brief overview of this literature, to provide a context to the technical discussion that is the core of our paper. As Wilson and Sutton (2003 p. 1) note, 'Although CCTV has expanded rapidly in public spaces it remains a controversial measure whose outcomes and appropriateness are hotly contested.' We follow five key threads in discussing the literature on the law enforcement effectiveness of CCTV: measuring impact; success in preventing crime; accuracy, particularly with regard to convictions; public support and belief in its effectiveness; and workload implications.

Readers of the academic literature on CCTV effectiveness may be struck by the repetition of one particular word: inconclusive. A key reason for this is that it is very difficult to measure impact due to factors such as absence or incompatibility of figures for prior periods, inability to measure whether crime has simply been pushed into other areas, and differing methodologies (see Gill et al., 2007; Gill and Sprigg, 2005; Wilson and Sutton, 2003). Added to this is the challenge of measuring impact, since comparison of crime statistics is fraught by the reality that crime statistics may not be disaggregated to a useful degree, that many factors affect changes in measurements, and that monitoring periods may not be sufficient to draw firm conclusions (Short and Ditton, 1998, p.12; Wilson and Sutton, 2003, p. 2). In this context, Welsh and Farrington (2004) conducted a thorough comparison of a large number of studies to compare the crime deterrent effect of installing CCTV in public spaces with that of increasing lighting. They found that both actions 'represent effective situational measures for reducing crime', particularly in the case of property crime (as opposed to violent crime). They also found that in city centres, street lighting had a greater impact on crime than installing CCTV cameras (Welsh and Farrington, 2004, p. 513).

With respect to deterrence, a long term study comparing application of and attitudes to CCTV in eight European countries found that

> the majority of CCTV systems aim to prevent deviant behaviour by symbolic but more or less incompetent deterrence because cameras are highly visible but those under surveillance are hardly visible for an observer due to irregular monitoring, informational overkill or even the deployment of dummy cameras. (Hempel and Töpfer 2004, p. 7)

Reinforcing this perspective, Privacy International (2007) notes that the existence of CCTV surveillance in London did not deter the July 2005 terrorist attack, nor did it detect attempted attacks in 2007. In contrast, Gill and Spriggs' report to the UK Home Office noted that police and security staff found it useful to be 'able to remind individuals that cameras were watching them as a way of increasing compliance' (2005, p. 115)

In relation to accuracy, Henderson, Bruce and Burton (2001) conducted a series of tests that revealed that even under optimal conditions, the accuracy of face matching techniques using CCTV, broadcast quality recording, and still photographic images was at best unreliable, not least due to the low quality images used. The highest success rate (75%) for face matching was achieved when comparison was between different posed photographs, while comparing still photographs with CCTV footage of a person achieved a success rate of only 20%. While it has been stated that CCTV footage is particularly useful when 'you know *who* you are looking for' (Coleman and Sim, 2000, p. 629, emphasis in original interview), Henderson et al. discovered that even when asked to state which of just two posed photographs showed the offender in a high quality CCTV, accuracy remained at just 65% (2001, p. 460).

There is also some disagreement about the appropriateness of using CCTV for public surveillance. Conflicting social attitudes to these technologies have been reported, both between countries and between social groups (see for example Singer 2009 and Hempel and Töpfer 2004, pp.8-9). Levine (2000) has argued that people's response to surveillance is significantly influenced by their social location (or 'group membership') – that is to say, how they locate themselves in relation to those advocating or performing the surveillance. McCahill and Norris cite a range of papers that report negative effects on young people arising from CCTV usage, whether or not it is specifically targeted at them (2002, p. 14).

[6] Such tragic examples are not new, and the Hillsborough football disaster of 1989 stands as a stark example of actively police-monitored CCTV that did not facilitate a police response that saved lives (see McMillan 2009).

Coleman and Sim (2000, p. 635) note that CCTV has been touted as promoting human freedom, in the sense of allowing citizens to feel safe in public spaces, however there has also been protestation that CCTV infringes on people's freedom and privacy. Privacy International (2007) states that the international trend for governments to collect and retain an increasing amount of information about people within their borders implies that 'all citizens, regardless of legal status, are under suspicion.' Mann (1998, p. 94) challenges that the individual has a right to 'self ownership' that is compromised by CCTV, while Vitale (2006, p. 180) writes of a 'creation of a new kind of sociospatial order and a new neoliberal urban subjectivity' – and indeed other authors point to its disproportionate effects on those already marginalised (e.g. White and Sutton, 1995, pp.89-91; Coleman and Sim, 2000, p. 634).

Perhaps the strongest outcomes around CCTV usage can be seen in public perceptions of personal safety, which a range of studies have found to be positive (see Wilson and Sutton, 2003, p. 5, Gill et al., 2007, p. 306). Yet O'Donnell et al. point out that CCTV use 'may be perceived either as promoting the safety of those in the area or as motivated by a lack of trust in the residents' (2009, p.2). In other words, if one feels that surveillance is being used to protect one's person and property, and identifies with the group implementing the surveillance, then one is more likely to feel it is a positive technology. Conversely, however, if one already feels marginalised and mistrusted – as may be the case for example with homeless people, or others who feel they are only liminal members of society – CCTV surveillance is likely to increase this sense/experience of marginalisation.

Finally, in addition to significant physical costs[7], live streaming of CCTV footage has significant human workload implications. If footage is to be screened live rather than stored, then it must be monitored. Monitoring by police necessarily removes officers from other tasks, at a time when there is continued political and community demand for *visible* policing 'on the streets', and when it is unlikely that policing budgets would be expanded to allow for extra staff to do this work – with the result that some police feel 'imaged out' (Gill and Sprigg, 2005, p. 115). In many cases, CCTV footage is therefore monitored by private groups or individuals, in what Norris and McCahill (2006, p. 105) describe as a move towards 'hybrid policing' in which distinctions between 'public' and 'private' become less clear.

Perhaps the most famous example of this took place in Liverpool Council in the 1990s, when a group of business owners and the city council collaborated to have CCTV cameras installed in key areas of the city, with the intent of increasing perceived safety and thus consumer traffic. While the local police had input into the location of cameras, it was members of the business partnership who undertook monitoring of the camera footage (Vitale, 2006; Coleman and Sim, 2000). A similar example can be found in many Australian cities, where business interests have had input ranging 'from simply offering in principle support through to full responsibility for funding ongoing operations' (Wilson and Sutton, 2003, p.3). In a current example, the Japanese police authority reportedly intends to install security cameras in residential areas in 14 prefectures, and to 'entrust volunteer groups of residents to operate and manage the equipment and image data' (Japan Times, 2009).

Those monitoring or reviewing CCTV footage 'face a daunting task', in that they must make judgements based on limited information (e.g. there is no sound), and in an unnatural context, in which the act of surveillance itself may generate an expectation of guilt (Williams, 2007, p. 100). Michael and Michael (2009, p. 5) argue that the combination of implied guilt and absence of trust can lead to a society in which behaviour is performative, determined by 'what we think we "must" do'. There are also several authors who argue that the expectation of guilt is particularly directed towards marginal groups, and that CCTV is part of a 'process by which economically powerful groups in society gain power through the private management of public space' (Fussey, 2004, p. 231; White and Sutton, 1995).

This brief discussion reveals a range of concerns and opinions regarding CCTV. We identify a gap in this literature concerning the data implications of CCTV, in that we believe that discussion of the utility of CCTV in law enforcement remains incomplete without a full understanding of the various dimensions of the data and monetary costs of CCTV use. We therefore move to that discussion now.

TECHNOLOGY IMPACT AND IMPLICATIONS

The collection of CCTV video has several impacts on information and communications technology (ICT). These can be loosely categorised as relating to: *volume* (impact on network services and provision of sufficient storage capacity); *integrity* (storage and retrieval and preservation of chain of custody); and *identification* (cataloguing, marking, indexing and searching for data of interest).

Collection of CCTV imagery is not useful in law enforcement unless it is captured and stored in an identifiable manner. The imagery must be of a sufficiently high quality that it can be reasonably expected to accurately and usefully reflect the actions and activities being recorded. The volume of data that is generated by each camera is substantial and must be transferred, stored, marked and labelled, indexed, archived and made available for view or retrieval. The common multi-camera CCTV environment compounds this data transfer and management issue into the kind of problem normally only seen in specialised data processing environments such as video pre-production. For this reason, CCTV

[7] For example, the Mayor of Melbourne City Council stated that installing 31 new cameras (to a total of 54) has cost $AU1.8 million, and maintenance will cost $AU1 million annually (Johnston, 2009).

data can easily overload an unprepared network in interesting and unexpected ways (as we will explain below) and will quickly overwhelm all but the largest of data storage environments resulting in substantial cost impact.

The expected and supported use of CCTV within an organisation will modify the degree to which CCTV will impact the ICT environment. Decisions such as whether live-feed CCTV footage must be provided to a centralised monitoring facility are critical factors. Optional storage, playback and archive of this data present additional problems. In technical terms, CCTV footage is characterised as large-packet, high-volume, continuous, time-critical, and order-sensitive. Each of these characteristics is important, and in combination they present a uniquely challenging data stream. The high volume of data has some immediately obvious impacts on the underlying network and storage infrastructure. The continuous delivery of large packets also has impacts on both the network and storage infrastructure and on other (seemingly unrelated) applications and services. In other words, communicating this volume of data can cause unexpected problems elsewhere in a system.

Diverse scenarios for CCTV networks

There are several levels of CCTV data communication and storage, with different ramifications for networks and ICT resources and support. We outline three simple CCTV streaming scenarios here as a guide for the reader, to help contextualise the following discussion on ICT implications. In each case, we are talking specifically about *public space* systems, rather than monitoring of private premises. The minimum and simplest case for CCTV use is simply the central collation of CCTV imagery for the purpose of (near) real-time monitoring. This usage case has an impact on network services that, at a base level, is proportional to the number and quality of CCTV cameras in the environment. The lack of a long-term retrieval or review requirement simplifies the data storage needs and almost eliminates any need for a structured data labelling/marking/indexing and search facility. This environment will experience a reasonably well understood network bandwidth impact. The continuous transfer of CCTV data may also impact other services, such as IP telephony or video conferencing, in a manner that is less obvious.

A somewhat more demanding case involves active monitoring with a medium-term retrieval requirement. This case includes all of the attributes of the previous environment, but also adds a requirement to store CCTV data for longer periods of time. This means that very large volumes of data storage must be provisioned, with a consequent increase in aspects such as: systems/hardware support and maintenance; systems and storage management overhead; data archiving and recovery facilities; physical and environmental factors (space, power, air-conditioning); and the network and licensing costs of maintaining these additional systems.

A much more complex case involves active monitoring with a requirement for strict data integrity, chain of custody protection and search/playback facilities. This environment provides the highest level of data integrity, capacity and capability for review of identified and surrounding footage. This is the hardest and most expensive environment discussed. This environment has the added challenges of requiring multiple and delayed playback facilities; comprehensive audit logging and data tracking capabilities; and an ability to guarantee data integrity.

Timeliness

It is generally expected that, for live-feed CCTV video to be useful in identifying current events, it will be available for display within 2 seconds of capture. CCTV differs from some other video environments (such as video-conferencing) in that the imagery does not need to be transferred with high priority transfer queues to meet very tight time constraints (i.e. instantaneous transmission) and constant frame-refresh rates. The requirement to have the imagery available within 2 seconds does, however, require that all captured data be transferred *as it is collected*, regardless of any other applications or services that the underlying network infrastructure may need to support.

Data size

CCTV system manufacturers regularly recommend video frame-rates of 5 to 15 frames (images) per second, and regularly provide '4CIF' resolution (704x576 pixel) (see for example JSVG, 2009). A single CCTV camera operating at the industry standard 4CIF resolution with H.264 encoding, capturing 10 images per second in a high-traffic public area can easily generate 864,000 frame each day, requiring 6.6 gigabytes (Gb) of data storage and 0.64 Mbps of dedicated network capacity. The same location with a camera collecting digital-TV quality video can easily generate over 200Gb of data per day at a rate of 20 Mbps of constant network traffic for over 1.7 million individual frames. Additionally, an environment using older cameras or less efficient image encoding protocols will get lower quality images with higher data sizes.

The nature of CCTV streaming drives a number of aspects of the transfer of that data over a network infrastructure. Streaming video data manifests as continuous, regular pulses of small groups of large data-packets. This makes it quite different from the majority of traffic that modern data networks are expected to support. The underlying infrastructure and protocols that go together to create a modern data network are designed to ensure the reliable delivery of data (packets) from one system to another. They are designed with the expectation that the arriving data will be reasonably well distributed and fairly random in packet size and frequency. Very few applications have any firm performance requirement, and those few usually have low individual time-on-delivery data volumes (for instance IP telephony, user

authentication, time synchronisation) or have burst-idle traffic flows (database replication, thin-client terminal services). Live streaming of CCTV, however, is both time-critical and high volume and this translates into extremely high pressure on networks.

Horizontal impact

In real terms, as each frame is transmitted (5-20 times per second) the data associated with that frame will be transmitted in a single pulse (burst), each of which will be at least 64kilobits (8kilobytes). This will generate a burst of 4 to 8 maximum size packets in a short continuous stream. This will repeat 5 to 20 times each second. When this traffic exists solely within a single LAN[8], the impact will be minimal. Where this traffic has to traverse lower-speed networks (such as WAN, Microwave, Satellite or Internet networks) or networks already experiencing some congestion, this pattern of time-critical traffic can have a substantial impact on such resources as WAN/router performance, reliability and quality of IP telephony, backup time, capacity planning, and network management. The impact of these large data packets is further multiplied over legacy or long-distance network connections.

Constant Traffic

An often unexpected impact of real-time streaming video such as CCTV over modern networks is that this workload can cause much greater congestion in small to mid-range network equipment than would normally be expected. Modern networks and protocols are designed to handle relatively random traffic arriving as short, medium- to high-volume bursts, followed by a period of calm. The semi-continuous stream of large data packets that typifies the collection and capture of near-real-time CCTV footage acts to generate a constantly repeating interruption to the 'normal' flow of network operations. The larger and more capable network equipment is designed and built with sufficient local buffering capacity to smooth this localised congestion, and still provide most efficient functioning. Less capable equipment will however suffer local inconsistencies of packet-delay and port congestion that can have a visible impact on the display of real-time streaming video, and a disproportionate impact on time-on-delivery services such as IP telephony. Unlike many streaming video applications, it is not feasible to pre-load live-stream CCTV video.

Data Volume

The storage capacity required to support this volume of data for even a small installation is staggering. As discussed above, a single medium-resolution camera can generate over 6Gb of video per day, 200Gb/month or 2.4Tb per year. An environment such as a small university campus, technology complex or passenger terminal may easily have over 200 cameras. These cameras alone would generate over 128 megabits/second of traffic (enough to fill over 80 home ADSL connections) and need more than 1,300Gb of storage each day. Providing the capacity to store 28 days of this data will require close to 40Tb of disk and/or tape. While the physical dimensions of this storage are roughly equivalent to a bar fridge, it would draw about 4 kilowatts of power[9], and would need to be maintained in an air-conditioned and environmentally controlled room (with a set-up cost of $50,000-100,000, and commercial rental costs for the space of around $3-4,000 per annum).

Network infrastructure faces similar challenges due to both the volume and nature of the traffic. On initial inspection, 0.64 Megabits/second does not appear difficult to modern network professionals who implement networks based on 100 or 1000 Megabit connections for local and/or campus networks. Using the example above, however, the deployment of just 200 cameras requires either the deployment of multiple dedicated 100 Megabit services, or upgrading core networking infrastructure to support 1,000 Megabit solely to service the CCTV management facility.

Data Storage

When contemplating the provision of capacity for storage of CCTV footage, a number of decisions need to be made with respect to how and when the footage will be used, and for how long the footage will be available. Due to the data volume already outlined, many organisations have a hierarchical scheme for maintaining their CCTV footage. For instance, they may by default, keep all cameras for 24 hours, 25% (of-interest cameras) for 48 hours, and 5% (entry/exit cameras) for 7 days. Using the figures described above for 200 standard resolution cameras, this would require: 1.3Tb for the day, 320Gb for of-interest, 330Gb for entry/exit – or about 2Tb purely to support storage of transient CCTV data.

There are several important points to note about this environment. First, it does not provide for storage of ANY video footage beyond seven days, thus any archival or *ad-hoc* storage, labelling, marking or indexing of footage would have to be managed both separately from this system and within those time-frames. Second, this example uses a fairly low resolution environment, such as one that is designed primarily for security guard use, rather than being of use for law enforcement or investigation. Finally, as a point of comparison, 2Tb of storage would constitute a substantial portion of the full corporate data storage resources of many commercial and government environments.

[8] Local Area Network – specifically in this case, a high-speed switched network (100Megabits/second or faster).
[9] An energy efficient office building uses 0.90watts/ft^2 (9.7watts/m^2), thus 4kw would light over 4000m2 of commercial office space (California Energy Commission 2008, p.2).

Design, operation and audit problems

The factors outlined above add a layer of complexity in the design, implementation, day-to-day operation of a data environment, as well as in the review and audit processes. This complexity will vary according to the organisation's policies and legislative requirements. These aspects are beyond the scope of the current paper, but warrant further exploration.

LAW ENFORCEMENT IMPLICATIONS

The data volume and impact outlined above constitutes significant implications for any organisation. They are particularly relevant to police forces because CCTV is receiving increasing attention internationally as a point of synergy between emerging technologies, mounting financial constraints on public institutions, and growing demands for visible policing in increasingly risk-averse societies. Indeed, 'the most common reason advanced for installing CCTV in town centres has been to combat loosely defined "anti-social behaviour"' (Wilson and Sutton 2003, p. 2).

Our concern is that installation of these systems places unrealistic expectations on police in terms of ability to resolve crime accurately, as well as unsustainable resource needs that will have significant impacts on other areas of police capacity unless expertly managed. The most recent CCTV systems serve their *intended* purpose very well when installed competently and professionally, with well-defined areas of use. However most such systems are utilised for area surveillance – that is, to provide a general overview of a broad area rather than providing close, sharp images of a face. This renders them close to useless for prosecution in many cases.

The fidelity required for CCTV to be effective in investigation and prosecution has extreme implications for networks and storage. Compounding this, the vast majority are installed by salespeople rather than network specialists, and/or are installed according to budget needs rather than outcome needs, and thus they do not effectively monitor what people think they can monitor. The importance of skilled professional installation of CCTV monitoring systems is critical to deploying a system that can satisfy the implementation objectives without severely impacting on other resources. Critically, these systems cannot be retrofitted to an existing environment, because the technology needs are vastly different.

CONCLUSION

An important question arising from this study is where this information leaves decision-makers within police forces and other organisations. In terms of what is available in the present moment, this information reveals that it is possible to have a very effective monitoring system that is targeted to carefully identified and clearly specified needs. Where this is matched by an appropriately designed system that is professionally installed and fully covered by budget, it will not disrupt other services and may be an effective supplement to other policing measures. Considering these factors carefully before committing to a CCTV system (or any other policing approach) will help to ensure appropriate expectations and operational effectiveness.

In terms of what is desirable, this points to a need to explore ways to a) reduce the raw data network overhead (for instance through improved data compression techniques that don't adversely affect visual acuity); b) enhance the stored data as and when required; and c) improve the point-effectiveness of CCTV through features such as facial recognition technology or facial feature recording. Development is progressing in all of these areas, as is the skill of professional CCTV designers and installation professionals. This means that with time and ongoing technological improvements, CCTV will become an increasingly useful tool in policing. To ensure that this becomes reality, it will be important to have clear communication from police regarding their needs and desires with respect to such systems.

There is not good evidence that CCTV is any more useful in crime prevention than any other ambient factor. For this reason, costs and technological impacts must be carefully considered, and we have shown that these are significant – and certainly not cost-savers for politically and financially pressured law enforcement agencies. Set-up and maintenance costs are further increased when monitoring, data transfer and storage costs are added. For victims of crime, such costs may appear entirely justified if they help to secure convictions, and where clear CCTV images exist, investigators and prosecutors will find their tasks more streamlined and efficient.

In contrast, low image quality, conflicting goals of camera systems (e.g. area surveillance vs. face identification), and inadequate ICT systems can severely undermine the utility of CCTV in crime prevention. In this sense, CCTV systems must be carefully planned: systems aimed at deterrence or perhaps rapid response to incidents at events such as sporting matches require significantly less storage capacity, lower image quality and thus less streaming capacity. It should not be expected, however, that such a system would be equally effective for prosecution. On this basis, it is important to fully understand technological implications as well as effectiveness of CCTV *before* systems are designed, costed and implemented.

CCTV is not a golden bullet: it requires significant financial, technological, storage and systems input to work effectively – and even then, challenges remain such as the social impacts on marginalised groups. We conclude that

police (and their governments) would be well advised seriously to consider alternative means of meeting identified needs before turning to CCTV. The kind of investment needed for CCTV that fulfils the fourfold law enforcement purpose (deterrence, rapid response, investigation and identification, and prosecution of crime) is certainly not a cost- or resource-saving exercise. Video-based surveillance systems are surprisingly resource-intense, expensive and task-specific.

REFERENCES

AAP. (2007). *Hundreds of CCTV cameras for APEC*, July 8 2007. Retrieved August 22 2009, from www.news.com.au/story/0,,22037971-1242,00.html.

California Energy Commission. (2008). Task/Ambient Lighting: Efficient, Stylish, and portable, *PIER technical Brief.* Retrieved November 22 2009, from www.energy.ca.gov/research.

Coleman, Roy and Joe Sim. (2000). "You'll Never Walk Alone": CCTV surveillance, order and neo-liberal rule in Liverpool city centre, *British Journal of Sociology* 51(4), 625-639.

Fussey, Pete. (2004). An interrupted transmission? Processes of CCTV implementation and the impact of human agency, *Surveillance and Society* 4(3), 229-256.

Gill, Martin, Jane Bryan and Jenna Allen. (2007). 'Public Perceptions of CCTV in Residential Areas: "It Is Not As Good As We Thought It Would Be"', *International Criminal Justice Review* 17(4), 304-324

Gill, Martin and Angela Spriggs. (2005). Assessing the impact of CCTV, *Home Office Research Study 292,* United Kingdom: Home Office Research, Development and Statistics Directorate.

Hempel, Leon and Eric Töpfer. (2004). CCTV in Europe: Final report, *Working Paper No.15,* Berlin: Centre for Technology and Society, Technical University Berlin.

Henderson, Zoe, Vicki Bruce and A. Mike Burton. (2001). Matching the faces of Robbers Captured on Video, *Applied Cognitive Psychology* 15, 445-464.

Japan Times. (2009) Security Camera Networks Eyed: Residential streets to get cop cameras, *Japan Times* June 26 2009. Retrieved July 8 2009 from www.japantimes.co.jp.

Johnston, Matt. (2009). Melbourne Mayor Robert Doyle ready for more CCTV cameras, *Herald Sun* August 20 2009. Retrieved August 22 2009 from www.news.com.au/heraldsun/story/0,,25957996-5000117,00.html.

JSVG. (2009). *Bandwith Storage Space Calculation*. Retrieved August 15 2009 from www.jvsg.com/bandwidth-storage-space-calculation.

Levine, M. (2000). SIDE and Closed Circuit Television (CCTV): Exploring surveillance in a public space, in T Postmes, R Spears, M Lea, S Reicher (eds.), *Side issues Centre Stage: Recent development in studies of de-individuation in groups.* Amsterdam: Royal Netherlands Academy of Arts and Sciences.

Mann, Steve. (1998). "Reflectionism" and "Diffusionism": New tactics for deconstructing the video surveillance superhighway, *Leonardo* 31(2), 93-102.

Martin, Chris. (2009). Freedom's fine line as cops go on the wire, *The Australian* July 11 2009. Retrieved August 22 2009 from www.theaustralian.news.com.au/story/0,,25761048-28737,00.html.

McCahill, Michael and Clive Norris. (2002). Literature Review. *Working Paper no. 2*, University of Hull: Centre for Criminology and Criminal Justice. Retrieved August 22 2009 from Available at www.urbaneye.net/results/ue_wp2.pdf.

McMillan, Nicola. (2009) *The Hillsborough Football Disaster: Context and Consequences,* Great Britain: Em-Project Limited.

Michael, M.G. and K. Michael. (2009). Uberveillance: Microchipping People and the Assault on Privacy, *Quadrant* LIII(3), 85-89.

McCahill. (2006). CCTV: Beyond Penal Modernism?, *British Journal of Criminology* 46, 97-118.

O'Brien, Natalie and Steve Creedy. (2009) Sydney Airport in the dark on bikie threat, *The Australian,* March 24 2009. Retrieved August 22 2009 from www.theaustralian.news.com.au/business/story/0,,25232851-23349,00.html.

O'Donnell, Aisling T, Jolanda Jetten and Michelle K Ryan. (2009). Who is Watching Over You? The role of shared identity in perceptions of surveillance, *European Journal of Social Psychology*, published online. Retreived July 8 2009 from www.interscience.wiley.com.

Privacy International. (2007). *Video Surveillance*, December 18 2007. Retrieved August 22 2009 from www.privacyinternational.org/article.shtml?cmd[347]=x-347-559088#[51].

Short, Emma and Jason Ditton. (1998). Seen and now heard: Talking to the targets of open street CCTV, *British Journal of Criminology*, 38(3), 404-429.

Singer, Jill. (2009). Bring on City's Big Brother, *Herald Sun* August 21, 2009. Retrieved August 22 2009 from www.news.com.au/heraldsun/story/0,,25957996-5000117,00.html.

Vitale, Alex. S. (2006). Review, *Contemporary Sociology* 35(2), 179-181.

Welsh, Brandon C and David P Farrington. (2004). Surveillance for Crime Prevention in Public Space: Results and policy choices in Britain and America, 3(3), 497-526.

White, Rob and Adam Sutton. (1995). Crime prevention, urban space and social exclusion, *Journal of Sociology* 31(1), 82-99.

Williams, David. (2007). Effective CCTV and the Challenge of Constructing Legitimate Suspicion Using Remote Visual Images, *Journal of Investigative Psychology and Offender Profiling* 4, 97-107.

Wilson, Dean and Adam Sutton. (2003) Open-Street CCTV in Australia, *Trends and Issues in Crime and Criminal Justice No. 271.* Canberra: Australian Institute of Criminology.

COPYRIGHT